UNIVERSITY OF TARTU
Institute of Computer Science
Cybersecurity IVCM

Alar Paas

Testing Wireless Security Alarm Systems from the Estonian Market

Master's Thesis (30 ECTS)

Supervisor: Danielle Melissa Morgan, MSc

Tartu 2024

Testing Wireless Security Alarm Systems from Estonian Market

Abstract:

The goal of this thesis is to research if wireless security alarm systems sold in Estonia are vulnerable to replay attacks, radio signal disturbance, and RFID token cloning. The possibility of recording and replaying signals from different components and alarm system hubs with the main goal of disarming is analyzed. The complexity of transmitted signals is assessed to see if there might be a chance to use a brute-force attack to break the code or build up a self-generated code-signal based on system parameters. Also, smart cards and tokens used by security alarm systems are reviewed to see if they can be cloned. An Anonymous questionnaire was made for alarm system providers and users to find out general knowledge about attacks dealt with within this thesis and to see how different parties perceive the nature of possible security vulnerabilities. Research has been conducted using the most common security alarm systems with wireless sensors provided by security product resellers and also systems purchased from the secondary market in Estonia. This research has not been sponsored by any company and presents an independent assessment based on conducted tests. Testing was conducted in the home environment, one system at a time, and only commercially available tools were used. Not all tested security alarm systems have analogous capabilities, and therefore, every system was analyzed separately according to the current specifications and components available. Test results show problems with old and new nowadays security alarm systems. Today it is possible to purchase a well-known manufacturer of wireless security alarm systems that are easily attackable. The problem is also with cheap Chinese products that can be purchased online and often do not meet any recognized security standard. As a result of this thesis, an overview is given about the security of wireless security alarm systems currently available in the Estonian market – which systems should not be trusted blindly and recommendations to mitigate possible threats.

Keywords: Replay attack, jamming, RFID cloning, wireless security alarm system

CERCS: T120 – Systems engineering, computer technology

This thesis is written in English and is 79 pages long, including 5 chapters, 58 figures, and 1 table.

Eesti turu juhtmevabade valvesüsteemide testimine
Lühikokkuvõte:

Magistritöö eesmärk on uurida Eestis levinud juhtmevabade valvesüsteemide haavatavust kordusrünnete ning raadiosegamise suhtes. Analüüsitakse võimalust erinevate juhtmevabade komponentide signaale salvestada ning taasesitada ja seeläbi valvesüsteeme eksitada ning võimalusel süsteem valvestatud olekust välja lülitada. Vaadeldakse edastatavate signaalide komplektsust ning hinnatakse võimalusi kasutatava koodi toore jõuga murdmiseks. Samuti vaadeldakse süsteemides kasutatavate kiipkaartide ja žetoonide kloonimiskindlust. Koostati anonüümne küsitlus kasutajatele ning valveteenuste ja süsteemide pakkujatele, et välja selgitada milline on üldine teadlikkus antud töös käsitletavatest rünnetest ja kuidas kogevad erinevad osapooled võimalike turvanõrkuste olemust. Uurimustöö on läbiviidud kasutades turvatooteid pakkuvate ettevõtete enamlevinud juhtmevabade sensoritega valvesüsteemide valikut ja ka järelturul kättesaadavaid valvesüsteeme. Käesolev lõputöö ei ole ühegi ettevõtte poolt sponsoreeritud ning esitab sõltumatu hinnangu tuginedes läbiviidud testidele. Testimine on läbi viidud koduses keskkonnas eraldiseisvalt üles seatud süsteemidega ja avalikult kättesaadavate vahenditega. Kõik käsitletud valvesüsteemid ei ole omavahel analoogse võimekusega ning seetõttu käsitleti iga süsteemi eraldiseisvalt vastavalt tema olemasolevatele osistele ja spetsifikatsioonile. Testitulemused näitavad, et probleeme esineb nii vanadel kui ka uutel tänapäevastel valvesüsteemidel. Täna on võimalik osta endale tuntud pakkuja juhtmevaba valvesüsteem, mis on kergesti rünnatav. Probleemiks on ka odavad Hiina turult pärinevad seadmed, mis enamasti ei vasta ühelegi tunnustatud turbestandardile. Magistritöö tulemusena antakse ülevaade hetkel Eesti turul levinud juhtmevabade valvesüsteemide turvalisusest - milliseid valvesüsteeme ei tohiks pimesi usaldada ning esitame soovitused võimalike ohtude maandamiseks.

Võtmesõnad: Kordusrünne, raadiosegamine, RFID kloonimine, juhtmevabad valvesüsteemid

CERCS: T120 – Süsteemitehnoloogia, arvutitehnoloogia

Magistritöö on kirjutatud inglise keeles ning koosneb 79 lehel 5 peatükist koos 58 joonise ning 1 tabeliga.

List of abbreviations and terms

3G	3rd Generation of cellular networks
4G	4th Generation of cellular networks
AES	Advanced Encryption Standard - a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information (NIST[1]).
API	Application Programming Interface - a system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality (NIST).
ASK	Amplitude Shift Keying
Attack tree	A branching, hierarchical data structure that represents a set of potential approaches to achieving an event in which system security is penetrated or compromised in a specified way (NIST).
Attack vector	Method attacker can use to get unauthorised access
Brute force	An attack that involves trying all possible combinations to find a match (NIST).
CSRF	Cross-Site Request Forgery - a type of Web exploit where an unauthorised party causes commands to be transmitted by a trusted user of a Web site without that user's knowledge (NIST).
DESFire	MIFARE high security contactless smart card series developed by NXP Semiconductors
DEZ	Decimal format used in Proxmark3 tool environment
DoS	Denial of Service - the prevention of authorised access to a system resource or the delaying of system operations and functions (NIST).
DREAD	Risk assessment method.Damage-Reproducibility- Exploitability-Affected users- Discoverability
Frequency hopping	Repeated switching of frequencies during radio transmission according to a specified algorithm, to minimise unauthorised interception or jamming of telecommunications (NIST).
FSK	Frequency Shift Keying
GDPR	General Data Protection Regulation
GNU Radio	An open source signal processing software development kit
HEX	Base-16 numbering system known as hexadecimal
IOS	An operating system that Apple phones and tablets use
IoT	Internet of Things
Jamming attack	A deliberate communications disruption meant to degrade the operational performance of the RF subsystem. Jamming is achieved by interjecting electromagnetic waves on the same frequency that the reader to tag uses for communication (NIST).
Jeweller	Wireless communication protocol used by Ajax devices

[1] NIST glossary for terminology and abbreviations: https://csrc.nist.gov/glossary

LTE	Long-Term Evolution - successor of 3G technology
MAC	Media Access Control – used as an identifier in networking
MIFARE Classic	Smart card technology (with broken security) by NXP Semiconductors
MobSF	Open source automated Mobile Security Framework for testing mobile applications
Modmobjam	Open source tool to conduct automatic mobile phone jamming
NFC	Near Field Communication
Ostorlab	Mobile application security testing tool for vulnerability detection
OWASP	The Open Worldwide Application Security Project
PIN	Personal Identification Number
PIR	Passive infrared sensor
PSK	Phase Shift Keying
PWM	Pulse Width Modulation
Quixxi	Solution for mobile application security and management
Reed switch	A switch reacting on magnetic force – magnetic contact sensor
Replay attack	An attack in which the Attacker is able to replay previously captured messages (between a legitimate Claimant and a Verifier) to masquerade as that Claimant to the Verifier or vice versa (NIST).
RF	Radio Frequency
RFID	Radio Frequency Identification (NIST)
RTL-SDR	A software defined radio dongle
SCTP	Stream Control Transmission Protocol
SDR	Software Defined Radio
SIM	Subscriber Identity Module
SMS	Short Message Service
SNR	Signal Noise Ratio
SSL	Secure Socket Layer
STRIDE	Model for identifying computer security threats
UID	Unique Identifier – string with a single entity within given system
URH	Universal Radio Hacker – open source tool for wireless protocol investigation
USRP N210	Software defined radio produced by Ettus Research
Vbox	Oracle VM VirtualBox
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (NIST).
Weakness	Defect or characteristic that may lead to undesirable behaviour (NIST).
Wi-Fi	Wireless Fidelity - a generic term that refers to a wireless local area network that observes the IEEE 802.11 protocol (NIST).
Wings	Wireless communication protocol used by Ajax MotionCam devices for sending pictures
XML	Extensible Markup Language - a flexible text format designed to describe data for electronic publishing (NIST).

Table of Contents

List of Figures

List of Tables

Introduction

For years, home and company-based alarm systems have been usually separate systems that use landline or mobile phone call/SMS notifications using a simple GSM modem and perhaps a voice robot. Within the last two decades, step-by-step IP networks have been taking over or have at least been provided as an option to fulfill the needs of more demanding clients. Today we live in an era where everything becomes the “Internet of Things” and wireless. Security alarm systems also benefit from wireless systems development and, over this, try to provide convenience and savings for users.

Many nowadays IoT devices are not as secure as they claim to be or to be true, many of them do not even intend to make claims. These are systems that protect us in our homes and also probably in companies or state institutions where valuables are probably from different grades. After finding only 7 papers while doing a literature review, which were actually researching security alarm systems, and all were finding problems - it seemed that alarm systems in general are not researched enough. Nisbet and Kim in 2013; Lindeberg in 2021; Lamb in 2017; Hamid and Möller in 2020; Fabial in 2019; Van Diermen in 2018; Ringvall and Ekholm in 2020 - all of these researches were finding serious problems in security [1, 2, 3, 4, 5, 6, 7]. The security alarm systems researched can be used in homes but are also used at a business level, and are supposed to efficiently protect valuables worth several hundreds of thousands of euros. Similar systems are also used in state-funded premises as it was a whole research motivation in the Lindeberg thesis in 2021[2].

The free version of “Grammarly” was used to help format small parts of text in this thesis but not to create new content. “ChatGPT” helped with proper formatting of References according to APA 7th edition.

1.1 Motivation

With the constant development of technologies, all new is accepted and pushed on the market in the early stages as it helps a lot with the general economic state and also raises funding for future expansion and to be true, becoming the first one who introduces an innovative technology in their products will control the market. This sometimes brings a situation where the released product has not actually been thoroughly analyzed against all possible security vulnerabilities. Somewhat strange examples can be taken from iPhone and iOS upgrades and updates where usually a few days later after a release an already new version with fixed security is available to download. Within the last few years, the same has happened with security alarm systems. Almost all manufacturers have decided to provide wireless devices with so-called smart functionality. As it has become a new normality, it puts in place who controls the market and who can survive or not in this competition. Nevertheless, not all companies can keep their developments up to a level that can compete with the current-day threat level. Security alarm systems are not usually managed and updated as greatly as iOS. For some systems, there will never be any updates. Some systems on the market probably have never been tested against known attacks. Some systems still use hardware today that has been declared as weak and attackable - none of us really runs to upgrade our alarm systems on a daily basis. Consumers and users take a Samsung mobile phone security patch as everyday normality but most of the security alarm system users do not even know how to update their system. According to CTV News and Washington TV Channels within the last year several security alarm systems over the world have been declared as vulnerable to some kind of attacks [8, 9]. In the NordVPN blog an article by Grigutyte was published in 2024 February about "Ring" alarm system components being hacked [10]. Most of the affected systems are not known to Estonian users and are not sold by our local providers. Nevertheless the same systems are available over online stores. The Estonian market is a bit different but the general mechanism of how the market works and how security alarm systems are designed is quite universal over the world. It is estimated that products available in Estonia can also be affected, and this thesis will clear the situation. Thorough research within our limited scope is conducted to determine the best available wireless security alarm system available in Estonia today.

1.2 Scope and goal

Concentration is on wireless security alarm systems available in the Estonian market. These systems are tested against simple replay attacks over RF channels. Cloning of RFID tokens and smart/chip cards provided with the systems is also looked at. Systems reaction to radio signals disturbance is investigated and tried to find if systems are secure or can be bypassed. To the best of our knowledge no publicly available research has been done yet to analyse the security of the wireless security alarm systems chosen for this study. Nisbet and Kim in 2013; Lindeberg in 2021; Lamb in 2017; Hamid and Möller in 2020; Fabial in 2019; Van Diermen in 2018; Ringvall and Ekholm in 2020 were analysing the security level of alarm systems within different scopes, but none of them concentrate on wireless replay attacks or radio signals disturbance testing on the systems covered in our research [1, 2, 3, 4, 5, 6, 7]. RFID attacks are handled also by several researchers like Fernandez-Carames in 2017; Morgan in 2017 Pistorius in 2023 and Mackewicz in 2020, but this thesis does not go into theoretical level, but conducts practical tests with systems available to us having this function included to give overview of general security level used [11, 12, 13, 14]. Outcome of this research ideally would be a method to defeat the certain alarm system together with documentation of used attacks and results achieved. Even if the system turns out to be tough enough that an attack will not work during our research then at least documentation is collected as a start point for further analyze. Questionnaires aim to gather more info about how well people are informed about security of wireless alarm systems and if providers are aware of potential threats.

Limitations: availability of the systems, money to purchase systems; time to analyse systems; knowledge of actual systems weaknesses and available attack tools. Wi-Fi or mobile phone signals replay and hacking of applications are excluded from our scope.

1.3 Problem Definition and Research Questions

Research question of this thesis would be to find out if it is possible to bypass or disable wireless security alarm systems by using following methods set by our scope and limitations: cloning systems RFID tokens; conducting replay attacks on wireless signaling and disturbing the radio signals from effectively reaching their destination. Wireless security alarm systems available in the Estonian market are examined to find out the actual situation about their security. Our hypothesis is that it is possible to defeat the systems to gain access to the guarded premises without the system notifying the user about break in.

For years, alarm systems have provided security in several layers including homes, cars, warehouses, businesses, state parties, banks and so on. For some reason there is not much information about the research of these systems providing that essential value to our lives. It might be that manufacturers keep their mistakes or known weaknesses to themselves for financial and business reasons. Nevertheless researchers claim that alarm-systems are not secure enough and can be defeated by cheap means. If a security is really in that level then it raises a question about an overall fiction of security provided by alarm systems. Today there is no adequate information about the security level of wireless security systems available in the Estonian market. Thesis tries to answer this question by looking into the basic level of attack vectors that have been noted as successful on other systems elsewhere in the world. It is also tried to find out if a more expensive system is actually better or follows the same pattern as its cheaper competitors.

1.4 Novelty

Novelty in our study is to do a research against the wireless security alarm systems available in Estonia taking into consideration three simplest attack vectors. According to our knowledge no-one has actually provided active test results about conducting replay attacks against wireless security alarm systems available in the Estonian market. Nor have these systems been tested for RFID tokens security and response to disturbance of radio signaling. Main contribution is to give more knowledge about available wireless alarm systems weaknesses and strengths in general as this area is under examined. No one according to our knowledge has analysed higher end expensive wireless systems within our scope.

1.5 Contribution

Several cases according to articles in newspaper “Postimees” and also statistics of the Ministry of Justice have shown that burglary and break-ins have been increasing since 2020 and there have been documented cases where alarm systems did not function properly for unknown reasons [15, 16]. Our goal is to research some of the wireless security alarm systems' possible deficiencies to see if problems could be related to poor security of the systems themselves.

A questionnaire was made about security alarm systems to address people who have systems, who do not have systems and also to systems providers. The results of this questionnaire are going to illustrate how people perceive security in general and how they feel about systems that they have; how much people actually are aware of threats and what is actually important to them. Also points about using wireless systems instead of wired ones for the convenience level upgrade are observed.

Security level of the wireless alarm systems available in the Estonian market is evaluated to derive a general estimation of protected premises real security based on results of our tests correlated with people’s answers in the questionnaire.

Cheap Chinese wireless alarm systems which are currently invading our market are compared with brand products available by recognized suppliers. Most secure wireless security alarm system in the Estonian market within our limited scope will be given as a result.

Main aim of the thesis is to draw attention to the possible weaknesses and vulnerabilities of wireless security alarm systems and raise general knowledge about the theme so people would think before trusting systems blindly.

1.6 Structure

The thesis contains 5 chapters. In Chapter 2 background information of alarm systems in general is presented with literature review and summary of known problematic systems. Attack vectors and wireless security alarm systems user and provider questionnaire results are overviewed. Chapter 3 will focus on practical testing methods and results are given in Chapter 4. In Chapter 5 summary with conclusions and recommendations is given. Appendices contain questionnaire questions overview and detailed information about tested systems hardware and firmware. Also a more detailed overview of the Paradox and DSC systems signals analyze process is given. A full version of the possible attack tree is presented and lastly licence of this thesis.

1.7 Ethics

From an ethical perspective it is highly ethical to let people know about possible flaws in systems they own. More damage will be caused when only criminals and bad people who have done their research have access to the knowledge of how to attack wireless security alarm systems and the common people have no idea that her or his system can be simply blocked or disabled without any notification. Open discussions were held with some of the suppliers to get their perspective and it seems that some of them already knew about possible problems connected to the systems that they sell. Others only mentioned that it is interesting research and as they do not have power to conduct their own research they would also like to know if there are any problems with systems that they sell. Possible outcomes have not been discussed with manufacturers since the latter is adequately aware of the security level of their products and are possibly keeping that level for business reasons like it is. Also because the vectors touched by this research are in general known for a long period of time and all reasonable security providers have had enough time and opportunities to test and fix their systems. While gathering information with questionnaire it was kept simple and avoided gathering any personal information whatsoever. All dataset given in the research is based on individual research and all data is gathered over testing and anonymous questionnaire. No harm of any kind is being done deliberately during the research and all possible measures are taken to avoid interfering with other systems and the environment.

2 Theoretical overview

2.1 Background

Acumen Research and Consulting has been indicating that the home security alarm system market globally was estimated to be over 51 Billion USD in 2021 [17]. And it is estimated that in 2030 it will grow up to 106 billion USD [17]. In the beginning of 2024 it was estimated by Dun & Bradstreet that annual revenue was over 88 billion dollars [18]. These numbers will describe the actual importance of home alarm systems in general perspective. The growth of this market has been immense in the last few years. As technology has evolved and systems get more affordable in time to people in general, the expectancy of having a home alarm system has started to be a normality when buying a new flat or house. It is possible to even say that having a home alarm system has become a certain norm in From estonian real-estate website "www.kv.ee" it is possible to see that nowadays almost all new buildings in Estonia are designed to at least support the alarm systems for several years now [19]. As getting all the cable works done even to have preparedness of the system is quite expensive for real estate developers then new wireless alarm systems get more and more desirable. These wireless systems also are very welcome for the people who live in the older apartments and houses where it is really hard or expensive to install new cabling.

In today's world there is constant development of burglar alarm systems. The main goal seems to be- not to be left behind, compared with other competitors and it means that companies rush together with this century modernization scheme meaning everything ends in the palm of the human hand on a small screen. But not all companies are there yet and it seems that for some companies it is more important to make money instead of providing real security. Security and safety are basic needs for humans to operate correctly. Without proper relaxed safe feeling people will get anxious and their quality of life suffers greatly. Saul MCleod, PhD - describes in the "Simply Psychology" article that safety and security in general are on level two in Maslow's hierarchy of needs pyramid [20].

Home alarm systems are the exact product that is pointed towards this market. Most providers know that security is a state of mind. And it depends highly on threat sense and knowledge. SDM Magazine provides a 2021 year annual revenues overview and it also illustrates companies efforts to make profit [21]. There are a lot of different alarm system providers who all want to acquire a share of the market and some of them do not care if the earned money comes from taking advantage of common people's poor knowledge levels. It is a commercial industry like any other where there are companies who have developed their products while taking account threats and assessments compared with a return of investment and most likely chosen the acceptable middle way to fit the market cap properly. Cap in the market is different in different geographical areas and also depends on demographic and financial properties. Many providers want to get a part in the new wireless "IoT era" bubble. Same situation is occurring in the home alarm market.

As there has been different information coming from the world describing that some of the alarm systems are not secure enough it was decided to conduct a similar research in Estonia and focus on the systems provided in Estonia. Thefts have been rising in recent 3 years according to the Ministry of Justice and in newspaper "Postimees" there have also been articles including insights that alarm systems have not been functioning properly [15, 16]. Figure 1 provides yearly statistics of thefts in Estonia and it can be seen that since 2020 the curve has gone back up and is rising.

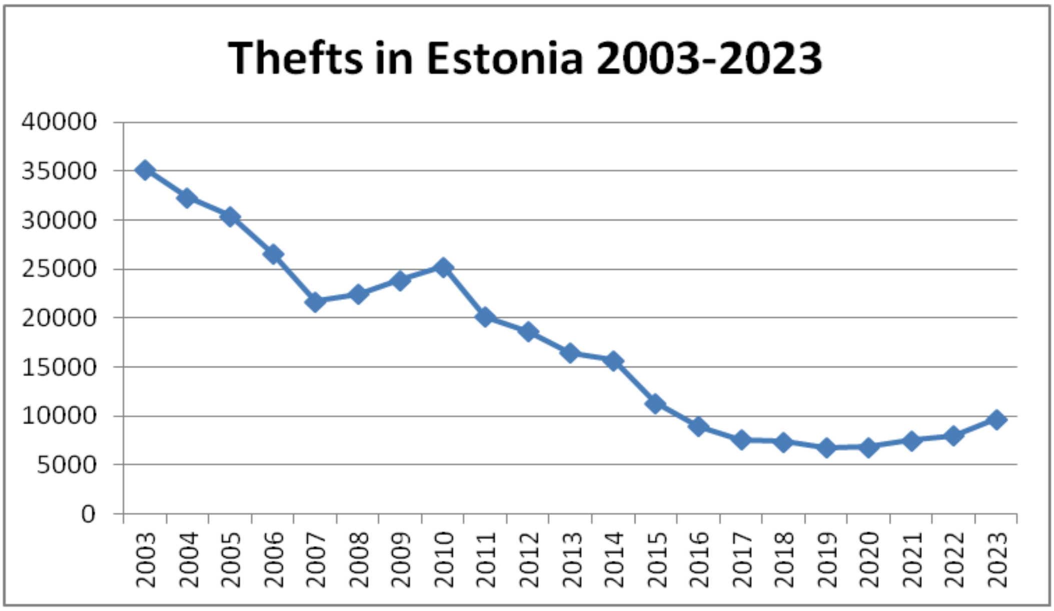


Figure 1. Statistics of thefts in Estonia according to the Ministry of Justice [16].

Police captain Inna Toater gave a good overview about burglaries in recent years in Estonia during interview on television show “Terevisioon" at the 26th of the March 2024 [23]. It was noted that burglaries and break-ins into people’s homes have been on the lower side in recent years but still numbers reach 200 and even more in a year. Most of the thefts which happen together with break-ins are against businesses and construction sites and other public places - numbers go above 1000 burglaries in a year. Toater also mentioned that a big part of attacks are being done by professional thieves and other parts are usually covered by addicts who are looking for easy money for the dose. Figure 2 illustrates mentioned numbers on a graph.

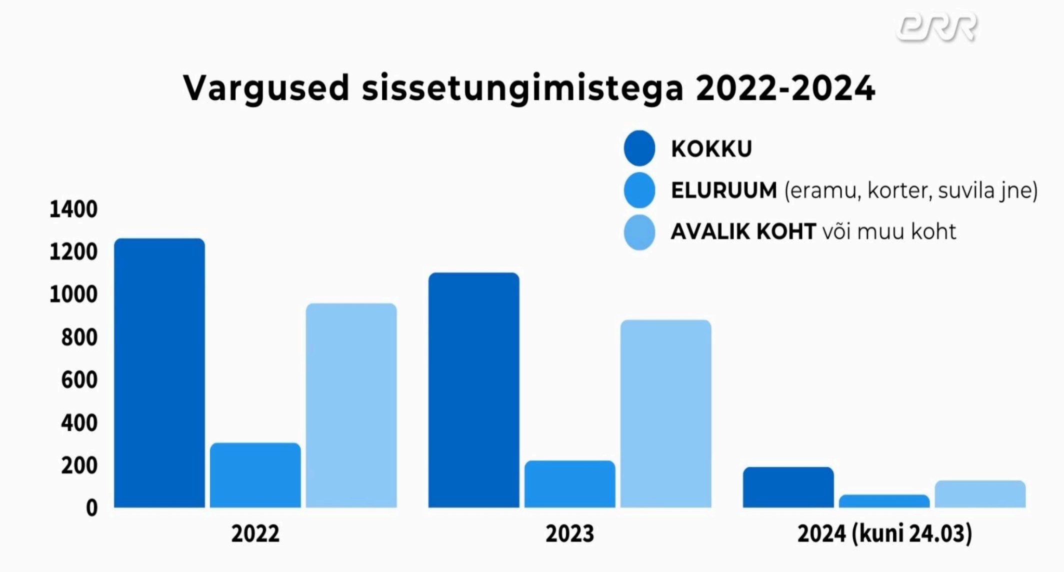


Figure 2. Burglaries in Estonia according to Police captain Inna Toater [23].

As general statistics of the thefts have been rising Police are worried about it also transferring into burglaries having more personal influence and are warning people to better safeguard their premises and not to share everything online especially when it comes to holiday pictures or other info letting a wider amount of people know that they are not at home.

2.2 Literature review

For literature research Google Scholar and Scopus were used. Terms like: alarm system; cyber security; home alarm system; burglar; ethical hacking; RF radio; intrusion detection; radio channels; residential alarm; wireless; paradox; G4S; Ajax; Jablotron; security; smart home; penetration testing; sensors and some other terms by themselves and in different combinations were used to filter out relative content to us. Over 40 documents were collected and further analysed of which 7 were discovered as actually related. Also open web search using Google search engine and YouTube video search was conducted to find related information.

Related researches:

A. Nisbet, M. Kim (2013), "Security Analyze And Forensic Investigation Of Home & Commercial Alarm Systems in New Zealand: Current Research Findings" [1]. This is a research about attacking keypads PIN number of alarm system having a Paradox system as an example. It is an experimental study. They concentrate to see if it is possible to brute force these keypads taking into account most usual used 700 passwords in New Zealand. They can see in year 2013 that this home and commercial alarm security area is not properly researched. As a key finding they claim that it is possible to brute force the Paradox PIN keypad (space 10 000 numbers) system within a few hours. It is valuable knowledge to take into account doing our research that there may be weaknesses in PIN management. Research gaps of this study can be counted in as no RF level attacks observed; no application or software/firmware level analyze. This kind of brute force attack can be considered as a physical vector attack as it needs actual physical presence. Nevertheless Nisbet did not include other physical or cyber level attacks. Our research adds a view that concentrates on wireless keypads.

Lindeberg Axel, (2021) "Hacking Into Someone's Home using Radio Waves: Ethical Hacking of Securitas' Alarm System" [2]. A.Lindeberg conducted a real life scenario of attacks on the real SecuritasHome alarm system. He found out that the current system has its own weaknesses and can be quite easily attacked using radio wave replay attack. Lindeberg managed these weaknesses ethically and was in constant contact with providers. Lindeberg realised that alarm systems in general are very complex and it is not possible to conduct a thorough research that covers all the possibilities and attack vectors. So several delimitations were made before starting the study. For example cloud servers and 3G wireless telecommunication together with Android and iOS application analyze and also physical level attacks and peripherals were excluded. His main research problem was stated by the Swedish army and it was to find out with exact wording: "Is the SecuritasHome Home Alarm System secure against cyber attacks?". Lindeberg used a seven-step penetration test methodology by Weidman (2014) [24]. He conducted threat modelling according to Guzman and Gupta (2017) technique that is specialised for IoT systems together with ETSI EN 303 645 standard [25]. His data was collected by researching available materials and by experiments on real system and analyze of its behaviour. OWASP IoT Top 10 (2018) was followed and 5 different related studies were examined [26]. Lindeberg used the Universal Radio Hacker tool with HackRF to conduct a replay attack on the system and he was successful. In general a reverse engineering to some level of RF part and decomposition of the system was made. This thesis will have similar delimitations and even as our systems will be from different providers it is going to also include the RF part and replay attacks but also would like to include peripherals signals into that research. In general Lindeberg's study was well performed and gave a good example of how these analyses give actual results. Testing 14 different systems instead of one sets things in different perspectives and more practical work is conducted leaving high level theory in second place.

Logan Lamb, (2107). “Home Insecurity: No Alarms, False Alarms, and SIGINT” is another good material that supplies real attacks on home alarm systems [3]. In his study he is compromising three systems ADT (largest home security dealer in North America), Honeywell and Vivint. Lamb is also attacking RF fields by analyzing systems and doing research and experiments with systems to gather information. Lamb used USRP N210 SDR and GNU Radio. Lamb also applied jamming attacks that generate a DoS attack vector. Lamb uses reverse engineering on packet level and uses replay attacks. Problem statement is simple: sold systems are not providing enough security – and to prove that Lamb manages to successfully attack three different systems. Research gaps can be also derived from earlier – systems available in Estonia are not analysed. Again Lamb work was done in 2017 – all these attacks should be known to our supplier and weaknesses should be repaired.

LE. Hamid, S. Möller, (2020).“How Secure is Verisure's Alarm System?”study researches Sweden's most used alarm system and found many *CSRF* weaknesses that can be used to take control over the unit [4]. Hamid and Möller focus on the signaling going into the main unit and signaling going out from it. Research topic itself gives the problem statement. Hamid and Möller identify the threats using STRIDE (Kohnfelder and Garg 1999) and DREAD (LeBlanc and Howard 2002) models. Different use cases or setups are handled. Forwarded information and commands are analysed by Wireshark. All threats are assessed and penetration testing is conducted. According to found weaknesses 17 different penetration tests are done and 7 vulnerabilities are found: DoS on the Vbox’s SCTP host; CSRF for refreshing authentication cookies; CSRF for creating new alarm system users; CSRF on user settings; Brute force and DoS on users’ 4-digit combination; CSRF on the “disarm“ functionality in the web application; DoS on a user’s mypages account. Methodology of this research is experimental and relies on immense theoretical background, a conclusion Hamid and Möller define that Verisure has not done a proper software security analyze. As a research gap comes out RF level attacks and physical level. RF level will be elaborated in our work against our chosen systems but network and application testing levels are excluded.

Dan Fabian, (2019). “Examination of LUPUS-Electronics devices” [5]. An examination of the alarm system that is provided in Germany. Of course this research problem is to find out how secure the unit is. Fabian found a shared SSL certificate problem; root password was derived from MAC address; configuration (including current passwords) was downloadable without authentication; XML API was vulnerable to CSRF. In general the conclusion was to update the device to new firmware after discussion with the vendor. Nevertheless it never came out how many old systems are out there and waiting to be exploited. Fabian's work gaps are related to physical and RF fields. Also none of our chosen systems has been addressed.

Rob van Diermen, (2018) “The Internet of Things: a privacy label for IoT products in a consumer market” [6]. This thesis includes a part where the Egardia alarm system, which is available in Belgium, France and Germany, is penetration tested. Information was gathered and vulnerabilities were found. For example RF signaling attacks; physical attacks; cloud service was running on HTTP – so everything was sent in clear text. It was possible to turn off the alarm remotely; open telnet ports etc. Tools like Quixxi, MobSF and Ostorlab were used to assess mobile application weaknesses and several were found. Risk assessment was conducted. Diermen did thorough work and it is a good example but 6 years old and not against our systems. Nevertheless if these attack vectors have been taken seriously by providers then today's researches should not find any similar problems anymore.

L. Ringvall, O. Ekholm, (2020) “Penetration Testing of GSM Alarm: Using Radio Frequency Communication“ [7]. Testing a home alarm system “Home Secure Basic V2" which is provided in Sweden. Research question: “How can radio frequency attacks be used to disable the alarms of HS-BASICV2?“. This system uses a GSM module and 433MHz radio module. Both of them are radio devices that can be examined for possible attacks also in our thesis. Ringvall uses threat modelling and identifies threats by STRIDE (similarly to Hernan 2006) method. He breaks his penetration testing into two parts as a theoretical assessment of potential security vulnerabilities and then a real life testing. He uses RTL-SDR to conduct brute force attack and replay attack and sniffing attack – jamming was not conducted. Ringvall found that the replay attack was quite easy and successful. He mentions also that there are several different similar alarm systems out there in use and it would be vital to assess all these systems in future as they are protecting real valuables and it would be harsh if some big systems fail due to poor alarm systems. For this reason it was tried to look into many different systems available in our market at the same time. Ringvall’s work was similar to other real alarm system assessments - after thorough theoretical search a practical attacks were experimented and as before on other researches they were successful. It only determines that our thesis topic is chosen from the right area and is valuable when examining systems available in the Estonian market. Millions of people around the world rely on alarm systems and if they are really acceptable to such kinds of attacks then this information must be available to every purchaser. Ringvall did not do a physical level estimation or attacks, neither was his work related to the systems under our observation. He focused on RF in general but all other vectors from application or cloud or firmware were also not made. Ringvall’s work and experience is a good value when estimating our systems RF vulnerabilities.

More and more people understand that security alarm systems are worthy of investigation. To be true they are protecting the most valuable items and are even part of nuclear plants security as described by White in 1999 where commercial grade items suitability is under review [27]. All of these studies were good examples indicating that there are many problems with consumer home alarm systems. Nevertheless most of the vulnerabilities found should be already old at today’s point and systems available today should be protected against similar attacks. Most of the studies only covered bits and pieces of some system parts and did not cover the entire system analyze. That is so because these systems contain a lot of different technologies and vectors all together and it is very time consuming to conduct all possible tests against all possible vectors included. Our scope is also settled with limited research about every system under observation but it is hoped to cover more systems that are actually available in the Estonian market at the same time to see if and how many of them are vulnerable against simplest known vectors. All studies gave information about different problems and all studies left something out – nevertheless getting all that information together gives us a good starting point to do our own research. In future works the scope can be broadened to also cover IP network and application level.

2.3 Summary of known affected systems – and relation to our scope

2013 - Paradox keypad PIN numbers brute force on a wire researched in New Zealand [1].
2017 - ADT, Honeywell, Vivint alarm systems researched in North America [3].
2018 - Egardia alarm system widely available in Belgium, France and Germany - researched in the Netherlands [6].
2019 - Lupus alarm system researched in Germany [5].

2020 - Verisure alarm system researched in Sweden [4].
2020 - Home Secure Basic V2 alarm system researched in Sweden [7].
2021 - SecuritasHome alarm system researched in Sweden [2].
2022 - Adobe Iota All-in-One kit; Cove Home Security System; Eufy 5-Piece Home Alarm Kit; Ring Home Security Kit (2nd gen); SimpliSafe The Essentials SS3-01 -in Canada TV publication [8]. Also broadcasted on Washington channels [9].

At the same time it is quite easy to find videos in YouTube web portal where "Top 5 BEST Home Security Systems of 2023" promote systems from the same upper mentioned brands and no information about possible security flaws is ever mentioned [28].

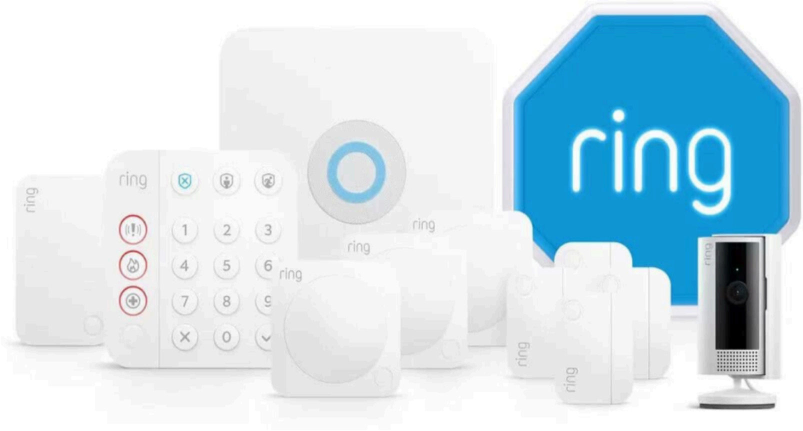


Figure 3. Example set of typical "ring" security alarm systems [29].

As security alarm systems are complex and consist of many devices and combine different technologies it is always questioned how well they are protected against attacks themselves. It is a constant race between attackers and evolving technologies. Ring security alarm system in Figure 3, which had problems with its first generation, has not effectively reached the Estonian market yet but it can be purchased over the Internet [29]. At first it was announced that the replay attack vulnerability on Ring doorbell that first generation Ring systems had was fixed with updates and second generation should be also designed to be protected against it. But just some time ago it was noted in public media that the current system was still vulnerable to jamming attacks and it is possible that some of the flaws are still there even as the system itself started using encryption [10]. This system is only one example of security alarm systems which have been affected with security problems as can be seen also from our literature review. In the last 10 years there have been similar and different related works over the world but when it is looked into the scale of how many different systems are really out there then it can be seen that current issues about security systems and their own security have not been sufficiently studied and addressed.

2.4 How security alarm systems work in general

Security alarm systems are comprehensive systems that are designed to protect people and their property against intruders and different hazards like fire and water damages. Nowadays these systems have been migrating into the IoT world and can include different automatic smart home sensors like for example smart power outlets or motion sensors with camera and two-way communication or smart-locks and even voice assistants like for example Alexa, Siri or Google Assistant. Security alarm system can consist of a wide range of components depending on precise needs and preferences of the user.

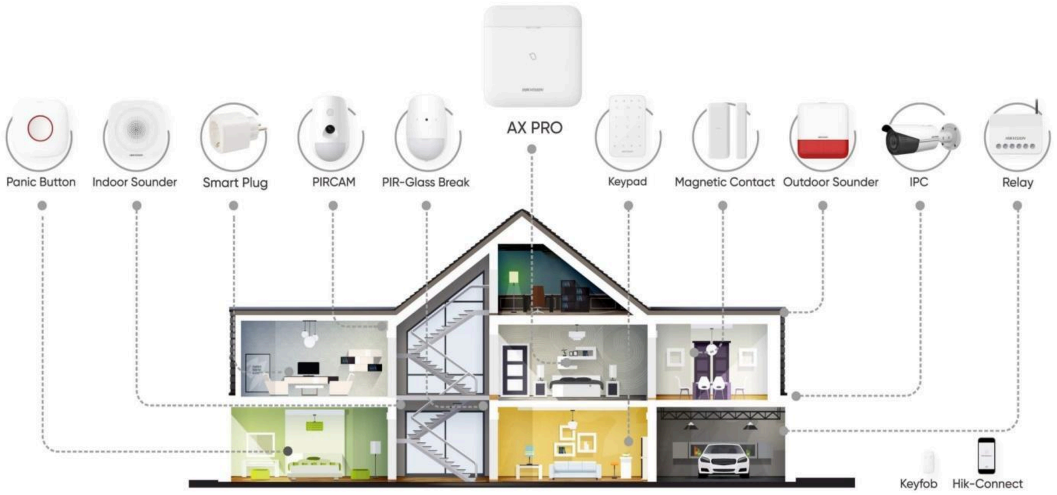


Figure 4. Hikvision AX PRO typical components [30].

Main core of the security alarm system is its hub –like Hikvision AX PRO in Figure 4 [30]. It is a brain and a heart of the system, which processes all the inputs received from the sensors and detectors in case of triggers. As a central communication centre a hub decides upon current configuration and status how to react on different signals generated by peripherals. Under armed status it will generate an alarm to notify the owners or service providing company about the situation. Alarms can be differently organized and also channels of notification can be different. A hub is usually controlled over a keypad or touchpad but it can also be managed over keyfobs and nowadays it gets more and more common to have a system that is connected to the Internet and can be controlled over mobile applications.

Sensors or detectors are responsible for control of the environment and if a certain threshold is exceeded a reaction signal is sent to the hub which is sometimes also called central station. Most usual sensors used within a security alarm system are motion sensors to detect movement inside a determined area. These are usually passive infrared sensors that react to differences in environment caused by body heat of the moving intruder. Microwave and dual technologies motion detectors also exist. Reed switches or magnetic contact sensors are sensors that react to a change of magnetic field. These, sometimes also called contact sensors, are usually used to control the status of windows and doors or other compartments to detect, if they are properly closed or not. Different sensors like glass break, smoke, gas, water leakage, temperature and others could be also part of an alarm system to provide protection to people, their premises and valuables or equipment. Because of the sensors nowadays included and peripherals like smart plugs, the systems are not referred to as intruder systems anymore. Many other options provide more than just stopping the intruders.

Importance of a local alarm capability to notify people about fire or gas hazards or intruders while asleep by local siren cannot be underestimated, but it is only a part of why people use the systems. Main reason to have a security alarm system is to protect premises while people are away from home or office. It usually means that only local sirens might not be enough and some other connectivity channels make systems actually viable. Today these notification channels can be combined over several possibilities like LTE, Wi-Fi, radio modem, landline, Ethernet and others.

As alarm systems are complex technical devices that have several different technologies overlapping and supporting each other then every normal higher level security alarm system has a proper manual. Usually it includes specialised technical information for the user and also for installers and is often more than 100 pages long. As our thesis includes many different alarm systems, exact detailed information about all aspects of the systems within this research is not provided, and all related information about certain systems can be found in their specific user manuals. Peripherals will not be assessed on a deep technical level, but will test their reaction and moreover the hub reaction on different situations connected to our chosen threat vectors including fake PIR and reed switch signaling. It is worth mentioning that usually none of the alarm systems specify their exact wireless scenarios and protocols used in detail level and proprietary protocols are used. Most of the time only used frequency is provided to declare that the system uses wireless signaling. From time to time an encryption scheme is mentioned that is most of the time AES-128.

Security standards

Different security alarm systems may or may not be in compliance with standards set by different standardisation organisations from national or international bodies from the Europe; United Kingdom etc. Some of the tested products had markings on them or on their papers. For example declaring compliance with: EN 50136-1; EN 50136-2 SP4; EN50131-1; EN50131-3 or just Grade 2 or Class II etc. Some of these standards also fix security minimums that must be met when transferring information wirelessly or being acceptable to electromagnetic interference. Standardisation verification responsibility burden is someone else's to carry and that part is left out of the scope of our thesis as some products may have everything according to set standard by the book but in real life might have some simple problem with some unrelated vector. It is decided to test all systems as similarly as possible to see how they react on our test setup independent of the papers and labels included with the systems. Previous experience has shown that some Chinese companies have their own label printers and they hardly care if their products really comply with certain standards or not what is printed on the label.

2.5 Attack vectors to get pass the security alarm system

There are several different attack vectors that can be thought of when designing an efficient attack on a chosen target. A small set of possible vectors is given using an attack tree method introduced by Bruce Schneier in 1999 [31]. This kind of modelling is not meant to provide a deep level overview of different connections between certain processes but rather to mark down different possibilities and address them one by one to see which part of the chain would be most reasonable to take while taking into account different resources and risks. Schneier attack tree is a great method, because it usually also includes out of the box thinking that is necessary when trying to figure out illegal ways. All of the possibilities would be inconvenient to provide with a pictorial model, so a list is given with a attack tree in Appendix V. It all depends on the goal chosen and level of precision and depth being addressed, but as our goal is informative, it is not dived too deep into explaining the several tree branches for example how there are 5 different methods to bribe a user and for each of these there is another splendid 10-part plan behind it. Attack tree was the foundation for chosen scope and tests.

Mentioned attack tree in Appendix V contains several ways that are not acceptable in our research and only few vectors are chosen according to our scope what will be presented here as an extraction from the fuller attack tree given in Appendix V:

OUR GOAL: Secretly enter premises protected by wireless security alarm system

1) Using the code to disarm the system (OR)

    1.3) Get the code by eavesdropping communication

        1.3.3) Eavesdrop wireless keypad radio channel on 433MHz or 868MHz to get the code

            1.3.3.2) Replay recorded messages known to disarm the system

2) Using the keyfob to disarm the system (OR)

    2.1) Get the physical keyfob

        2.1.4) Conduct replay attack using recorded keyfob signals

3) Using a token to disarm the system (OR)

    3.1) Get the physical token

        3.1.1) Clone the token physically from original

4) Avoid alarm system getting activated

    4.2) Jam the communication between sensors and hub (OR)

    4.5) Avoid system to get armed

        4.5.1) Jam wireless keypad/keyfob frequencies (OR)

        4.5.3) Jam Wi-Fi or mobile communications

There are several other attack vectors and possibilities to defeat wireless security alarm systems, but these vectors were chosen because they do not need too much specific knowledge; measures can be learned from YouTube videos and tools can be ordered from online stores easily - a doctor degree is not needed.

2.6 Questionnaire

An anonymous questionnaire was made to investigate the general situation in Estonia about knowledge of alarm systems security. A platform provided by a website “www.surveyplanet.com” was used and several different questions from users and providers were asked. Also users who do not possess an alarm system were included. Separate questions were asked especially about replay attacks; jamming attacks and smart/chip card or token/tag cloning attacks. It was also tried to find out if it has been noticed that cheap Chinese systems are conquering the market and if it is important to the users where their system is coming from. Three different questionnaires were created in Estonian and in English languages to get different people’s perspectives and compare to questions asked from providers. Thesis is not focusing on the analyze of every single question separately at a deep level. Some extra questions asked in different wording or from different angles clarified the situation and provided info to understand people's answers better. In subsection 2.6.2 we are providing the most interesting results. Overview of questions in English is given in Appendix I.

2.6.1 GDPR related information

The questionnaires were totally anonymous. All information that was collected is not related to any person or company. No personal info was gathered. All data was generalised and people giving information were notified about the purpose of the questionnaire and usage of the data. It was possible to pass questions if chosen not to answer. It is impossible to chain data in any way to certain users or companies as measures to connect data to participants identities or verify any parties were not available.

2.6.2 Results from the questionnaire

Average answerer was 44 years old. 77,3% live in a city and 86% have their own real estate. 73% do not have an alarm system at all and out of them 63,6 % say that they feel safe as they are, but at the same time 68,2% also think that having an alarm system can raise their sense of security. 13% are sure that they will never invest in an alarm system. 85,7% have heard about wireless security alarm systems and 67% would prefer wireless security alarm systems if they would buy one. 66,7% of people not owning an alarm system declare their general security knowledge as “informed and wise” and only 22% say that they need consultation in security awareness.

Questionnaire showed that Ajax was the most recommended system by providers - at the same time the medium amount of money that people are willing to give for the security alarm system is around 205€. It is not enough to get the sophisticated and reliable system that is recommended nowadays as Ajax prices easily twice or thrice as high [32]. People are willing to pay for security service 19,7€ on average a month. The AIKO system provided by Estonian G4S and using Ajax products is minimally about 32% more expensive and first time joining in for 99 € is also extra expense added [33].

Providers:

100% of providers have noticed an increase in wireless products in the last few years and 50% have noticed cheap “Made in China” alarm systems rising in the market. Ajax, Hikvision and EZVIZ products are most popular at this moment in the Estonian market, and in providers opinion clients prefer these systems because they are easy to install and use. 50% of providers also indicate that a high security level is important for customers and 33,3% also mention cheap price level. Estimated market share of wireless security alarm systems compared to wired ones is about 57%. 66,7% of providers marked that wireless systems are more expensive. 83% of the providers marked Ajax as the most popular system and 50% recommended Ajax as the most secure one. 66,7% declare that higher price brand products are more secure.

83,3% say that most of the time clients need consultation, but it is also mentioned that for some clients the security of the alarm system itself is not important.

All providers claim that they are aware of the security level of wireless systems they provide. 33,3% on the same time did not mention any standards. 33,3% of providers still sell systems without smartphone support and 16,7% claim that some higher level security systems that they sell do not support smartphone solutions. 66,7% think that cloud solutions decrease security. 60% say that clients are usually not aware of different notification channels and only 50% say that clients actually ask for systems that support different channels at the same time.

As in Figure 5 stated, notification channels commonly used by people are according to providers most of the time based on GSM or 4G. Ethernet and Wi-Fi follow and landline together with radio modem are rear cases nowadays.

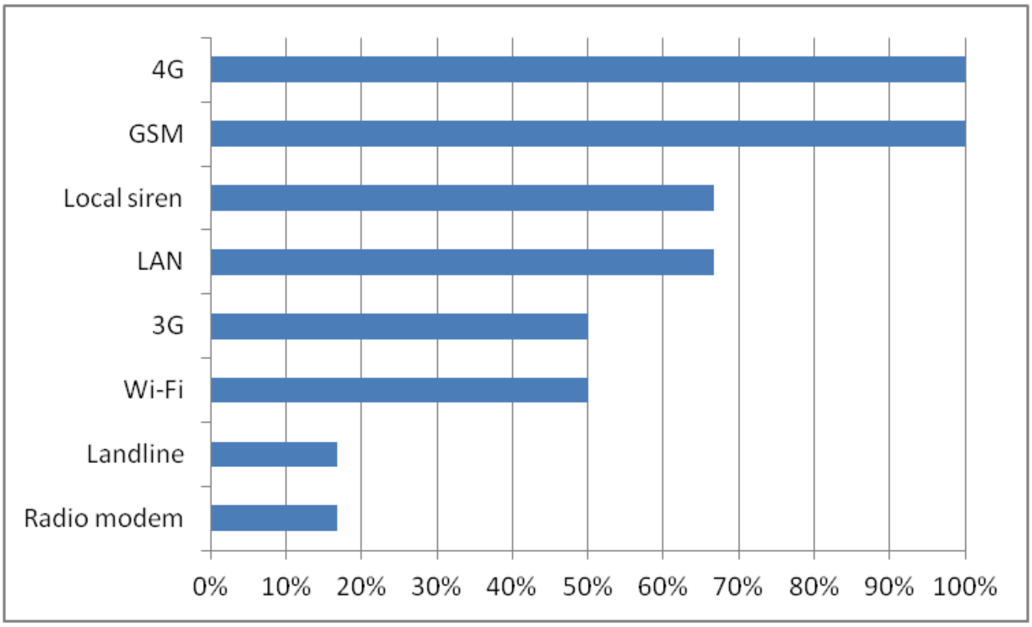


Figure 5. Most used notification channels according to providers.

54,5% of the time updates are offered automatically over providers own solution or manufacturers support over cloud service. 16,7% say that they will notify clients about the update but it is the client's responsibility to actually do it and also 16,7% say that they do not provide updates and related info to clients. 33,3% provide technicians to go to the client and update the system if necessary.

66,7% of providers test the alarm systems by themselves and 33,3% rely on trusting manufacturers information. All providers claim that they notify clients about vulnerabilities and weaknesses before the purchase and 33,3 % say that they also provide information to the client if some vulnerability or weakness has been discovered later.

33,3% say that wireless alarm systems are easier to attack and 16,7% disagree with that, 50% are not sure. 50% of the providers have been in touch with radio interference problems and 16,7% say it happens often. Only 16,7% claim that the systems that they provide are protected against replay attacks. 33,3% are sure that alarm systems they provide are protected against jamming attacks. 66,7% of the providers were unsure that their provided systems are protected against RFID token/tag or smart/chip card cloning attack. 16,7% admitted that their systems are not protected.

One provider who is selling or renting out more than 1000 alarm systems per year was sure that systems they provide are not protected against any of these three vectors - at the same time they also most likely provide Ajax alarm systems and were aware of standards. This means that providers provide what is out on the market and what buyers would buy - it is business as usual and one cannot lose a customer because the last one cannot afford the highest level products.

People having an alarm system:

100% of people who had alarm systems lived in a house. 66,7% of users have thought about security of the system itself and 70% of people owning a system would like to get consultation. As can be seen from Figure 6 more than 80% already use security alarm systems containing wireless technology. 42,9% of people owning alarm systems do not have security service and installed the system by themselves. 20% have a 3-5 years old system; 40% 6-10 years and 40% 11-20 years old system. 27,3 have been thinking about purchasing a modern alarm system. 20 % are afraid that their system is outdated. 45% only have a local siren and no other notification channel is used. 60% are satisfied with the system they have. 40% trust their system. 27% think that more expensive systems are overrated and 63% say that price depends on a brand not on real security level.

21% have security services together with a service provider system. 36,4% maintain their system once within a year or two, 27,3% say that it has not been necessary yet. Only 33,3% know where their alarm system is manufactured. 50% chose their system based on convenience of use and installation and only for 10% high security level of the system was important. While choosing their product 20% also took into account the system having different notification channels.

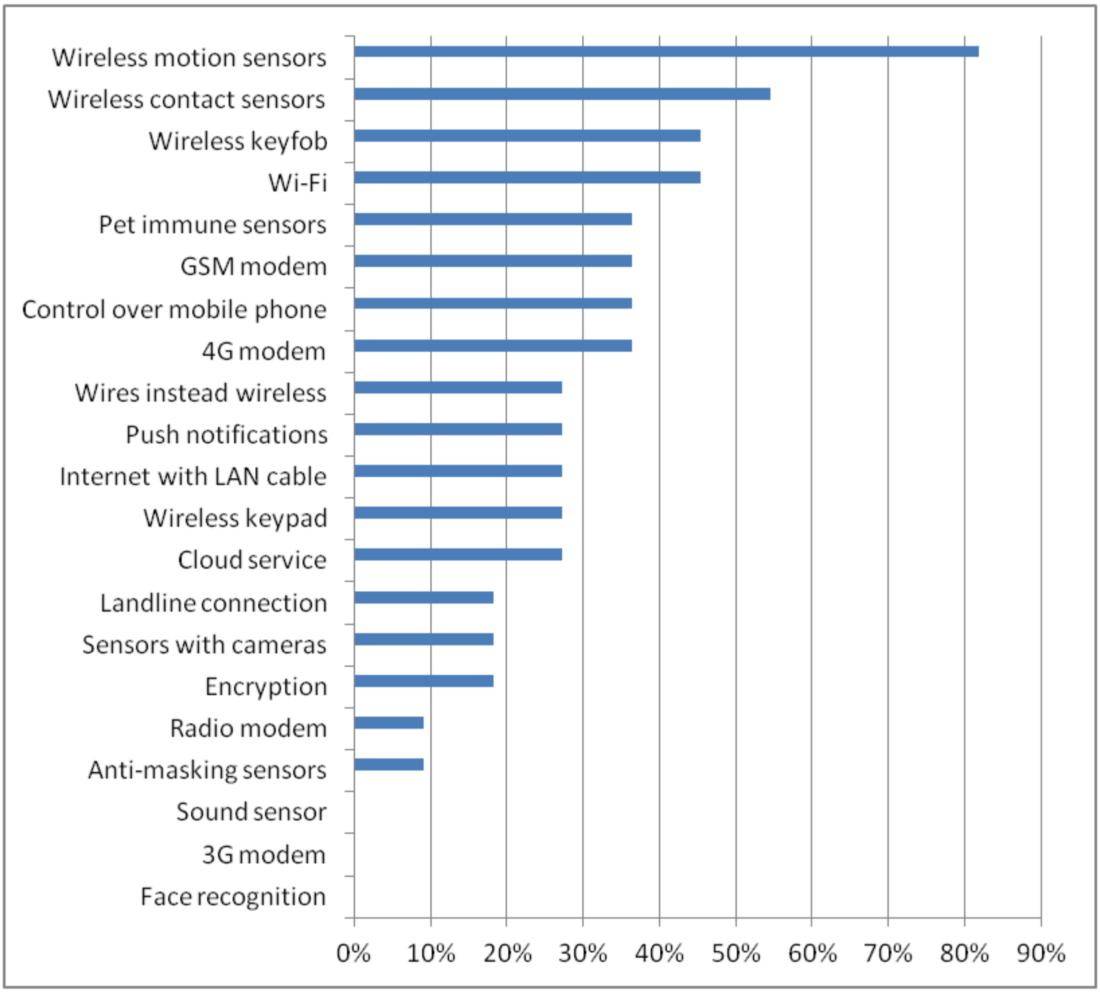


Figure 6. Overview what properties are available in alarm systems already in use.

60% do not know their system security class. 50% do not know how their alarm system updates are organized. 70% claim that manufacturers or service providers have never informed them about possible vulnerabilities or weaknesses. Cloud service increasing or decreasing security got basically equal answers both ways- only one system owner stated that had no knowledge about what it means.

0% claim that their systems are protected against replay attacks. 40% think that their systems are vulnerable against jamming attacks and others are not sure. Only 17% claim that their system is protected against RFID token/tag or smart/chip card cloning attacks.

66,7% use mobile phones to control their alarm system and 22% use an application for that. 11% do not think that using a smartphone to control their alarm system is secure. 10% of systems are connected to some other IoT device. 33% get help in case of anomalies or problems from restarting the system, 44,4% will isolate problematic issues in case of anomaly or malfunction and arm other sensors before leaving home. 20% will reach out for the service provider. 10% say that they have had an incident where an alarm system saved the day and 10% say that there was an incident, but no benefit of having an alarm system.

People not using alarm systems:

Figure 7 gives an overview about properties seen important by people who are not using alarm systems.

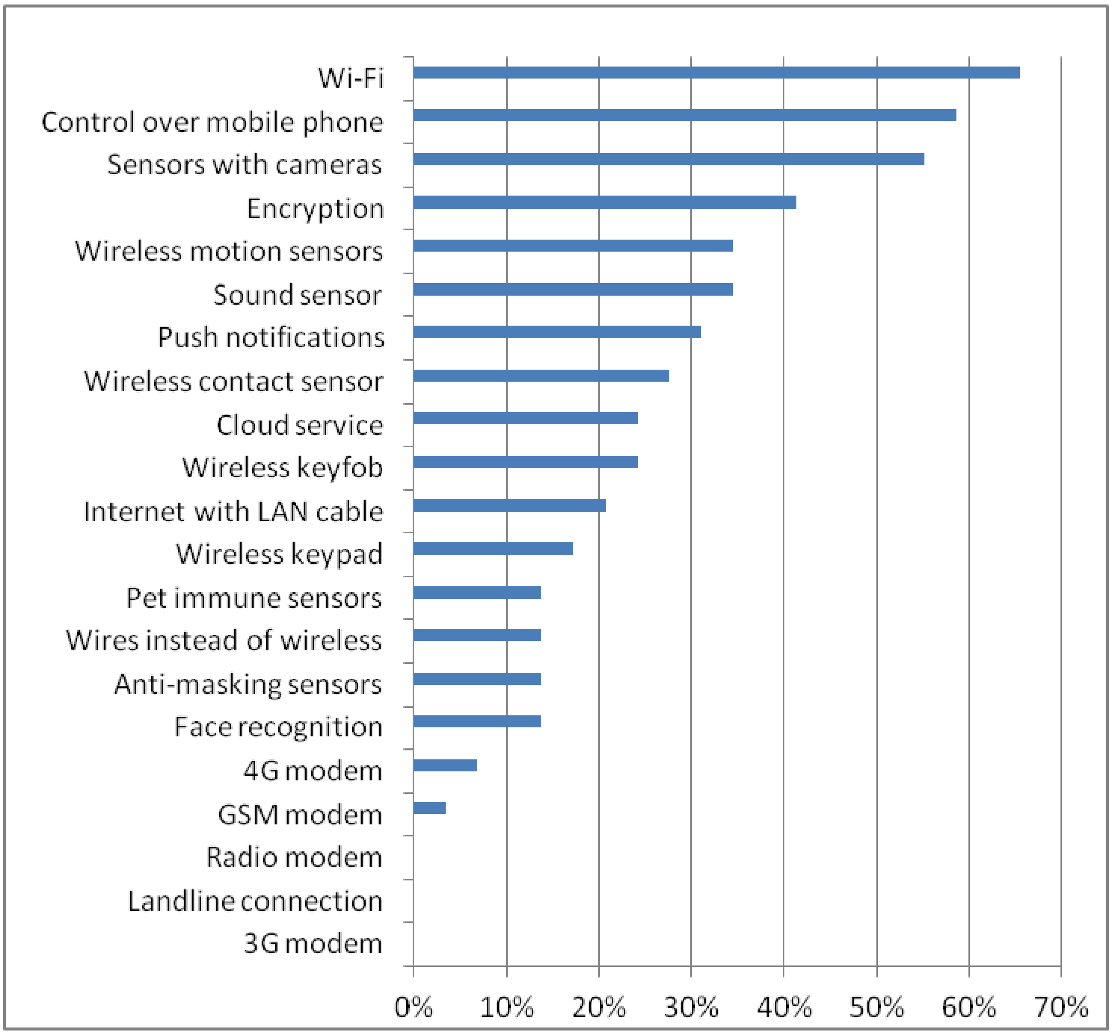


Figure 7. Alarm system properties what seem important to people not using alarm systems.

95,2% would like to use their smartphones to get notifications and control their system. 67% say that it is important that the alarm system has Wi-Fi connection. 57% think that alarm systems should have sensors with cameras. 34% care to have wireless motion sensors and 41% care about encryption.

33,3% of people not having one would buy an alarm system from an online store and would install it by themselves. 43% care where their alarm system would be made and 33% avoid Chinese products. 13% equally do not care where their product is made and care only about the price. 52,4% say that they are aware of different attacks against alarm systems. 38,1 % have not heard about RFID tag/token or smart/chip card cloning attacks. 61,9% have not heard about replay attacks. 42% have not heard about radio jamming attacks.

Correlations

Most important correlations to notice were that many users and providers and also people not using an alarm system agreed that wireless technologies are important and part of everyday life providing convenience within security alarm systems. On the same time

It was interesting how the question about cloud service raising or weakening the security split the answers. With having a sensor with a camera of course people see some privacy concerns. Also some people can see that being connected to the Internet that is full of threats also introduces the same threats to their security alarm system.

Another thing that raises caution is the age of the used alarm systems. Even if some new systems would be safe choices then when 60% of people are satisfied with 40% of the systems being older than 6 years, and 40% with older systems than 11 years and only 27% thinking about modernization - means that there might be a lot of old and outdated or vulnerable systems in peoples homes and businesses.

Information about vulnerabilities and weaknesses claimed as being shared by providers 100% of the time at least during the purchase process has reached only 30% of people. Also there is different understanding between providers and customers about price tag being relative to actual security as people tend to think that brand products are just a nice name behind almost the same product.

Most providers not being sure about their systems protection level against replay, jamming and cloning attacks was actually giving a good description of how the market works. In general everything is good but if a specific question is raised then uncertainty will arise also.

Upper Figure 6 and Figure 7 indicate that convenience of controlling and installing security alarm systems by having wireless sensors; wireless Wi-Fi connection to the Internet and push notifications on mobile phones are important to people.

Links to the survey were sent out by an email to all major public universities also including art and music or even construction and gardening students besides IT and technology related ones. For provider contacts a website “www.turvamees.ee/turvaettevotted” was used where most accredited companies are enlisted with contact information. Questionnaire was not really popular and at the point of collecting the results 45 people and 6 companies had taken the task to answer. We admit that for more qualitative results a bigger set of input data is needed.

3 Practical testing methodology

14 wireless alarm systems seen in Figure 8 were collected from the Estonian market and tested against replay attack, handling radio interference and when RFID tags or smart/chip cards were supported, security measures against cloning attacks were observed. Two Paradox sets were tested: MG5000 and MG5050+. Jablotron JA-63; Hikvision AX PRO DS-PWA96; Ajax Hub2 Plus Jeweller; DSC WP9010-K-FR; Yale Smart Living Sync Smart home alarm - IA311 were also tested. 7 cheap Chinese systems from the second-hand market over the Estonian portal “www.osta.ee” were purchased - some of them were unused systems. Three different PGST sets; three different Tecpeak sets and one G-Homa Wi-Fi-Alarm-Set produced by REV for the German market. Totally new sets were Paradox MG5050+; Hikvision AX PRO and Ajax Hub2 Plus; DSC was also bought from dealer company BK Eesti as storage leftover. Other systems were purchased on the second hand market and some borrowed from a friend. Not all systems contained the same type of peripherals so not all tests are exactly the same but based on current available hardware.

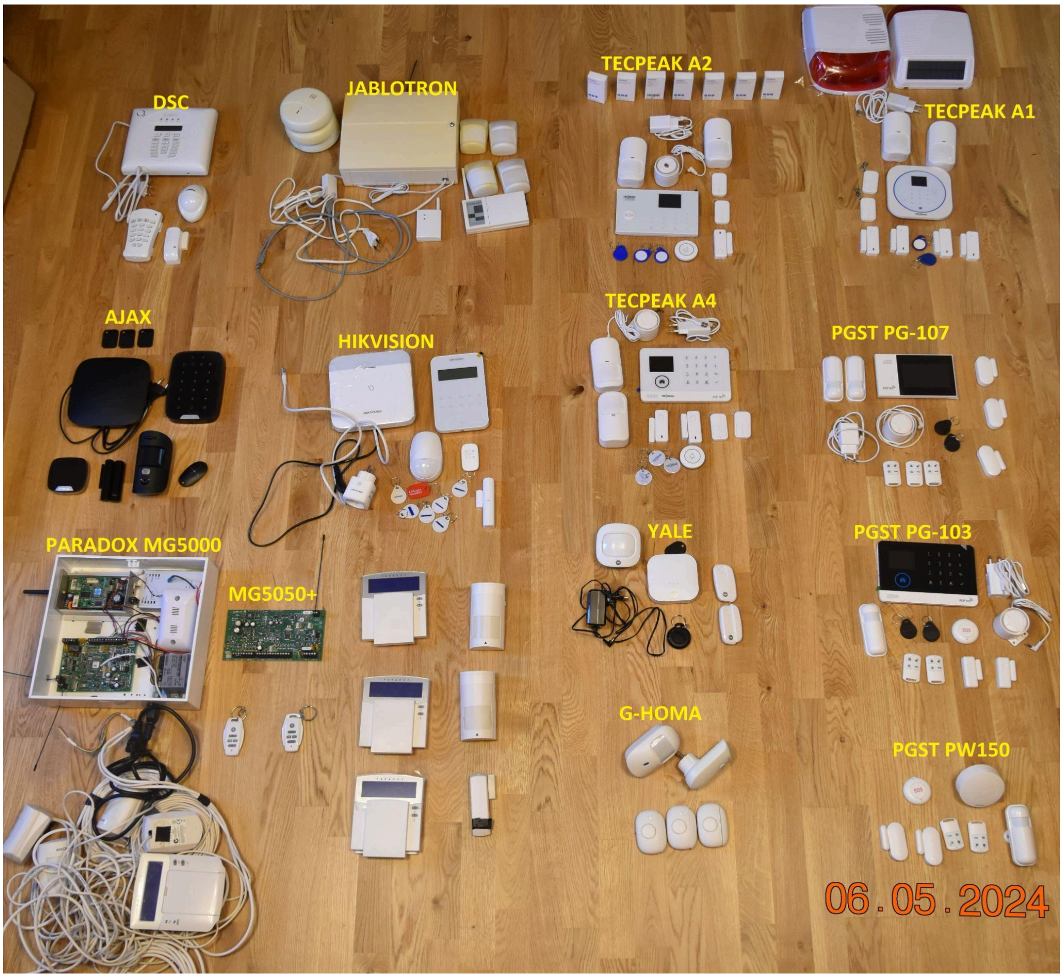


Figure 8. 14 different wireless alarm units used for practical testing.

More detailed information about the system's details with links to manuals can be found on Appendix II.

Our study will be an experimental case study. Different wireless security alarm systems available on the Estonian market were tested against radio signals replay attacks, radio signal disturbance response and also RFID tags cloning possibilities were reviewed in case systems equipped with relative hardware.

Testing environment:

For our testing a virtual environment with Ubuntu 20.04 Focal Fossa release ran on Oracle VM Virtual Box Manager (Version 7.0.12 r159484) was chosen together with URH (Universal Radio Hacker software - version 2.9.3) made by Johannes Pohl and Andreas Noack and for hardware a HackRF (HackRF One) software defined radio by Great Scott Gadgets with firmware 2018.01.1 was chosen. As HackRF's capture capabilities were not providing first class results over virtual machines several different tests with the same alarm system were made. In total several URH sample files were collected with different code numbering and this material can be used for further assessment and analyze of the used protocols in future research. Testing was conducted in a home environment at a countryside village away from other possible communications on the same frequency bands. Interference tests were conducted in the start at basement level with no windows and added extra shielding with metal pots and pans - original transmitters were taken on the farther positions where they hardly were able to reach the receiver. Only low level radio signals generated by GNURadio were used within a close range of hubs not exceeding 0.1 metres to test disturbance and only unlicensed bands were tested. Effective area of disturbing signaling generated did not leave our premises. Only our own test set was influenced. Tabletop solutions were set up with different sensors connected to the hubs at different times and working signals were analysed one by one. Even though our solution for testing is a small scale version it can be upgraded and taken to real life scenarios with the right toolset applied. It was not possible to conduct similar testing on a bigger scale real world scenario but small scale results can be transferred to determine possible results on a bigger scale.

3.1 Replay attacks

All systems were tested separately and test setup was made similar to original home based installation with a limitation to one PIR; one reed switch; one keyfob; one keypad at a time to get clear and distinguishable signals recorded between hub and peripheral device. For replay vulnerability testing purposes signals were collected using Linux Ubuntu system with URH and HackRF. This solution was chosen as it was known to us from previous lab works and access to HackRF was already available - it did not demand any extra investment. Also URH provides a possibility to analyse captured signals and it was in our interest to investigate more deeply what is the actual structure of the messages being sent. After collecting signals they were tried to replay instantly to see if just a simple store and replay attack is possible. Similar measures were used with systems PIR signals, reed switch signals, keyfob signals etc.. With keypad signals on some systems several different access codes were used while collecting the samples. Samples were compared to each other and in case two or more similar components were available then the components were switched and change in transmissions was observed to get a clearer picture of message structure used with a purpose to evaluate the possibility of brute force attack. With URH signals representation in HEX format and also in binary was produced and that info was manually compared with each-other. It is noted that it would be more efficient to use some machine learning techniques but unfortunately relevant knowledge and tools were not available. For URH frequency settings information provided by the security alarm manufacturer was used. Most systems used 434MHz and 868MHz bands that do not require any licence if operated within stated limits [34]. Exact frequencies were monitored using URH spectrum analyzer and it was verified that for recording the bandwidth used by signals were covered.

With replay attacks it was important to have two-way communication channels working while recording as otherwise some devices did not function properly.

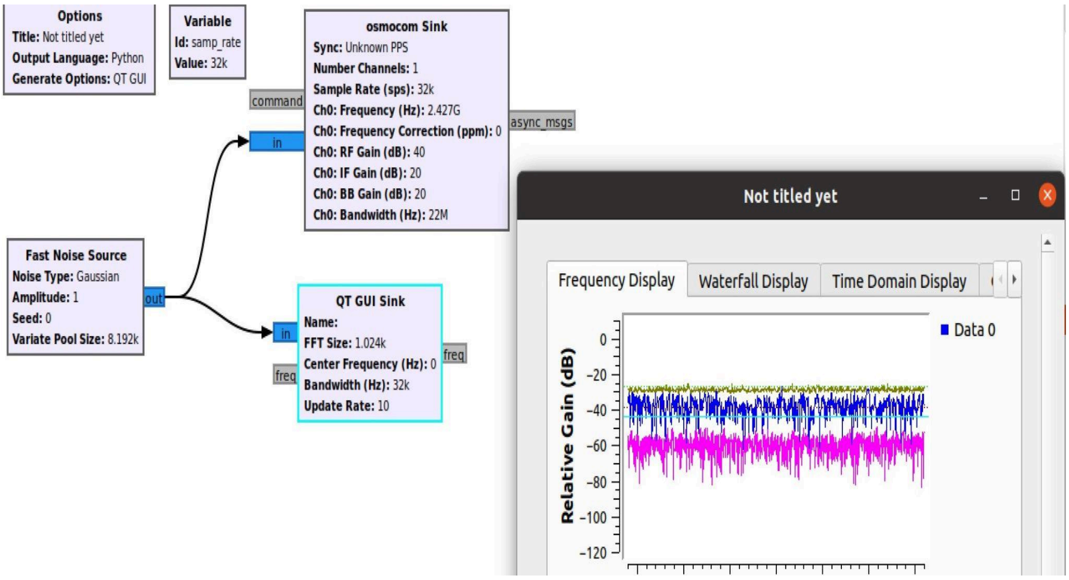
3.2 Interference testing

According to Estonian legislation and frequency plan frequencies covered by our research are noted as: “Not specific close range devices and alarm systems” at 433MHz and 868MHz band. 2400-2483MHz for “wideband data communications systems” is a typical Wi-Fi band and effectively radiated power can be up to 100mW [34, 35]. All of these frequencies do not need a special licence if a certain power level and spectral density is not exceeded and other systems not disturbed. Any disturbance generation on licenced mobile communication bands like 2G/3G/4G etc. was opted out. The guidelines of the Consumer Protection And Technical Regulatory Authority website were followed and Electronic Communications Law; Regulation “Estonian Radio Frequency Plan”; Regulation “Conditions for the use of radio frequencies and technical requirements for radio equipment exempted from frequency licence” were looked through [34, 35, 36]. Regulations stated that at 433-434MHz band it is allowed to generate a signal with power of 0dBm if signal bandwidth exceeds 250kHz, but in reality as we see power of the exiter we also need to consider antenna amplification and about -2,15dBm considering that a common dipole antenna is used. In 867,8-869,2MHz bandwidth it is allowed to generate a signal with power up to 7,85dBm and between 2400-2483MHz inside one 20MHz wide channel a signal with power up to 17,85dBm and all previous while limiting spectral access and interference decreasing measures are applied. In reality, we did not get even close to described power levels but kept our signal power most of the time under -10dBm.

Electronic Communications Law states that it is allowed to limit radio communications to provide public order and national security [36]. There is a special regulation setting rules for limiting radio communications named “Limiting radio communications” [37]. According to the Estonian Penal Code paragraph 410 the penalty for causing radio interference or transmission of false or misleading messages, if it causes danger or threat to many people's lives or health or environment is monetary punishment or up to 3 years imprisonment [38]. That is the main reason why testing was conducted in the countryside away from people and other systems inside a block built house and used metal pans and pots to shield our generated signals ever travelling out of premises on a level to influence others. None of the threats and dangers mentioned above ever emerged.

Radio signal disturbance was chosen as a testing measure because jamming tools have been more widely available nowadays, especially through the Chinese online market where it is possible to get a jammer for a few hundred dollars [39]. And according to enthusiasts YouTube channels, it is possible quite easily to conduct jamming also with SDR radios [40]. For interference disturbance testing several different means were used. Bad reception was created by moving equipment away from each other together with a basement without proper cell phone or Wi-Fi or other reception as our test environment for disturbance testing. Shielding of different components was used to imitate loss of radio connection and system response was observed - simple home kitchen pots and pans were used for that. Disturbance generator was built in GNU Radio using Gaussian noise and HackRF was used to send out signals in the frequency range used by the system under test. Similar signals were built by ourselves within URH by adding more data to the current captured signal by filling empty spaces in the time scale with copied parts from other similar signal blocks. It was made sure that during disturbance tests our transmitted signals were as weak as possible and HackRF close to receiving parties while real transmitters farther away. All activities were conducted within a controlled environment away from other possible systems and people. Especially for test purposes, a Wi-FI router was set up to try to influence its RF signals in our own and controlled environment. Mobile communications disturbance tests were not done because of the legal limits as it is a licenced band and not even short range low power devices are allowed without licence within these frequencies. Nevertheless it is known that it is one huge attack vector and can be effectively used against wireless security alarm systems notification channels to block users from getting any triggered alarm information over mobile networks. There are special tools like “Modmobjam”, “CleverJam” and others available online also for using SDR for jamming mobile communications [41, 42]. For example an Estonian company called Rantelon is manufacturing a mobile communication jammer called KJ-CaseL which can jam 12 different bands and use 20W power per band [43]. Depending on the environment this 20W power should be able to easily kill all signals near private house so burglars won't need to worry about Wi-Fi or 4G modem signals initiated by security alarm systems ever reaching their destinations. Fortunately this product is sold only to the military, not to average Joe. But if technology like this exists then villains might also have access to similar devices. To test disturbance and signal interference beforehand all frequencies were monitored with URH spectrum analyzer. Disturbance efficiency was measured by getting or not getting feedback from the system hub while triggering sensors. Also time taken for the alarm system to react was measured approximately within a few seconds precision with simple smartphone stopper function to evaluate possibility to get in and out from premises without ever noticed.

It was made sure not to disturb any other devices and kept our disturbing signals power as low as possible to conduct our testing with positive feedback. Figure 9 shows an example of a disturbance generator built in GNU Radio for Wi-Fi channel testing.



Options
Title: Not titled yet
Output Language: Python
Generate Options: QT GUI

Variable
Id: samp_rate
Value: 32k

osmocom Sink
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 32k
Ch0: Frequency (Hz): 2.427G
Ch0: Frequency Correction (ppm): 0
Ch0: RF Gain (dB): 40
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
Ch0: Bandwidth (Hz): 22M

Fast Noise Source
Noise Type: Gaussian
Amplitude: 1
Seed: 0
Variate Pool Size: 8.192k

QT GUI Sink
Name:
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 32k
Update Rate: 10

Figure 9. Example of how our own Wi-Fi channel was disturbed by HackRF signals.

3.3 RFID cloning attacks

For RFID cloning a Chameleon Ultra and ICopy-XS were used together with tokens/tags purchased from LAB401 online store as these are openly available on the Internet and can be purchased by anyone [44]. RFID cloning was conducted with ICopy-XS and Chameleon Ultra was used to read and store the tags and then emulate them for the systems. HF tags were used only by Hikvision and Ajax. All the rest of the systems that had RFID capability used LF tags. As there is not too much information about every single system, results are presented all together in Chapter 4.8.

4 Testing and results

4.1 Paradox MG5000 and MG5050+

First tested system was Paradox MG5000 wireless hub with KL37 wireless keypad and keyfob REM25. This system uses two-way communication on the 433MHz band as can be seen from Figure 10. Two different KL37 wireless keypads and 2 different REM25 keyfobs were compared to see if it would be also possible to extract some parts of signaling containing code or serial info and analyse what is actually in the air during communication. As our MG5000 hub and KL37 keypad was quite old it was decided to also include brand new MG5050+ and KL38 wireless keypad to our research. There was no tag or smart/chip card available in our system. More info about the system can be found in Appendix II.

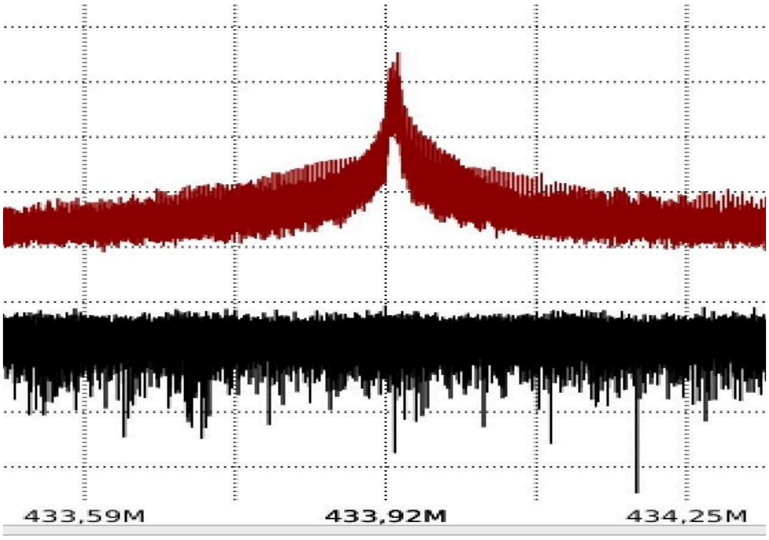


Figure 10. Paradox MG5000; MG5050+; KL38; REM25; PMD1P and DCTXP2 using the same frequency.

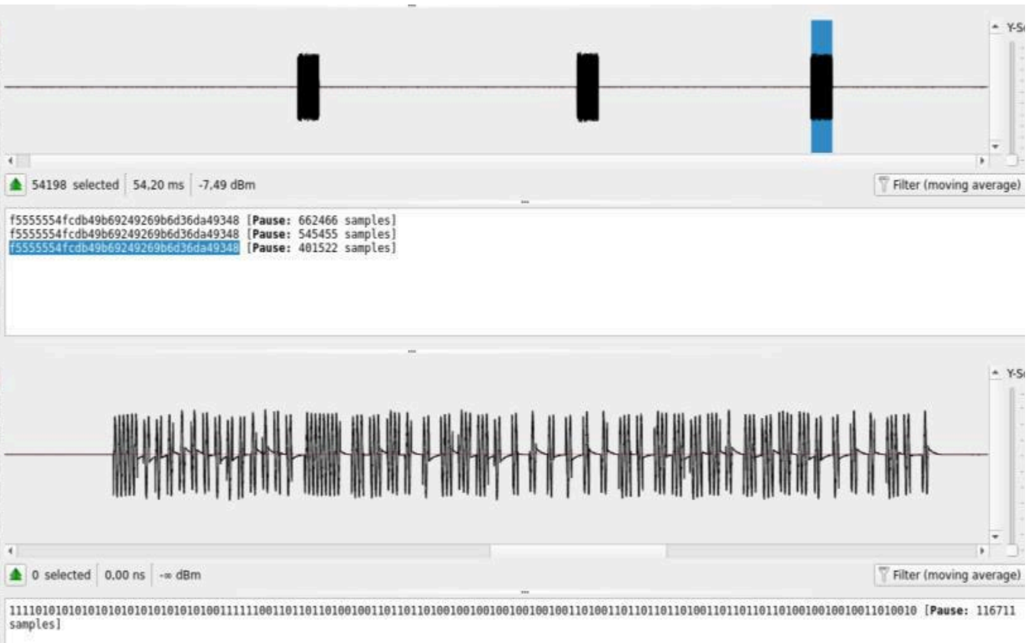
4.1.1 Replay attack

For testing effectiveness of replaying signals, system components were tested one by one separately with the hub. For testing setup system parts were separated from each other to get only one side signaling and brought close together to get both sides at the same time. HackRF amplification settings were modified accordingly with URH to provide a clear outcome. As home alarm systems are complex and combine many different parts and possible attack vectors, our scope is narrowed mainly to the part that consists wireless keypads and keyfobs and especially if it is possible to conduct reply attacks on these signals sent to the systems by wireless keypads and keyfobs during disarming and arming the system. Nevertheless a quick look into the possibility of generating false alarms from PIR and reed switch signals was taken while there was no actual triggering and change in the real environment and triggering signals were purely sent to the hub by URH over HackRF.

4.1.1.1 PIR

Wireless motion sensor PMD1P 433MHz FW: V2.02 Production week 38/2012 SN: 1270XX tested with MG5000 hub. URH detected ASK as used modulation.

False alarm generation by replying PIR trigger signals:



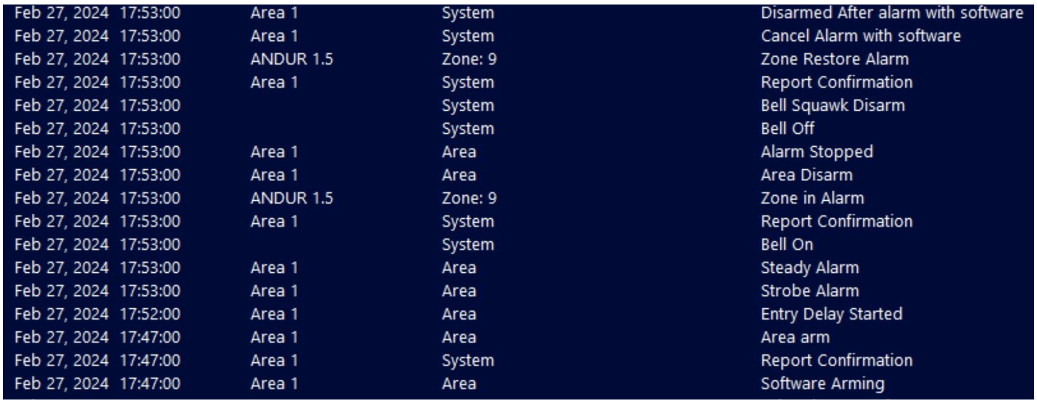
```
f5555554fcdb49b69249269b6d36da49348 [Pause: 662466 samples]
f5555554fcdb49b69249269b6d36da49348 [Pause: 545455 samples]
f5555554fcdb49b69249269b6d36da49348 [Pause: 401522 samples]
```

```
11110101010101010101010101010101001111110011011011010010011011011010010010010010010010011010011011011011010011011011011010010010010011010010 [Pause: 116711
samples]
```

Figure 11. Paradox PMD1P PIR alarm trigger signal example.

Signal bitstream:
1111010101010101010101010101010100111111001101101101001001101101101001001001
0010010010011010011011011011010011011011011010010010010011010010
Signal in HEX: f5555554fcdb49b69249269b6d36da49348

The signal is repeated several times to make sure that it will be received. As can be seen from upper Figure 11 – only one dataset of the triggering signal was extracted and it worked fine without repetition. This means that the system is willing to act on only one signal and does not need repetition of that signal. Repetition is generated as a safety measure from sensor side in case some signaling might be damaged by the noise on the same channel.



```
Feb 27, 2024  17:53:00   Area 1       System    Disarmed After alarm with software
Feb 27, 2024  17:53:00   Area 1       System    Cancel Alarm with software
Feb 27, 2024  17:53:00   ANDUR 1.5    Zone: 9   Zone Restore Alarm
Feb 27, 2024  17:53:00   Area 1       System    Report Confirmation
Feb 27, 2024  17:53:00                System    Bell Squawk Disarm
Feb 27, 2024  17:53:00                System    Bell Off
Feb 27, 2024  17:53:00   Area 1       Area      Alarm Stopped
Feb 27, 2024  17:53:00   Area 1       Area      Area Disarm
Feb 27, 2024  17:53:00   ANDUR 1.5    Zone: 9   Zone in Alarm
Feb 27, 2024  17:53:00   Area 1       System    Report Confirmation
Feb 27, 2024  17:53:00                System    Bell On
Feb 27, 2024  17:53:00   Area 1       Area      Steady Alarm
Feb 27, 2024  17:53:00   Area 1       Area      Strobe Alarm
Feb 27, 2024  17:52:00   Area 1       Area      Entry Delay Started
Feb 27, 2024  17:47:00   Area 1       Area      Area arm
Feb 27, 2024  17:47:00   Area 1       System    Report Confirmation
Feb 27, 2024  17:47:00   Area 1       Area      Software Arming
```

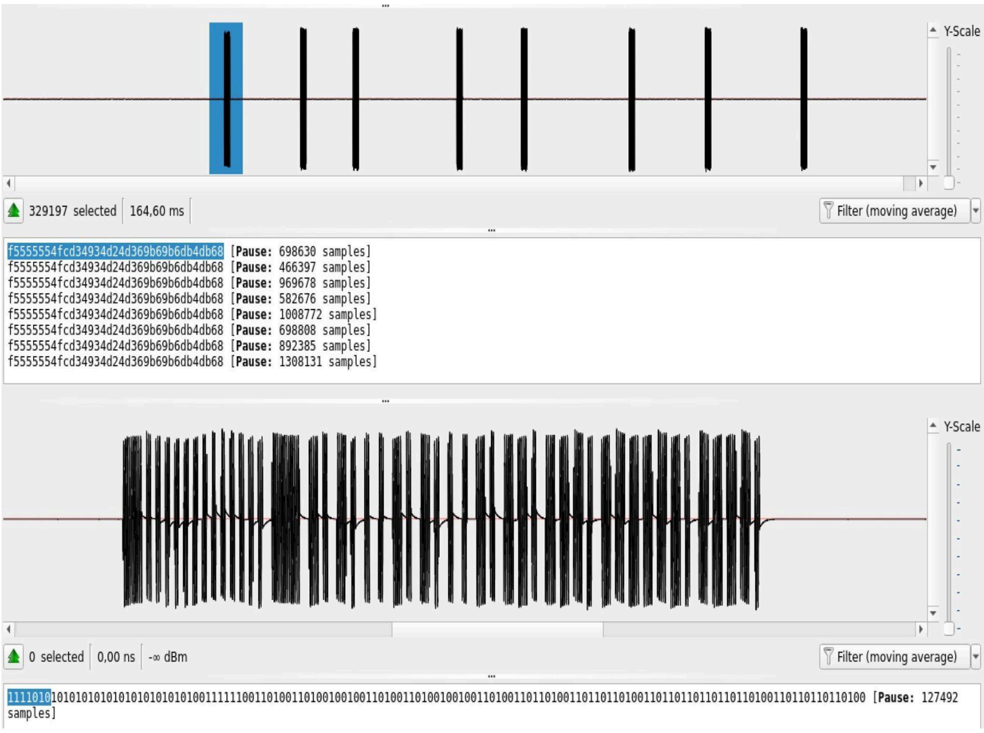
Figure 12. Replaying Paradox PIR triggering signals raises ordinary log messages.

Similar testing was conducted also with a second PIR and results were analogous – there was no problem to trigger false alarm as seen from Figure 12. With PIR it is possible that with every captured movement a signal is sent to the hub, but it is also possible that signals are not sent even if movement is detected. That is called "dead time" when after a triggering signal has been sent, a PIR will start a time counter and won't send any new triggering messages even if it detects another movement within this time window. It is configured to avoid several repeated movements in a row triggering too many excessive alarms. Also it helps wireless sensors to save battery. PMD1P PIR could be played with for about 5 minutes before it sent out another triggering message. It means that jamming can be briefer and with correct timing it would be also possible to avoid jamming detection by the hub. This needs more precise testing and is left out of scope of this thesis.

RF sensor health-check signaling is conducted in the Paradox MG5000 system after every 80 minutes or once in 24 hours. Test was not done as it is too long time for the URH collection. Also if getting to the sensor after jamming and shielding it by some cover then 80 minutes would be probably enough time for criminals to accomplish their doings. If it would be possible to jam signaling between PIR and the hub then there would be still a need to send OK messages to the hub after every 80 minutes to be sure that the hub does not generate a related "sensor lost" notification and send it to the user or service provider. It is important to recognize that this 80 minutes check-in time can be overridden in system software under Global System Options where wireless zones Presence Supervision can be simply disabled. This example shows that a lot depends on how the system is set up in the software. With poor setup it is possible to decrease the chances of effective reaction from the system.

4.1.1.2 Reed switch

Wireless reed switch DCTXP2 433MHz FW: V3.00 Production week 39/2012 SN: 0461XX was tested with MG5000 hub. Figure 13 shows that the reed switch also sends the same signal all the time.



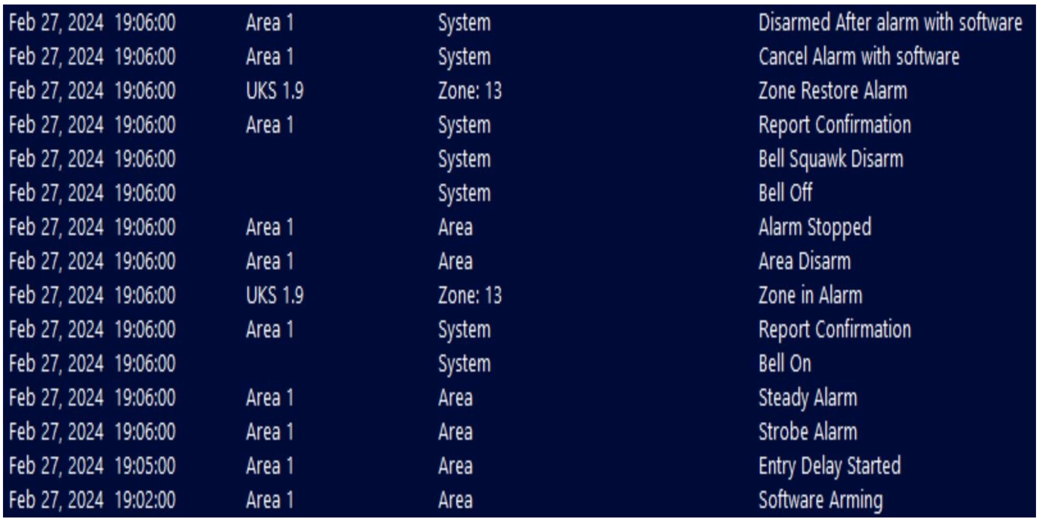
```
f5555554fcd34934d24d369b69b6db4db68 [Pause: 698630 samples]
f5555554fcd34934d24d369b69b6db4db68 [Pause: 466397 samples]
f5555554fcd34934d24d369b69b6db4db68 [Pause: 969678 samples]
f5555554fcd34934d24d369b69b6db4db68 [Pause: 582676 samples]
f5555554fcd34934d24d369b69b6db4db68 [Pause: 1008772 samples]
f5555554fcd34934d24d369b69b6db4db68 [Pause: 698808 samples]
f5555554fcd34934d24d369b69b6db4db68 [Pause: 892385 samples]
f5555554fcd34934d24d369b69b6db4db68 [Pause: 1308131 samples]
```

```
1111010101010101010101010101010100111111001101001101001001001101001101001001001101001101101001101101101001101101101101101101001101101101101100 [Pause: 127492
samples]
```

Figure 13. Paradox reed switch triggering signal.

Signal bitstream:
1111010101010101010101010101010100111111001101001101001001001101001101001001
001101001101101001101101101001101101101101101101001101101101101000
Signal in HEX: f5555554fcd34934d24d369b69b6db4db68

As with PIR it was not possible to test the health-check signals happening once over 80 minutes. But it is clear that triggering a false alarm is possible as seen in Figure 14 by a sensor named UKS 1.9.



```
Feb 27, 2024  19:06:00    Area 1     System       Disarmed After alarm with software
Feb 27, 2024  19:06:00    Area 1     System       Cancel Alarm with software
Feb 27, 2024  19:06:00    UKS 1.9    Zone: 13     Zone Restore Alarm
Feb 27, 2024  19:06:00    Area 1     System       Report Confirmation
Feb 27, 2024  19:06:00               System       Bell Squawk Disarm
Feb 27, 2024  19:06:00               System       Bell Off
Feb 27, 2024  19:06:00    Area 1     Area         Alarm Stopped
Feb 27, 2024  19:06:00    Area 1     Area         Area Disarm
Feb 27, 2024  19:06:00    UKS 1.9    Zone: 13     Zone in Alarm
Feb 27, 2024  19:06:00    Area 1     System       Report Confirmation
Feb 27, 2024  19:06:00               System       Bell On
Feb 27, 2024  19:06:00    Area 1     Area         Steady Alarm
Feb 27, 2024  19:06:00    Area 1     Area         Strobe Alarm
Feb 27, 2024  19:05:00    Area 1     Area         Entry Delay Started
Feb 27, 2024  19:02:00    Area 1     Area         Software Arming
```

Figure 14. Triggering false alarms with Paradox reed switch signal replay seems ordinary in logs.

Triggering false alarms can be positive for criminals as even if they cannot capture the “key“ to open and disarm system then if false alarms will be generated often and on non convenient times then people can drop using alarm system and also their readiness to react will change as they see alarm system as not trustworthy or reliable anymore.

4.1.1.3 Keyfob

Keyfobs were tested with the MG5000 hub in 2023, but as some uncertainty remained they were tested again after purchase of MG5050+ hub.

Keyfob 1: Paradox REM25 433MHz FW: V1.02 Production date: unknown SN: 0622XX
Keyfob 2: Paradox REM25 433MHz FW: V3.00 Production date: after 2019 SN: 2090XX

Keyfob 2 arm and disarm buttons were pushed while connected with MG5050+. Arm and disarm buttons were pushed for 10 times each and tried to analyse the results over URH by looking into signals in HEX format to discover similarities. From our captured signals it was possible to notice that similar info is transmitted with arming and disarming buttons being pushed. When replayed then disarming and arming signals for REM 25 worked, but not all the time. It needed more investigation to make it clear why keyfob disarming is not straightforward but seems occasionally random. Another keyfob was taken to see if the situation is the same. Keyfob 1 arming and disarming sequences with MG5050+:

Arming commands in HEX:

f5555554fcda4924d24936db6d26da69a68
f5555554fcda4924d24936db6d26da69a68
f5555554fcda4924d24936db6d26da69a68

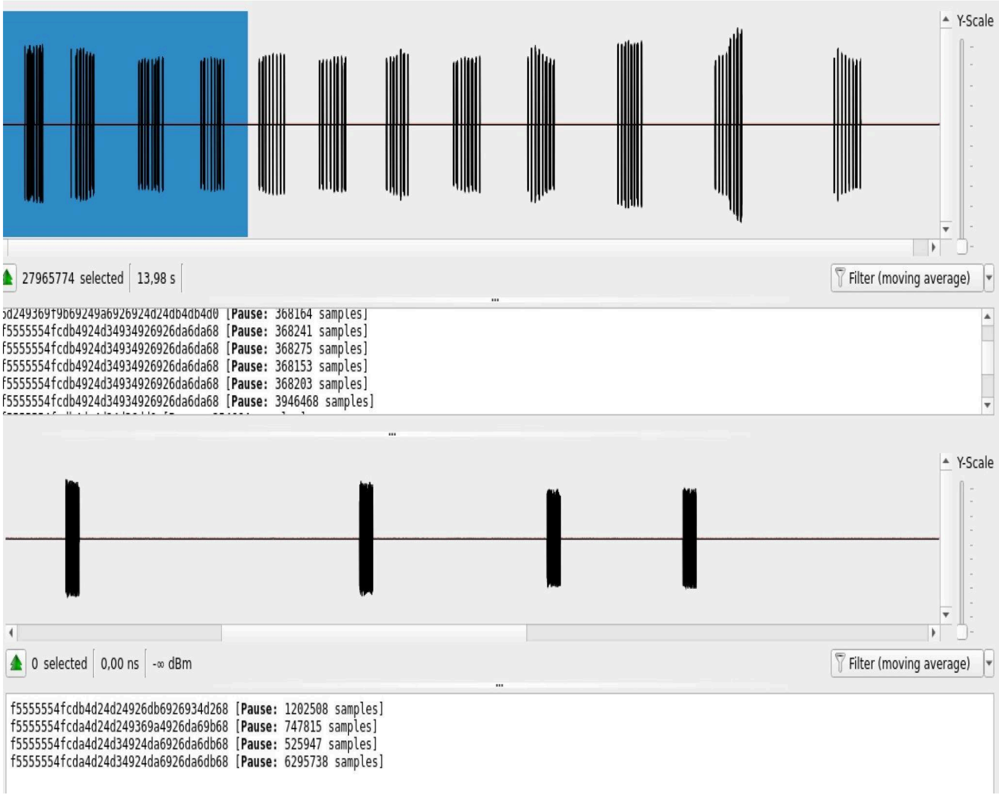
Disarming commands in HEX:

f5555554fcd34d**2**4da4**93**69b4926924d268
f5555554fcd34da4da4d26**d3**4926924d**a**68
f5555554fcd34da4da4d269b**6**926924d268

It is possible to notice that the arming signal seems to be the same all the time but the disarming signal is slightly different every time. It was possible to use a replay signal from the recording sequence from arming 1 but impossible to disarm it with disarming 1 or 2, but disarming 3 worked instantly on the first try. On the second try it was not possible to disarm the system with either of three disarming sequences.

A set of 12 disarming signals was then recorded in a row and the replay signal was left constantly running. At the same time tried to arm the system with the original keyfob but were not successful for over 20 minutes and over 50 tries. Even as the arming process sometimes had started “Exit delay” on the keypad screen, it could never finish it before the replay signal from URH and HackRF cancelled it out. After that, this chunk of data containing 12 disarming signals was analysed and tested with extracting different parts and signals inside. Finally the first 4 disarming signal chunks from that 12 chunk recording were taken and the result was the same. It was not possible to arm the system – it was disarmed every time before the exit delay was completed. 4 different datasets from these first four chunks illustrated in Figure 15, were separated and got following results for “Magic 4“ set of keyfob 1 signals in HEX:

f5555554fcd	b4	d24d	24	926d	b6	92	69	34	d2	68
f5555554fcd	a4	d24d	24	9369	a4	92	6d	a6	9b	68
f5555554fcd	a4	d24d	34	924d	a6	92	6d	a6	db	68
f5555554fcd	b4	da4d	24	d369	36	92	69	34	da	68



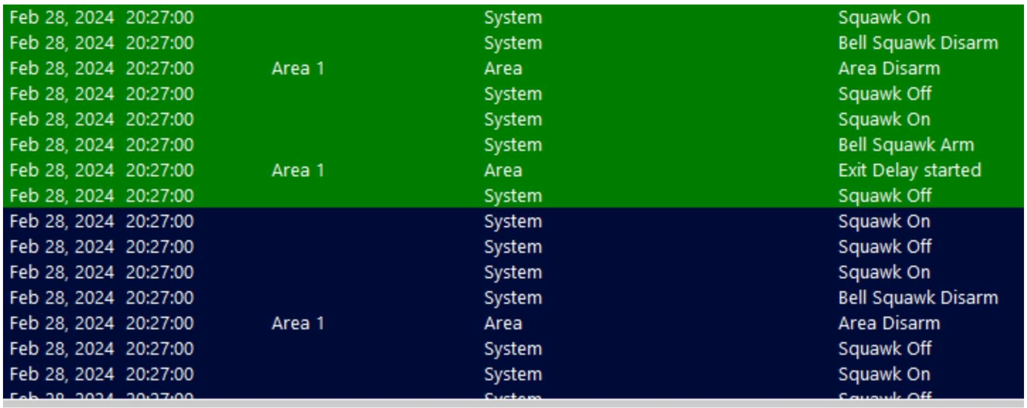
```
5d249369f9b69249a6926924d24db4db4d0 [Pause: 368164 samples]
f5555554fcdb4924d34934926926da6da68 [Pause: 368241 samples]
f5555554fcdb4924d34934926926da6da68 [Pause: 368275 samples]
f5555554fcdb4924d34934926926da6da68 [Pause: 368153 samples]
f5555554fcdb4924d34934926926da6da68 [Pause: 368203 samples]
f5555554fcdb4924d34934926926da6da68 [Pause: 3946468 samples]
```

```
f5555554fcdb4d24d24926db6926934d268 [Pause: 1202508 samples]
f5555554fcda4d24d249369a4926da69b68 [Pause: 747815 samples]
f5555554fcda4d24d34924da6926da6db68 [Pause: 525947 samples]
f5555554fcda4d24d34924da6926da6db68 [Pause: 6295738 samples]
```

Figure 15. Extracting “Magic 4“ datasets of Paradox keyfob 1.

Another test was conducted to verify results and once again everything worked perfectly. It did not matter if the MG5050+ hub was armed with keyfob 1 or by some other means, collected “Magic 4” was able to disarm the system at all times when replayed.

It was noticed that this disarming signal running in background did not alert any jamming alert even if it was constantly running. Figure 16 illustrates the log of that time.



```
Feb 28, 2024  20:27:00                  System              Squawk On
Feb 28, 2024  20:27:00                  System              Bell Squawk Disarm
Feb 28, 2024  20:27:00      Area 1      Area                Area Disarm
Feb 28, 2024  20:27:00                  System              Squawk Off
Feb 28, 2024  20:27:00                  System              Squawk On
Feb 28, 2024  20:27:00                  System              Bell Squawk Arm
Feb 28, 2024  20:27:00      Area 1      Area                Exit Delay started
Feb 28, 2024  20:27:00                  System              Squawk Off
Feb 28, 2024  20:27:00                  System              Squawk On
Feb 28, 2024  20:27:00                  System              Squawk Off
Feb 28, 2024  20:27:00                  System              Squawk On
Feb 28, 2024  20:27:00                  System              Bell Squawk Disarm
Feb 28, 2024  20:27:00      Area 1      Area                Area Disarm
Feb 28, 2024  20:27:00                  System              Squawk Off
Feb 28, 2024  20:27:00                  System              Squawk On
Feb 28, 2024  20:27:00                  System              Squawk Off
```

Figure 16. Unable to arm the system with Paradox keyfob 1 while our generated “Magic 4 disarmer” runs.

It is possible that all the other strange datasets or signals occurring between these 4 codes actually are deliberate to obfuscate the actual valuable dataset. This kind of activity could harden certain cloners work like for example Flipper Zero, but this needs verification in future works.

As keyfob 2 had been before troublesome as sometimes arming and disarming worked, it was tried the same thing to accomplish with keyfob 2 as was done with keyfob 1. After gathering HEX data from signals the “Magic 4“ datasets for keyfob 2 were following:

97aaaaaaa7e4924d34d34d369b49369a4da4
97aaaaaaa7e4926d34d34d34da49369a4da4
97aaaaaaa7e4d26d349b6d26d249349b49a4
97aaaaaaa7e49a4d34d34db69a49369a4d24

Results were analogous to keyfob 1. All replays for disarming now worked fine. Visual HEX was different but as keyfobs are from different eras and use different firmware it is not sure if changes are only related to keyfobs serial number or something else. And as collected signals work in sequence all with current keyfobs then it would be unnecessary to even think about brute forcing when a criminal mind simply needs to collect four button strokes. Deeper bit level analyze is left out of the scope.

4.1.1.4 Keypad

Two KL37 wireless keypads were tested with MG5000 hub and another new KL38 was tested with MG5050+ to see if there are any differences with newer devices.

Data collection description:

MG5000 was set up on premises together with HackRF and a laptop running URH and MG5000 settings were programmed accordingly so that wireless keypad number 1 would be in control and the system would react on code 0000.

Signals were recorded with URH while pushing keypad buttons to arm the system – it was waited until the system was fully armed and then used the same code to disarm the system. After that same recording was replayed once consisting of arming and disarming signaling and it was noticed some LED’s on the hub were flashing quickly. At first it was thought not to be connected to our replay and it was tried again to see if there is a connected reaction. This time infinite sending was chosen to replay signals and LEDs were starting to flash again as an indication of communication. Unexpected was that during that infinite replay from time to time the wired keypad was waking up and squawking. In closer look it was seen that asterisks were shown on the screen before squawks and after it. It meant that our recorded signals were actively interacting with the system and seemingly arming and disarming the system but as signals were recorded just one after another and replay was quickly repeating itself, the system had trouble reacting that quickly and was not able to always complete arming and disarming. After noticing that, several seconds of free space was added between arming and disarming signals and in the end the system was constantly arming and disarming itself just by signal received from HackRF. This quick replay attack with effective return gave us more motivation to take a closer look what is actually happening.

URH automatically determines the modulation scheme as ASK also for the keypad. Following is an example of the signaling happening between the MG5000 hub and wireless keypad KL37:

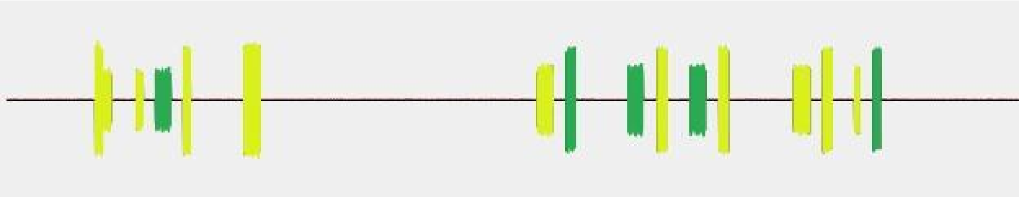


Figure 17. URH cannot determine real assignment of the signals.

As seen from Figure 17 - URH was not able to automatically determine correct belonging of signals to the hub or keypad. All recorded sets needed manual regrouping of the communication parties named Bob and Alice to get a normal overview together with correct association. Following is an example of signals captured and viewed in HEX format (for simpler overview) and assigned A and B for BOB and ALICE. Our testing was arranged in a way where A as Alice was corresponding to the wireless keypad or keyfob and B as Bob was corresponding to the alarm system hub. It is known that the keypad is used to send out the code and focus was on the messages sent by Alice and marked with a letter “A”. Number in front of letters A and B is describing the message number within the two-way communication.

In following part a typical beginning of an arming session with code 0000 between wireless keypad (A- as Alice) and MG5000 hub (B - as Bob) is presented in HEX format where at least some similarities are tried to mark with different colouring to illustrate data repetitions:

1A 53f36aaaaaa9f9b4d36924da49a49a69369b490

2B **f5555554fcd**26934926924db4db69b4d248

3B db69b5a69a6db4d**b6db6d**26db6da6d249248

4A 553f369b4d246da69369a69a49a69

5B **f5555554fcd**b**6d349**26d249b6d24da6da6db4d

6A **f5555554fcd**a**6d349**1b69a4da68d34934d2

7A **f5555554fcd**a6934926d269a6d24d**b6db6d**36d24d34da4d36db6d24d348

8B **f5555554fcd**26934926924db4db69b4d248

Real session did not end at 8B, but ended with 33A as can be seen in Appendix III. After collecting HEX data of messaging it was possible to see that different parts of signaling contained similar parts. As this arming signaling was containing all signals sent between keypad and hub it was noticed that actual code was being inserted with asterisks on wired keypad in the first part of this signaling. Actual code transmission part was tried to locate by separating different parts of the signaling and testing their functioning by seeing or not seeing asterisks on the wired keypad screen. In the end it was determined that the actual code transmission was contained in only one message. On the upper Alice&BoB HEX example it is 7A and that actual code transmission is followed by other 26 messages. Tests were conducted with different signal samples and it was verified that taking messages before and after the 7A were not functional for arming or disarming the system. Only one message sent from the keypad included all the information that was necessary to arm or disarm the system. If messages before or after the coded message were tried then arming or disarming the system never succeeded – it did not matter if these messages were tried one by one or all together. When only the message consisting of the code was removed from the stream it could be seen that MG5000 hub RX and TX LED's were blinking rapidly meaning that communication was initiated but the system was not armed or disarmed. There was no repetition of the 7A message including the code noted in the same format later or before. Some similar parts of the 7A message can be found also on before and later messages sent by keypad but some parts are only noticed in MG5000 hub messages. So it seemed that there was a built-in function to verify different parts of the code in two-way interaction but only one message consisting of correct code was responsible for real triggering of the action. If that one message containing code was replayed separately then the system was armed and also disarmed with the same message without problems. If that message containing actual code was tried to break into smaller pieces then arming and disarming was not functional anymore. It is unknown if that actual code number was represented only in that one message or also transmitted in others as verification or backup, but only one message was containing the actual arming and disarming altogether functional key, and its transmission time overlaps with the asterisks occurring on keypad screens.

Similar two-way communication was observed and analysed for several arming and disarming actions with code 0000. All the similarities were taken into account and while looking only at disarming signals it was noticed that some parts of the signals especially in the first part of the message are similar with each other.It was assumed that this was the part where the actual code was sent to the main unit and it was decided to extract accordingly log4 – 8A; log6 – 7A and log8 6A messages from the whole recorded disarm signals and test them individually. All of the extracted single messages could perfectly arm and disarm the main station unit. After that, the HEX format of disarming signals was captured using URH analyse window:

```
Log4:  8A: f5555554fcda6934926d269a6d24db6db6d36d24d34da        269b6db69269a2
Log6:  7A: f5555554fcda6934926d269a6d24db6db6d36d24d34da        4d36db6d24d342
Log8:  6A: f5555554fcda6934926d269a6d24db6db6d36d24d34da        4d36db6d24d342
```

After extracting upper signals and sending them without any other parts, the hub reacted just like nothing had ever happened. No other indication was detected and the system went into armed state and also properly disarmed with only the extracted signal part. It can be seen that disarming message containing code information is the same for Log6 and Log8, but it is different for Log4. Only the first part is the same but the end is different. It was assumed that this different end part is some kind of checksum code or something similar, and thought that maybe it is not relevant as both codes singlehandedly could arm and disarm the main station unit. It was tried to send out only the first part of that message with HackRF to see if the last part of the message matters or not to the hub. Last 18 chunks of data from Log8 A6 message was separated and verified it in URH analyze window to have only first part of the signal in HEX value as: f5555554fcda6934926d269a6d24db6db6d36d24d34da. Then tried to send it with HackRF several times but without result. It is clear that the last part of the message still holds an important role for the hub to accept the signals sent from the keypad. Also only the last 18 chunks of Log8 6A message were sent out with HackRF but no reaction.

After not getting any indication from separating the Log8 6A message parts it was clear that it needs more analyze from different disarm messages than only three. Now when knowing on which part the actual code was hidden inside the communication it was possible to estimate the final correct position by visual means over URH as the length or wideness of the code differs usually from other message parts sent by wireless keypad. Figure 18 shows that the message with the code is visually a bit wider than others.

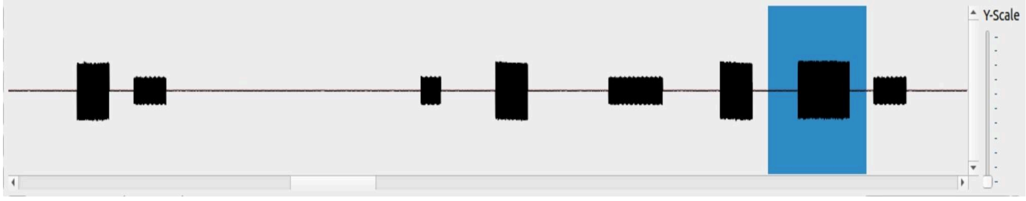


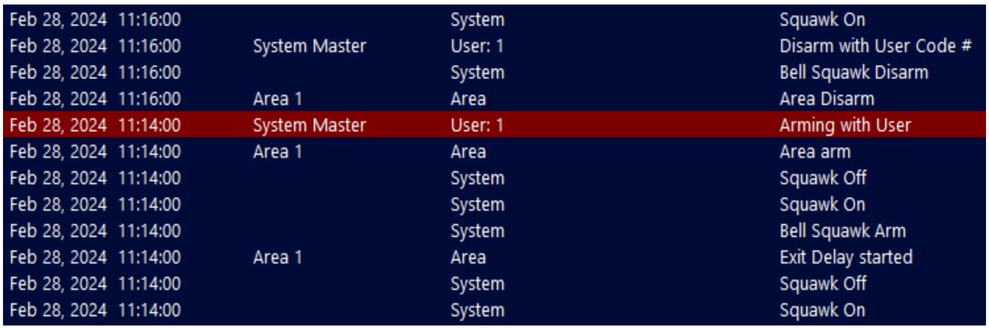
Figure 18. Message responsible for triggering Paradox arming or disarming functions differ visually.

More than 30 arming and disarming signaling sets were recorded and from that dataset it was possible to see that the actual position of the functional message is changing inside the signal: 1A; 5A; 6A; 7A; 8A - and there are also differences between arming and disarming messages. More detailed overview of the analyze is given in Appendix III. Nevertheless these differences probably only carry command status notification information and the system itself is not caring about the change and is tolerating triggering with both ways. Even though similarities can be seen with arming and disarming messages that actually carry function to trigger activity, it was verified during deeper testing, with different system components having different serials and using different master codes for arming and disarming, that bitstream inside that one functional message is most of the time changing within 21 bits but place of the bits may vary and overlap and is not fully predetermined with manual analyse means when arming code is changed within all four symbols. Using machine learning is seen as a measure to conduct a more precise analyze in future to determine the effective bit level position of the code itself and possibility to extract the real inserted numbers..

MG5050+

Similar testing was conducted with the newly purchased keypad KL38 and hub MG5050+ which are the newest Paradox wireless devices available at this time. The results were comparable to MG5000 and KL37. Giving in general the same result with MG5050+ accepting replayed signals originally sent from KL38. URH gave logical feedback again with ASK chosen as a modulation.

All actions were observed also within connected computer software Babyware. It can be seen from the system log that there was no difference for the hub if a signal was sent from the actual original keypad KL38 or with URH and HackRF. Neither the system cared about receiving all the other messages – if only one message, carrying code 0000, was separated and sent without other signaling parts, then the system was still effectively armed and disarmed. Similarly to MG5000, there was no difference between arming and disarming signal with keypad replay. The same message from disarm signaling could also arm the system without any problems.



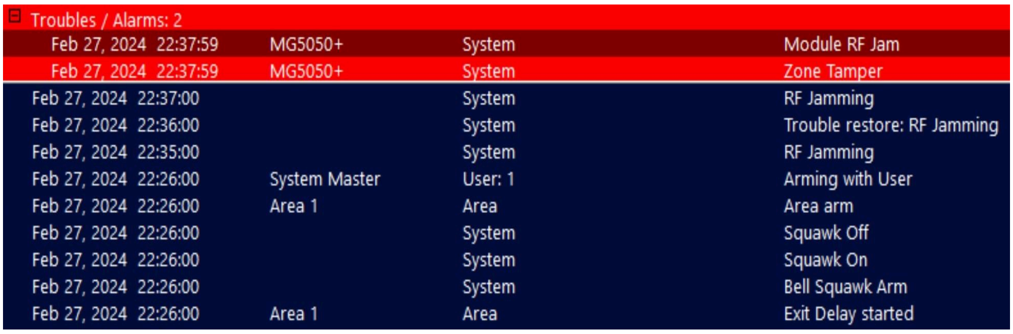
```
Feb 28, 2024  11:16:00                     System         Squawk On
Feb 28, 2024  11:16:00  System Master      User: 1        Disarm with User Code #
Feb 28, 2024  11:16:00                     System         Bell Squawk Disarm
Feb 28, 2024  11:16:00  Area 1             Area           Area Disarm
Feb 28, 2024  11:14:00  System Master      User: 1        Arming with User
Feb 28, 2024  11:14:00  Area 1             Area           Area arm
Feb 28, 2024  11:14:00                     System         Squawk Off
Feb 28, 2024  11:14:00                     System         Squawk On
Feb 28, 2024  11:14:00                     System         Bell Squawk Arm
Feb 28, 2024  11:14:00  Area 1             Area           Exit Delay started
Feb 28, 2024  11:14:00                     System         Squawk Off
Feb 28, 2024  11:14:00                     System         Squawk On
```

Figure 19. Replayed signal feedback in Babyware log window.

In Figure 19 it can be seen that replayed signal indicated exactly the same result in system log file as System Master “Arming with User” and “Disarm with user Code #” messages were written in log during replays as it was also when using the original KL38 keypad to arm and disarm the system. Different code sets were recorded and tested. For example : 0001; 1111;1234; 5678; 8899 etc. There was no difference with organising replay attacks while code was changed – it still worked. Dataset of several gigabytes URH recorded signals were collected from used different codes to save for the future works.

4.1.2 Interference testing

Within the hub software there is a place where it was possible to mark with a tick in a box “GSM RF Jamming Supervision” - it should activate jamming monitoring. With the MG5000 hub any indication of conducted disturbance was not noticed while the reed switch and PIR disturbance was tested. With MG5050+ it was possible to immediately notice RF jamming trouble activation like in Figure 20, when trying to replay an arming or disarming signal with poor recording quality.



```
⊟ Troubles / Alarms: 2
    Feb 27, 2024  22:37:59  MG5050+        System         Module RF Jam
    Feb 27, 2024  22:37:59  MG5050+        System         Zone Tamper
  Feb 27, 2024  22:37:00                   System         RF Jamming
  Feb 27, 2024  22:36:00                   System         Trouble restore: RF Jamming
  Feb 27, 2024  22:35:00                   System         RF Jamming
  Feb 27, 2024  22:26:00  System Master    User: 1        Arming with User
  Feb 27, 2024  22:26:00  Area 1           Area           Area arm
  Feb 27, 2024  22:26:00                   System         Squawk Off
  Feb 27, 2024  22:26:00                   System         Squawk On
  Feb 27, 2024  22:26:00                   System         Bell Squawk Arm
  Feb 27, 2024  22:26:00  Area 1           Area           Exit Delay started
```

Figure 20. Paradox MG5050+ hub can detect RF jamming.

This kind of indication of detection of jamming was never seen with the MG5000 hub. It is possible that older MG5000 hub is only actively monitoring the GSM frequency band and reacts only when the active notification channel is jammed - it is unknown. MG5050+ hub did not have any “GSM RF Jamming Supervision” tick box in this Reporting window within Babyware software that was configurable with MG5000. But instead “RF Jamming Supervision” was found under the “Areas Supervision” tab, where it was separated as Wireless options. Any GSM or LTE related Jamming option was not found.

Reed Switch and PIR interference testing

Problem with wireless reed switches in the Paradox case is that they will only send their trigger status within a few seconds and only when status changes. If those 2 seconds are effectively jammed by an attacker then no indication of status change will be notified to the hub and no alarm will be triggered. Placing the magnet back close to the switch is not going to trigger another alarm.

As our test set was not attached to any door or window, the sensor was just moved further away from the hub and if the switch was opened then no alarm was triggered. For effective interference testing a position, where removing the magnet still triggered the alarm, was marked and then tested the system with having HackRF close to the hub transmitting noise. It was possible to see that removing the magnet now did not trigger the alarm. This gives us proof that a simple SDR and GNU Radio program can generate a possible interference signal that can be effective to suppress original signals coming from wireless sensors and detectors. As always it is a question of power and sensitivity - SNR level.

PIR disturbance reaction testing was conducted in a similar way as reed switch and results were analogue. In both cases there was no indication of jamming in the wired keypad or within the software log window or at the sensor panel when the test was conducted with the MG5000 hub. With MG5050+ hub, the “Module RF Jam” message - seen on upper Figure 20, was quickest detected by control software log about 23-25 seconds after the GNU Radio program was activated. If the KL38 keypad was constantly asked for status information by pushing the “i” (information) -button for information then it was indicating trouble about 10 seconds after starting the interference. This might give enough time for an attacker to jam the reed switch - open and close the door or jam PIR signal, enter premises and shield/cover it and disable the jamming before the system detects that something is wrong. Of course one then needs to know exactly which system capabilities are used as protective measures.

Keyfob interference testing

Keyfob disturbance was not tested especially but we note that if we kept our discovered dataset of “Magic 4” signals from replay attack running in background then it was not possible to use keyfob REM25 effectively. In that case it was not possible to arm the system. But as mentioned before, usually criminals already having an “opening key” do not need to play with blocking signals. Nevertheless it is physics, if a generated interference signals received by the hub initiate a situation where SNR for the original keyfob signal is dropped under acceptable level- then keyfobs do not work. Of course it is a SNR fight and in case the keyfob is close to the receiver then interference signal power from distance needs to be big. In our case without having any extra antennas and amplifiers and being held back by legislation this kind of situation was not tested but if possible it will be tested in future works to bring clarity about actual effective distances where from criminals can work to stay unnoticed.

Keypad interference testing

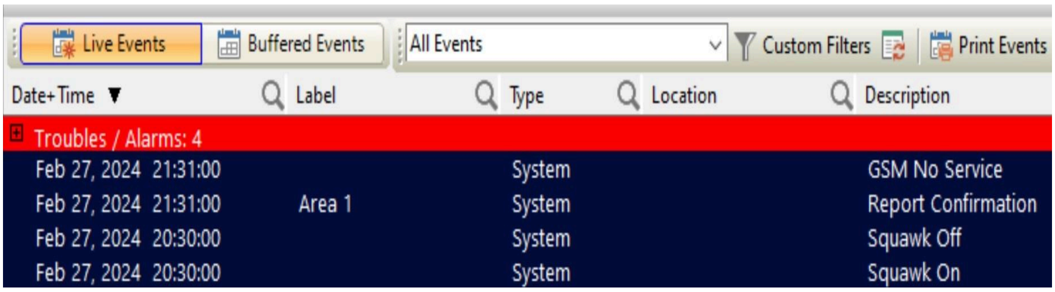
Disturbance reaction was also tested against keypad KL38 and it was noticed that it had no indication of jamming while the system was unarmed. If the interference signal was transmitted and the “i” button was constantly pushed to see new information about status, then about 10 seconds after starting the interference, trouble was indicated. It was not possible to arm the system while trouble was active and it was not possible to clear that trouble while the interfering signal was active. Nevertheless even if the system shows trouble, it can be configured in the software in a way to be able to bypass the trouble, and still arm the system. Keypad never indicated directly that this trouble was jamming. System indicated that “Zone 9” has a problem and if that was looked closer then “STAY” was active and “TROUBLE” and “ARM” notifications were blinking on the keypad screen.When the system was in an armed state and the disturbance was turned on, then not a single alarm trigger was generated and interference was unnoticed.

General RF band interference testing

Flooding the whole band at 433MHz with an interfering signal was not necessary as specific frequencies used by system peripherals were not detected and the system did not use any frequency hopping or other channels for wireless traffic. Only a narrow channel at approximately 433,93MHz was used. This kind of approach makes it quite easy for the attacker to jam the system traffic. There was no difference between the older MG5000 and new MG5050+ system nor newer keypad or keyfob frequency use. MG5050+ was able to detect jamming but MG5000 did not react to it.

Notification channel

Paradox MG5000 and MG5050+ do not have built-in Wi-Fi and the main notification channel is over mobile networks. It is also possible to connect a system to the IP network over a special module, but our system did not contain this opportunity. Jamming was emulated by simply shielding and taking away reception from the GSM modem. Just removing the antenna raised the “No GSM Service” message in the software log seen in Figure 21, and the wired keypad was notified of trouble with connection.



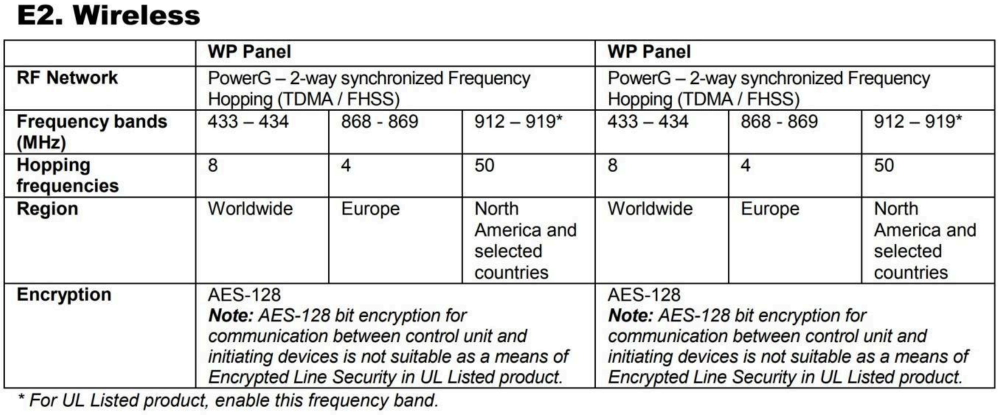
Date+Time ▼	Label	Type	Location	Description
⊞ Troubles / Alarms: 4				
Feb 27, 2024 21:31:00		System		GSM No Service
Feb 27, 2024 21:31:00	Area 1	System		Report Confirmation
Feb 27, 2024 20:30:00		System		Squawk Off
Feb 27, 2024 20:30:00		System		Squawk On

Figure 21. Paradox “GSM No Service” indication within control software.

Getting notification about different troubles is possible to set up in control software, but it raises a general question- how is that trouble going to be notified to the user if trouble itself is with the notification channel? So there can be a local notification of trouble, but if the owner is away from home or burglars are going to jam mobile connections during night time when the shop is closed, then no notification is going to be sent out from the jammed system.

4.2 DSC WP8010-K-FR

The DSC system is made in Israel. Keypad manual section “E.2 Wireless” shown in Figure 22 states that AES-128 is used and wireless PowerG devices two-way communication function have not been tested to comply with certification requirement standards and should be considered left out of scope bearing standardisation in mind. PowerG devices including keyfobs are using encryption. System also uses 4 different frequencies to send out messages. There was no RFID tag or smart/chip card available in our system.



E2. Wireless

	WP Panel			WP Panel		
RF Network	PowerG – 2-way synchronized Frequency Hopping (TDMA / FHSS)			PowerG – 2-way synchronized Frequency Hopping (TDMA / FHSS)		
Frequency bands (MHz)	433 – 434	868 - 869	912 – 919*	433 – 434	868 - 869	912 – 919*
Hopping frequencies	8	4	50	8	4	50
Region	Worldwide	Europe	North America and selected countries	Worldwide	Europe	North America and selected countries
Encryption	AES-128 ***Note:*** *AES-128 bit encryption for communication between control unit and initiating devices is not suitable as a means of Encrypted Line Security in UL Listed product.*			AES-128 ***Note:*** *AES-128 bit encryption for communication between control unit and initiating devices is not suitable as a means of Encrypted Line Security in UL Listed product.*		

** For UL Listed product, enable this frequency band.*

Figure 22. DSC WP8010 user manual page 69 claims to use AES-128 encryption scheme.

Frequency channels used by our unit were approximately 140 kHz wide and using centre frequencies approximately: 868,210MHz; 868,410MHz; 868,865MHz; 869,065MHz. Spectral layout is given in Figure 23. In the user manual it is presented that system uses 4 hopping frequencies between 868-869MHz. It was tried to distinguish between the hops and understand which hop belongs to a certain signal or bitstream inside the message, but that was not successful.

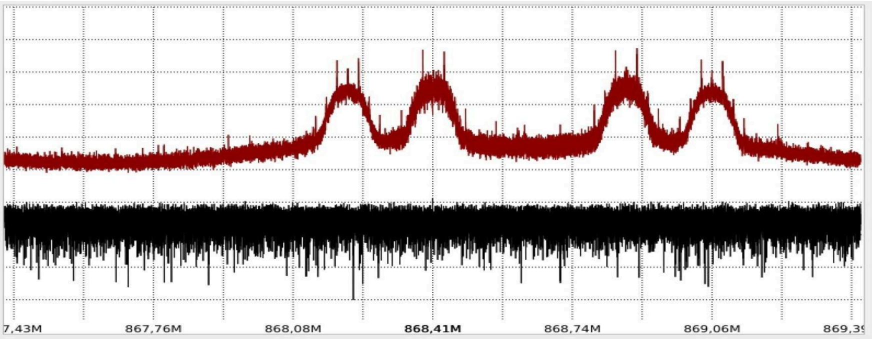


Figure 23. URH screenshot of DSC system using different frequencies.

It might need better radio analysing capability or at least two HackRF radios at the same time. One to capture signals frequencies in time and other to capture the consisting messaging part at the same exact time. While following the usage of frequencies during arming and disarming procedure, it was possible to detect that frequencies were randomly chosen and not in any logical order.

For example some random detected frequency usage sets one after other (in MHz):

Disarming	868,410; 869,065
Arming:	868,410; 869,065
Disarming:	868,865; 868,410
Arming:	869,065; 868,865; 868,210
Disarming:	868,865; 868,410
Arming:	869,065; 868,410
Disarming:	868,210; 868,410
Arming:	868,410; 868,210; 869,065

On some occasions it seemed that some signals occurred almost at the same time and usually the last part was up in the air after the code had been sent and the system was already in arming state. While arming and disarming with the keyfob it was noticed that most of the time frequency 868,410MHz was used by the hub to provide feedback. Only on rare occasions, approximately once per 8 to10 use, the same frequency was used by the keyfob itself to send out the signal.

At first it was thought that for the system it does not matter which frequency is used and it will accept signals on any frequency as long as the signal has correct data and hopping is only designed to provide better quality and redundancy. There might be an algorithm to decide which pattern is used to send out messages on different frequencies. Also on some occasions, once per 3 to 5 use, it was noticed that several frequencies were used by keyfob or keypad on the same session time. Even more rare occasions, once per 15 uses, it was noticed that the same frequencies were used at the same session time – signals concurrently in spectral view. After analysing signals in HEX format it was assumed that in these occasions the same message part is redundantly provided on both frequencies. Otherwise the usage of the frequencies seems to be random – sometimes same frequency is used for arming and disarming and sometimes different frequency is used and hopping seems to be without a certain pattern that was not possible to determine with more than 30 sessions.

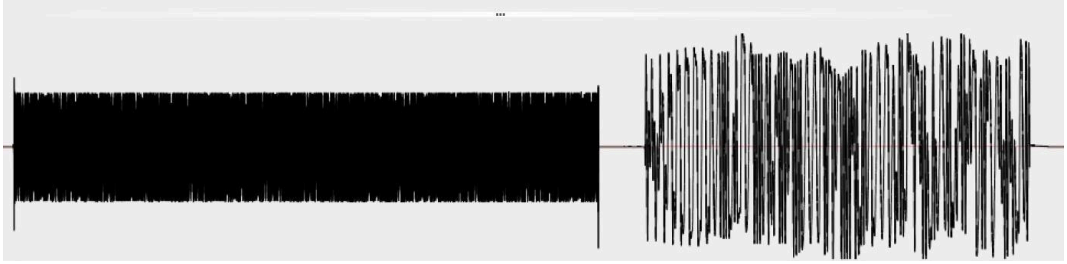


Figure 24. DSC differences in signal message format within one arming process.

As can be seen from the upper Figure 24 that different message parts within one procedure can be with different parameters. This picture is artificial as some empty space between these two signals was deleted but it is taken from DSC arming with keypad code 1111 try6 sample file. Similar effect with some different signal/message format included inside the same signal part could be noticed on all recorded samples. It might be that the system uses different modulation or coding techniques on different frequencies it uses. It can also be possible that the system uses this randomly instead of a specific algorithm but as our scope was to test simple replay attacks, deep analyze is kept out of scope. Nevertheless our notices during conducted tests are provided.

Testing process:

As already having some experience with the Paradox system, the DSC system was assembled together and programmed to work like in everyday life. At first it was observed how the system reacts on different cases and as it was seen that everything works as it should, focused on communication between the hub and keyfob and also on between keypad and hub later on. The Reed switch and PIR sensor were disabled to avoid extra noise while over 30 arming and disarming processes signaling from keyfob and about 10 from the keypad were collected. Keyfob was providing feedback with LED lights and sound when command was received by the hub: red, green and blue LEDs were used. On command not reached – only red light was lit.

4.2.1 Replay attack

4.2.1.1 Keyfob

30 keyfob disarming signal samples were collected with URH and their HEX outcome analysed. With every push several different signals were sent to the hub - usually containing 4 or 5 datasets . Following is an example how signals in sessions 15) and 27) and 13) and 26) contained similar dataset and only small part of the signal was actually with changed data:

15)	d55555550f9a8f9af77009b3	c6	e	59a520803f5	89	b64be2b955be	88f10
27)	d55555550f9a8f9af77009b3	d6	e	59a520803f5	86	b64be2b955be	d7108
13)	d55555550f9a8f9af77009b3	f6	e	59a52785d4a	6d	f84bedb955be	e3980
26)	d55555550f9a8f9af77009b3	ee	e	59a52785d4a	70	f84bedb955be	e7500

Only 9 HEX symbols between signal 15) and 27) and between 13) and 26) change:

15)	**c6 89 88f10**	13)	**f6 6d e3980**
27)	**d6 86 d7108**	26)	**ee 70 e7500**

Many signals were very similar to each other and contained only small changing parts. When taking a closer look to the sessions it was noticed that different similar signals what were colour coded seemed to correlate:

2)	d55555550f9a8f9af77009b3	ce	e59a5 2259647	1a	774be9b955be
2)	d55555550f9a8f9af77009b3	ce	e59a5 26a194b	ac	ad4be3b955be861c0
2)	d55555550f9a8f9af77009b3	ce	e59a5 21bb67a	a8	f0cbe0b955beb0398
11)	d55555550f9a8f9af77009b3	c6	e59a5 2259647	6c	77c9e9 b955bef3538
11)	d55555550f9a8f9af77009b3	c6	e59a5 255de07	e5	c5a5f7 5caadf 4168c
11)	d55555450f9a8f9af77009b3	c6	e59a5 26a194b	da	adcbe3 b955be83758
11)	d55555550f9a8f9af77009b3	c6	e59a5 21bb67a	de	f04be0 b955beb5100
28)	d55555550f9a8f9af77009b3	c6	e59a5 2259647	7c	77cbe9 b955bea2520
28)	d55555550f9a8f9af77009b3	c6	e59a5 26a194b	ca	adcbe3 b955bed2740
29)	d55555550f9a8f9af77009b3	ce	e59a5 2259647	7f	77cbe9 b955bee96b8
29)	d55555550f9a8f9af77009b3	ce	e59a5 26a194b	c9	adcbe3 b955be994d8

It is possible to notice from sessions 2); 11); 28); 29) that colour codes seem to be in order. Blue line always comes after pink. Some other similarities in other messages given in Appendix IV were also noticed. From this result it is hard to make final conclusions. It is seen that the keyfob sends several signals during one session. These signals might be with different frequencies and as it is two-way communication then all signals also get an answer. In the upper table it is only keyfob side signals because the hub was taken far away from HackRF and was shielded so it barely received the keyfob signal. From time to time it also occurred during testing that the keyfob could not receive an answer. In that case the keyfob light turned red and there was no feedback of positive transmission. As from session 11) it is possible to distinguish between 4 different colours, it might hint us the different frequency usage and also different messages travelling between the hub and keyfob.

From this in total it is possible to see that even though the system claims to use AES-128 bit encryption at least some parts of the signal sent out by keyfob can be derived using URH in FSK modulation and representing signals in HEX format show certain similarity. That can be used to further analyse the communication and after getting familiar with layout it might be at least possible to save time in brute force attack design. At the moment this is not our main focus, but results allow us to estimate that it is feasible to generate an effective tool for this kind of attack if in certain cases only 9 HEX values are changed. Extra 30 samples of arming and disarming with hub and keyfob together and 10 samples of hub and keypad communication was collected for future works. After collection was complete it was tried to replay different disarming signals on the armed hub but without any result or any indication. It was tried to send disarming signals on different detected frequencies but only one frequency at a time because only one HackRF was used. No positive feedback from replay attack was achieved.

4.2.1.2 Keypad

None of the keypad replay attacks worked similarly to keyfob. As the system uses two frequencies at near time to arm or disarm then it can also be a reason behind replays not working with a single frequency transmitter. Example is given on DSC arming with code 1111 in HEX as signal 6 out of 11 different ones in "try7" session:

d55555550f9a8f9af5700bb3dea501bb47d95d74984c838e3a6545c1f5868f5f8

Several different codes and signal sets were tested but without any positive results. As "d5555555" prefix was familiar already from keyfob signal analyze it is possible that actual code is forwarded during this signal transmission, but deeper analyze is kept out of scope of this thesis.

4.2.2 Interference testing

No interference was detected by the system during testing of the DSC system. At the same time the keyfob was blocked and same situation with PIR and keyfob signals. General RF channel jamming detection was not noticed. Reaction to notification channel disturbance was not tested as the system only used licensed bands.

4.3 Jablotron JA-63

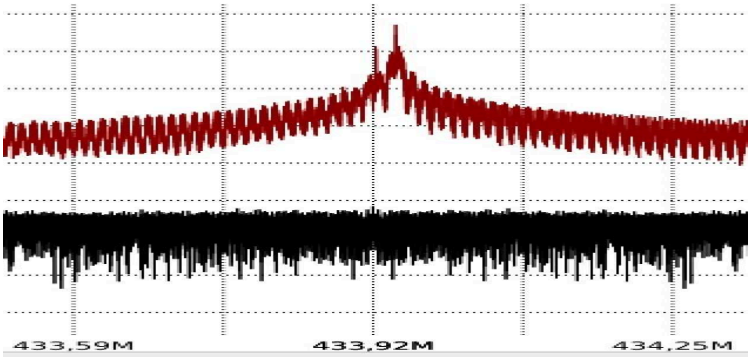


Figure 25. Jablotron frequency use on two close channels.

There were two different channels for the hub and keypad which were quite close and overlapping in close range seen in Figure 25. At first it was thought that the system itself would be able to separate them efficiently if really narrowband signaling would be used. In closer looking the difference is only 20kHz and in the current case it was not noted that frequency change from 433,93MHz to 433,95MHz would have any effect. Similar small jumps in frequency use were also noted with PIR. There was no RFID tag or smart/chip card available in our system and also the reed switch was absent.

4.3.1 Replay attack

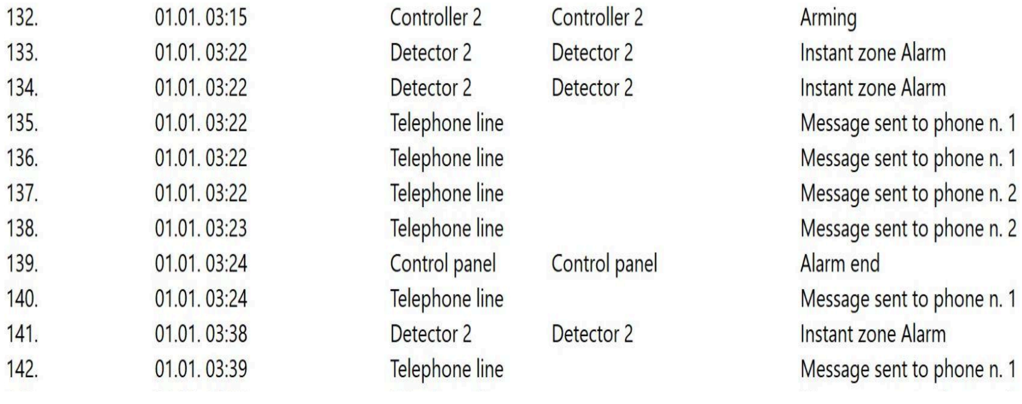
4.3.1.1 PIR

Several signals were recorded with HackRF in URH and noticed that not all of the signals were giving positive feedback all the time. As signals themselves were with totally random HEX dataset, testing was almost abandoned; it was not understandable why the same sequence once works and then again not.

Jablotron "PIR trigger 1" signal dataset in HEX:

```
002b354d35354b2b52ccaad53334aacd4b3359aa69a9aa595a966556a999a5566a599acd534
d4d52cad4b32ab54ccd2ab352ccd66a9a6a6a9656a59955aa6669559a9666
```

With that signal at least during some time it was possible to actively trigger false alarms. It was discovered that while the system was under armed state then about after every 15 minutes it reacted on that motion trigger signal. The hub itself activates a sleep mode after the alarm has been triggered. During that time one could easily walk in front of the motion sensor without any new triggers raising an alarm. That 15 minute pattern was discovered by leaving a PIR triggering signal just looping in URH and then looking at later software log output together with SMS'es received. For getting a clearer picture a second PIR was brought into the play. While starting a second PIR it was noticed that there is a small switch block inside the PIR which states if PIR is working in standard or higher sensitivity mode and if it is working on instant or delay mode. Both ways were tested and it could be seen that PIR working in delay mode looked dead for the next 15 minutes and did not react to any movement. Both PIR sensors were actively sending movement status to the hub while the alarm was active but after the hub ended the active alarm both PIRs were shut down for the next 15 minutes as shown in Figure 26. In general it means that the delay function can avoid criminals to leave some movement logs but what is worse is that while the hub is ending the alarm cycle it will send out that "be dead" or sleep order to PIRs. Timing correlation between logs seen in software and sensors acting in real life confirm it. That gives us another replay attack vector to investigate. It must be noted that the hub handles one sensor at a time meaning that if the sensor generated an alarm then sleep order would be sent only to that sensor which raised an alarm - other sensors will be still first served and active to react. Even though it is a really interesting vector it is left for future works.



```
132.   01.01. 03:15   Controller 2     Controller 2    Arming
133.   01.01. 03:22   Detector 2       Detector 2      Instant zone Alarm
134.   01.01. 03:22   Detector 2       Detector 2      Instant zone Alarm
135.   01.01. 03:22   Telephone line                   Message sent to phone n. 1
136.   01.01. 03:22   Telephone line                   Message sent to phone n. 1
137.   01.01. 03:22   Telephone line                   Message sent to phone n. 2
138.   01.01. 03:23   Telephone line                   Message sent to phone n. 2
139.   01.01. 03:24   Control panel    Control panel   Alarm end
140.   01.01. 03:24   Telephone line                   Message sent to phone n. 1
141.   01.01. 03:38   Detector 2       Detector 2      Instant zone Alarm
142.   01.01. 03:39   Telephone line                   Message sent to phone n. 1
```

Figure 26. Jablotron sleep mode for about 15 minutes since the last alarm triggered from the same sensor.

Several PIR motion signals and also a tamper signal was recorded. After analysing the dataset in HEX format it was seen that none of the signals visually contained exactly the same information but all of the signals were usable as a replay for creating a false alarm.

4.3.1.2 Keyfob

Keyfob used by Jablotron was RC-44. It was not possible to arm and disarm the system with the same button. There were separate two buttons with each having its own purpose and certain function. As keyfob signals also constantly overlapped with hub signaling it was needed to record keyfob signals away from the main system. Overlapping signals in time can be seen as a means of protection against replay attack but it only works when both devices are in close range.

Set of 15 different arming and disarming pushes were collected. After trying those replays near the hub, not a single one of them worked. Keyfob itself worked perfectly and when armed with the keyfob, it was possible to disarm the system with our recorded keypad signal, but none of the keyfob recordings worked. Another 30 keyfob disarm pushes were recorded and tried, but without a positive result. Figure 27 shows how a closer look was taken by zooming into the keyfob signal and noticed that signal curvature was not ordinary.

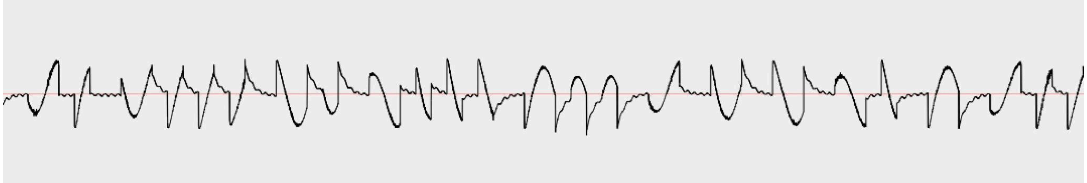
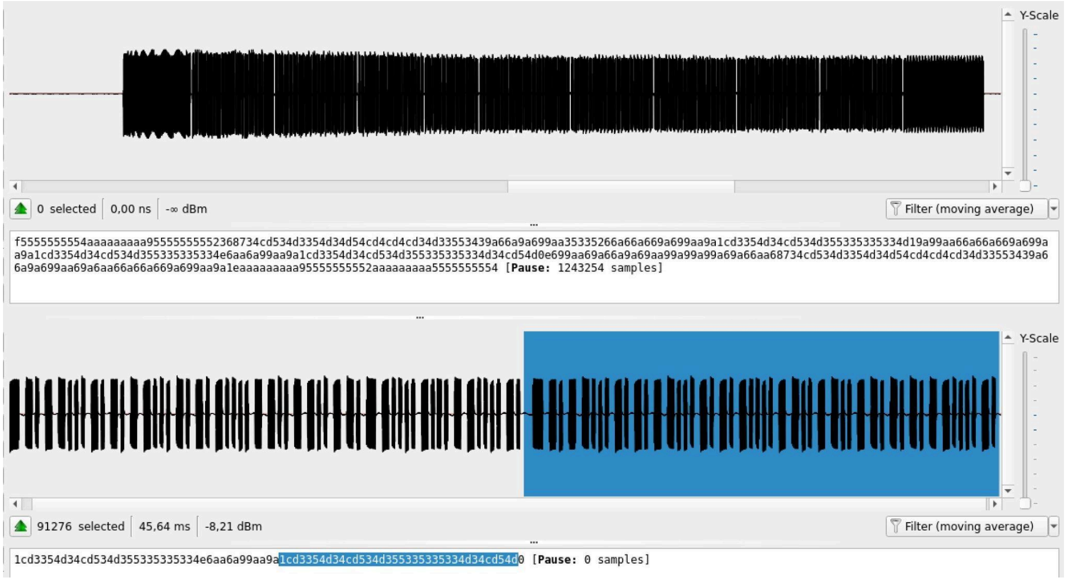


Figure 27. Jablotron having unusual keyfob signals seen in URH by zoomed in view.

Reason was probably a poor battery status of the keyfob. Even though the keyfob itself quickly and without any problems could arm and disarm the system, it was measured that the L1016 battery which should give out 6V had only 5.2V voltage and it dropped while pushing a button under 4V. It seemed too on the edge, so the battery was replaced and a new set of recorded 30 clean disarm signals were tested, but the result was the same. No simple replay attack on Jablotron keyfob.



```
f5555555554aaaaaaaaa95555555552368734cd534d3354d34d54cd4cd4cd34d33553439a66a9a699aa35335266a66a669a699aa9a1cd3354d34cd534d355335335334d19a99aa66a66a669a699a
a9a1cd3354d34cd534d355335335334e6aa6a99aa9a1cd3354d34cd534d355335335334d34cd54d0e699aa69a66a9a69aa99a99a99a69a66aa68734cd534d3354d34d54cd4cd4cd34d33553439a6
6a9a699aa69a6aa66a66a669a699aa9a1eaaaaaaaaa95555555552aaaaaaaaa5555555554 [Pause: 1243254 samples]
```

```
1cd3354d34cd534d355335335334e6aa6a99aa9a1cd3354d34cd534d355335335334d34cd54d0 [Pause: 0 samples]
```

Figure 28. Zoomed in view of Jablotron keyfob disarming signal using ASK modulation.

From the upper Figure 28 it can be seen that within one push several signals are being sent and some parts of these signals are similar to each other. Transmitting only one or two parts at a time also did not bring any positive result.

4.3.1.3 Keypad

Five sets of arming and disarming were recorded while the system was using the "JA-60F- EN COMFORT" keypad to see what was happening inside the signals. After opening signals with the URH analyzer it was seen that some of the recorded signals were still influenced by hub signaling which at some occasions overlapped in time with keypad signals.

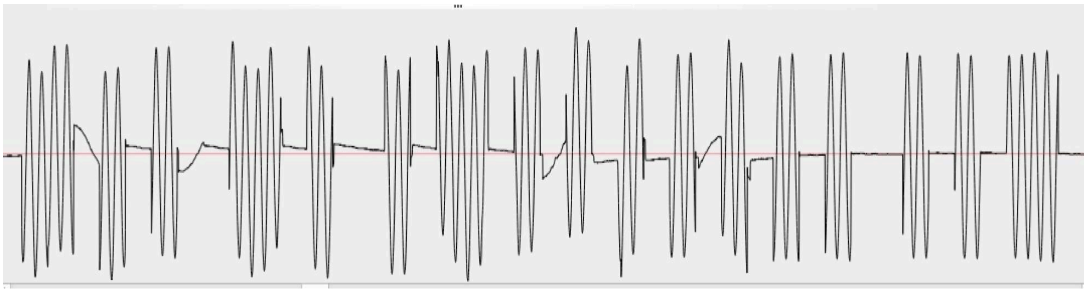
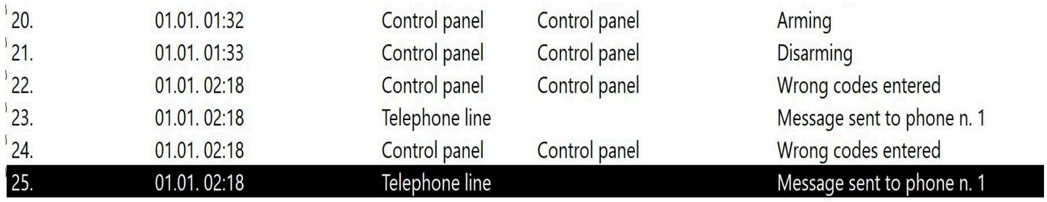


Figure 29. Jablotron keypad signal partially overlapping with weak hub signal.

When looking at upper Figure 29 it can be seen that when zoomed in into the signal some unusual situation has occurred. It was not seemingly big level interference but it evidently changed the coding inside the message and that is the reason why it was not possible to arm and disarm the hub at first.

When looking into the connected software events list, seen in Figure 30, it was seen that the system declared of wrong code being entered and also generated an alert SMS because of that – even though the system was currently in disarmed state. This might be a built in security measure to detect tampering from trying out the codes.



20.	01.01. 01:32	Control panel	Control panel	Arming
21.	01.01. 01:33	Control panel	Control panel	Disarming
22.	01.01. 02:18	Control panel	Control panel	Wrong codes entered
23.	01.01. 02:18	Telephone line		Message sent to phone n. 1
24.	01.01. 02:18	Control panel	Control panel	Wrong codes entered
25.	01.01. 02:18	Telephone line		Message sent to phone n. 1

Figure 30. Jablotron system declared that a wrong code was entered when a replay attack was generated.

After analysing our collected sets in URH, it was noticed that on one occasion illustrated in Figure 31, there was no overlapping present, and when tested then replay attack returned a positive feedback. It was possible to arm and disarm the system with the same code several times in a row.

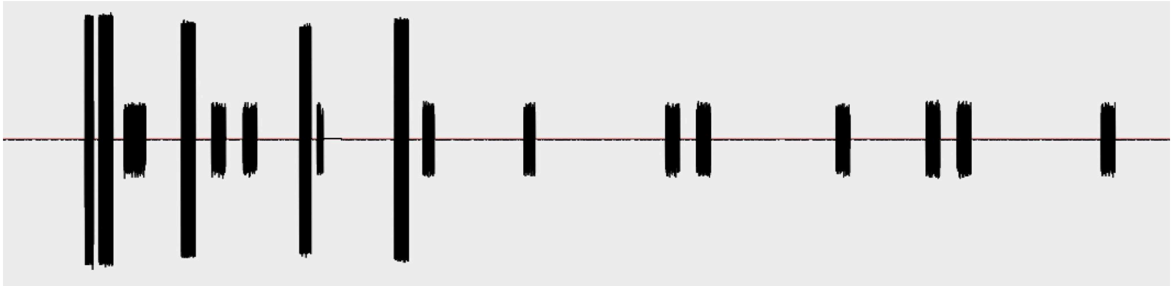


Figure 31. Jablotron non-overlapping set worked for arming and disarming the system as a replay attack.

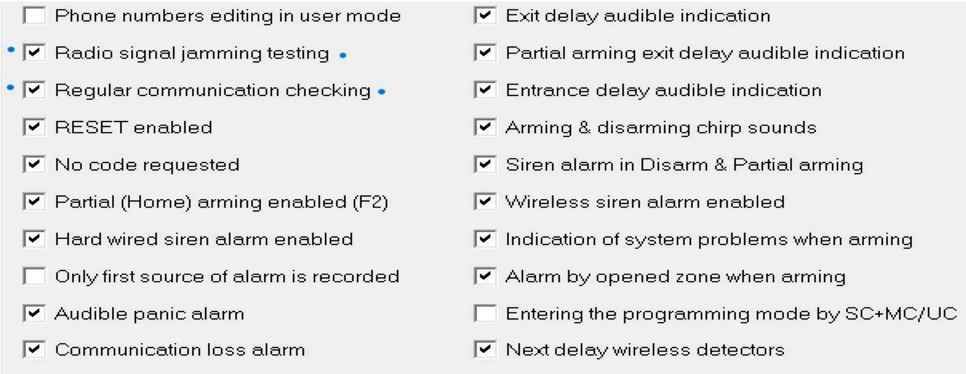
For the system itself it did not matter how the code was sent and there was no reaction or difference detected in the software event list.

It was possible to notice from the URH window that the system was armed when the last keypad data chunk had been excited. Different parts of that signal were extracted and tested separately but replay only worked when all parts were present.

Another recording was made of arming the system with the same code 1234. It was analysed in URH and was seen that no overlapping signals occurred. Nevertheless when it was tried to arm or disarm with that signal, it was unsuccessful. It can be seen that coding is different within these signals, but it is unknown how the system itself regulates that, and why one session is fully functional every time while other ones do not work when replayed. It needs more investigation and will be done in future works as in general it is proven that JA-63 can be attacked with replaying the signals, but not all collected keypad signals provide a straightforward replay attack.

4.3.2 Interference testing

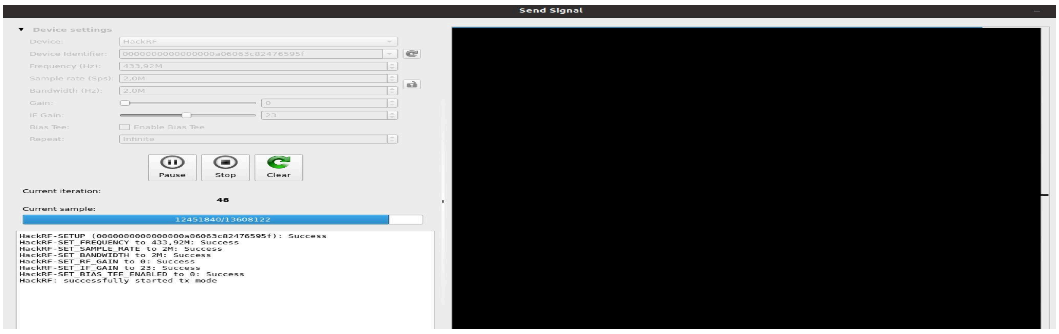
GNU Radio simple interference generator with HackRF was used for several minutes really close to Jablotron hub antenna, but there was no indication of jamming detection by the system. No new events were triggered. When observing settings over the Jablotron control software "ComLink" connection a section was discovered where it was possible to control jamming detection and also regular communication.



□ Phone numbers editing in user mode
• ☑ Radio signal jamming testing •
• ☑ Regular communication checking •
☑ RESET enabled
☑ No code requested
☑ Partial (Home) arming enabled (F2)
☑ Hard wired siren alarm enabled
□ Only first source of alarm is recorded
☑ Audible panic alarm
☑ Communication loss alarm
☑ Exit delay audible indication
☑ Partial arming exit delay audible indication
☑ Entrance delay audible indication
☑ Arming & disarming chirp sounds
☑ Siren alarm in Disarm & Partial arming
☑ Wireless siren alarm enabled
☑ Indication of system problems when arming
☑ Alarm by opened zone when arming
□ Entering the programming mode by SC+MC/UC
☑ Next delay wireless detectors

Figure 32. Enabling Jablotron radio signal jamming testing and regular communication checking.

From the upper Figure 32 it is also possible to see "Next delay wireless detectors" is enabled, probably to save battery and not to trigger continuous alarm with every single motion detected while in armed status. It was disabled to conduct quicker testing for the peripherals. An interference signal was created from one of the PIR triggering signals by replicating itself and adding it into empty spaces covering the whole time frame with energy as seen in Figure 33.



Device settings
Device: HackRF
Device Identifier: 0000000000000000a06063c82476595f
Frequency (Hz): 433,92M
Sample rate (Sps): 2,0M
Bandwidth (Hz): 2,0M
Gain: 0
IF Gain: 23
Bias Tee: □ Enable Bias Tee
Repeat: Infinite

Current iteration: 48
Current sample: 12451840/13608122

```
HackRF-SETUP (0000000000000000a06063c82476595f): Success
HackRF-SET_FREQUENCY to 433,92M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 23: Success
HackRF-SET_BIAS_TEE_ENABLED to 0: Success
HackRF: successfully started tx mode
```

Figure 33. Sending interference signal generated from Jablotron "PIR trigger 1" signal with low gain.

It was estimated that this interference signal, built as it was, is instantly going to trigger the alarm because it contained a code from PIR 1 motion signal. Nevertheless, it worked perfectly. None of our peripherals worked correctly - no indications were detected by the hub. The hub did not capture any tampering nor code from keyfob or motions, the keypad was out of play etc. No information was logged in the software and no jamming detection indication was available. The "PIR trigger 1" was not detected once. The system probably needs some empty pause before and after the signals to get full understanding of info being received. Whole 433MHz band was not needed to interfere as the whole system used frequencies close to 433,93MHz and no frequency hopping or alternative channels were present similarly to Paradox systems. For the notification channel the current system used a GSM modem which was not disturbed. It was tried to kill the signal by disconnecting the modem antenna, but no reaction was noticed in the software log. After removing a SIM card, it took about 10 minutes until "Telephone line failure" notification was declared in the software log and the alarm was started. After reinserting the SIM, it was announced that "Telephone Line is OK" and no failure was detected anymore in the system even though there was no antenna connected to the GSM module and when trying to call in, a nice lady told us that the phone we are trying to reach is turned off or out of coverage area - proving that there was no reception. System probably detects SIM failure, but is not reacting to interference. No actual jamming detection was detected.

4.4 Hikvision AX PRO DS-PWA96

Hikvision is a Chinese product, but higher end one and should actually comply with at least some standards. Nevertheless it does not clear it from possible China related spying problems [45]. The Hikvison system is quite similar to the Ajax system. Both of them are new and highly advertised systems currently at the market. AX PRO is equipped with two SIM slots, has Wi-Fi and Ethernet cable connection. Many different sensors are supported as can be seen on Figure 4 [29]. It has a mobile application which is constantly taking care of updates - still some pushes must be done to accept the update, and it is not fully automatic to update system firmware. That system was tested over several months and the biggest flaw of the system is probably usage of LF tags which are easily cloneable. Interference testing showed that the system has proper detection built in. None of the replay attacks succeeded. There is no straightforward easy replay possibility to interact with the system. Even reed switch and PIR signaling was constantly changing and the control hub did not accept any of the replays ever. Simple examples are given to illustrate works done, but to conclude it is admitted that in the replay attack context the system was unbreakable.

4.4.1 Replay attack

Replay attacks were conducted against PIR, reed switch and keypad signals. None of the attacks succeeded. Only a few examples are submitted to illustrate the complexity of the signals. Full bitlevel analyze of all collected data was not carried out.

4.4.1.2 Reed switch

HEX sample of signal 2) collected with URH:

```
d555555555555555555555555555555555555555555555555555555555555555555555555
555555555555555555555555555555555555555555555555555555555556768b20e80002d
23d4cd02c28edc0200001c8c004ebdc6540168a21994f2b6b783f784
```

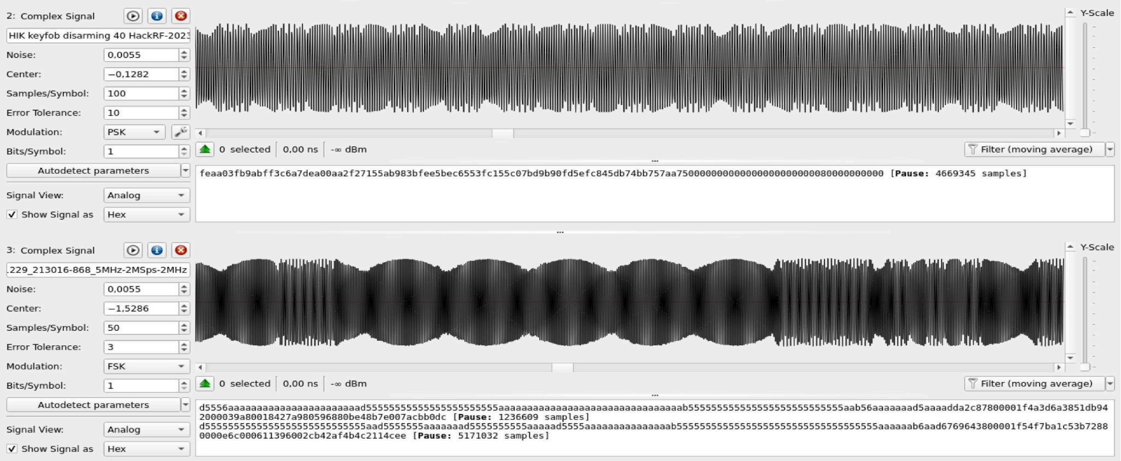
It can be seen that there is a big prefix for all the signals and it was possible to also find some similarities after the prefix for some signals:

```
18)  80c604   02c28edc  020000 1c 0 800 4e b9cb0  002d14  53ed63   ff  107dcb80a
20)  874c38   02c28edc  020000 1c 2 400 4f  05caf  002d14  6b4ee46  51  675cbfd8
2)   23d4cd   02c28edc  020000 1c 8 c00 4e  bdc65  40168a  21994f2  b6  b783f784
3)   329b32   02c28edc  040000 39 9 0009d cb8e5    005a28  0dae12d  6e  db4761978
16)  799660   05851db8  040000 39 d 0009d bb95e    005a28 70bfb166  6e   f2d9790
12)  6ddfaa   05851db8  080000 72 e 0013c  e72b8    00b45  0ff2752   d3  d1f942e6fffff
15)  ef208    02c51db8  080000 73 8 00176  ee578    01d28  98166b6   13   4bbbfddfffff
```

It was possible to see that there is some repetition in reed switch alarm signals but within over 10 repetitions ,it was seen that at least 33 HEX symbols are changing in unexpected way. It is assumed that more than 100 signals should be saved with URH and analysed to recognize some pattern or give final remarks about certain bits that could be taken into account of generating brute-force attack, but at first look it seems, that too big dataset is changing all the time to conduct actual working attack in reasonable time. More than 20 different recorded reed switch alarm signals were replayed, but not a single one gave positive feedback. Different frequencies that were detected beforehand were tested to replay reed switch signals: 868,023MHz; 868,223MHz; 868,423MHz, but without results to generate a falsified trigger for the hub. The system uses two-way signaling and algorithms are pre-shared for the next session to agree, which will be the next frequency channel and what kind of signal would be expected.

4.4.1.3 Keyfob

Fifty arming and disarming signals were collected for the Hikvision keyfob. Nevertheless none of the replays worked. It was problematic to analyse signals with URH as signals seemed to change their characteristics. Figure 34 shows that only logical readable results were sometimes given with FSK and other times with PSK modulation. Sometimes no reasonable data was seen at all with autodetection or manual configuration. Signals themselves consisted of several datasets and one set was usually 40-60 ms long. It is not reasonable to analyse these signals manually.


2: Complex Signal
HIK keyfob disarming 40 HackRF-2023
Noise: 0,0055
Center: −0,1282
Samples/Symbol: 100
Error Tolerance: 10
Modulation: PSK
Bits/Symbol: 1
Signal View: Analog
☑ Show Signal as Hex

0 selected | 0,00 ns | -∞ dBm

```
feaa03fb9abff3c6a7dea00aa2f27155ab983bfee5bec6553fc155c07bd9b90fd5efc845db74bb757aa75000000000000000000000000080000000000 [Pause: 4669345 samples]
```

3: Complex Signal
229_213016-868_5MHz-2MSps-2MHz
Noise: 0,0055
Center: −1,5286
Samples/Symbol: 50
Error Tolerance: 3
Modulation: FSK
Bits/Symbol: 1
Signal View: Analog
☑ Show Signal as Hex

0 selected | 0,00 ns | -∞ dBm

```
d5556aaaaaaaaaaaaaaaaaaaaaaad5555555555555555555555aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaab5555555555555555555555555555aab56aaaaaaad5aaaadda2c87800001f4a3d6a3851db94
2000039a80018427a980596880be48b7e007acbb0dc [Pause: 1236609 samples]
d555555555555555555555555555555aad5555555aaaaaaad5555555555aaaaad5555aaaaaaaaaaaaaaaab5555555555555555555555555555555555555aaaaaab6aad6769643800001f54f7ba1c53b7288
0000e6c000611396002cb42af4b4c2114cee [Pause: 5171032 samples]
```

Figure 34. URH was not able to adequately determine Hikvision keyfob signals.

4.4.1.4 Keypad

Ten clean arming and disarming sets of codes 0000; 1234; 5678 and 9999 were collected. And same code sets also together with central hub response included. Interaction with the hub by our replayed signals was not successful. Dataset is going to be analysed more deeply in future works.

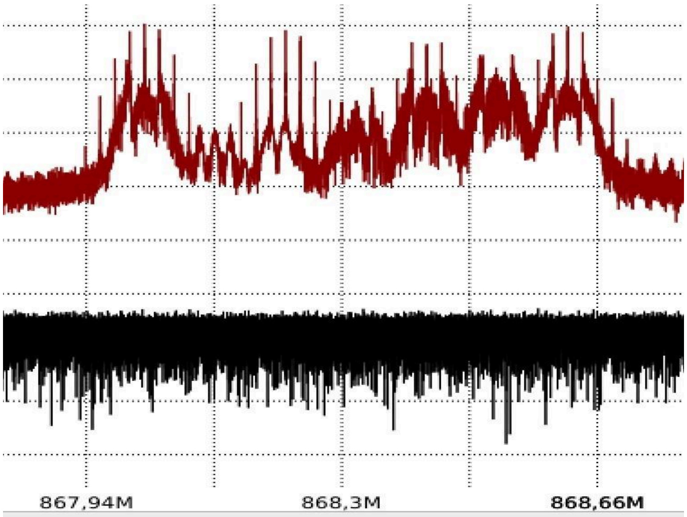


Figure 35. Hikvision keypad frequency use while arming and disarming with code 9999.

It can be seen from Figure 35 that different channels from 868MHz to 868,7MHz are used by keypad. That means a problem for our testing as a simple URH setup is not able to send a replay attack timed over different frequencies over URH. A python script needs to be created and proper timings and signal parts accordingly collected to send out the right signal at the right moment. It is left out of the scope as it is not considered as an easy store-and-forward replay attack anymore, which could be easily achieved by random criminals with poor knowledge and toolset. Figure 36 illustrates the session of keypad disarming signals.

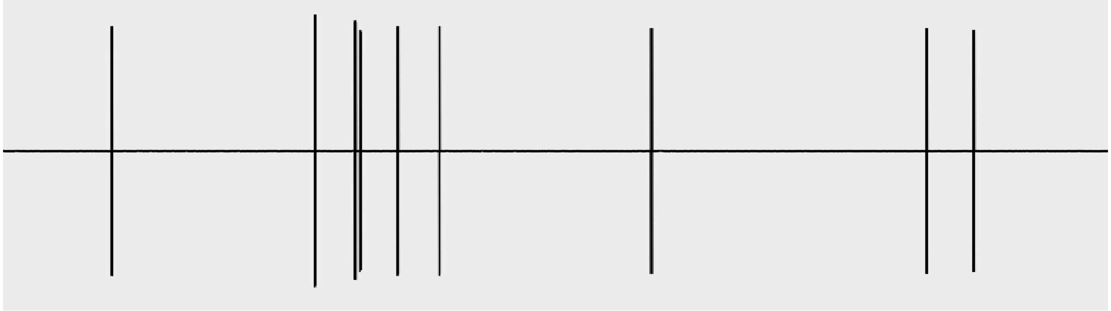


Figure 36. Disarming with Hikvision keypad using code 5678 with no hub signals included.

First set of signals was being sent when activating the keypad. Second set of signals was sent out after pressing the disarm button. Of course code was entered beforehand. Usually the system declared that it was unarmed after two close signals occurred (similar effect with arming) - third and fourth set, close to each other, on the upper Figure 38. The actual code data is forwarded with a second signal and two close-by signals will be transmitted as verification. After that, usually some other signals occurred, then there was a pause for some seconds and another transmission occurred. Then again pause for some seconds and two higher peaks in the end declared that the keypad switched off its screen. All signaling seems to be two-way communication – always the other side gives an answer. Total disarming process from the first keypad signal till the last one took over 36 seconds. Usually it was possible to get a reasonable result with FSK modulation, but from time to time URH was unable to properly demodulate signals and get readable results.

Example of close by signals changing parts using FSK and HEX in URH:

2000000bdf297b1b851db91a000039c8009c737bd0 07c7b1e41d6dd136c8d1b61f4297
1d00000bdd0ff7 1b851db91a000039c0009f9383c8 07c7bed15ef6eb23558a36

Example of signal sent before upper two close-by ones that could contain the actual code:

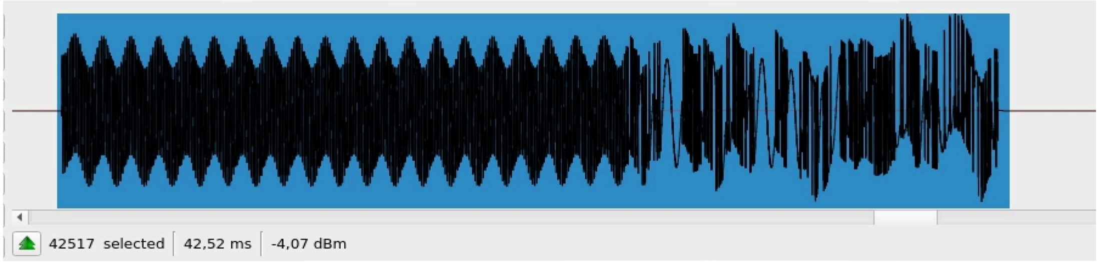


Figure 37. Hikvision keypad signals sometimes have strange signal formats.

Sometimes the signal containing the code was using the format seen in upper Figure 37 and then URH was able to provide HEX over FSK as having 36 HEX symbols changing. But sometimes the visual format was different and seemed normal, without any strange changes inside or in the end. In these cases logical HEX derived was similar to:

5555555555555555555555555555555555555555555555555555555555555555555555555
5555555555555555555555555555555555555555555555555555555555556768b212800006
3f88068dc28edc8d00001c20004e39bddc01f1eea0d47a84843cbfb8450606bc8a67ab58

Either way the changing part after the prefix of the signal is too big and random to try any manual analyze. The change in the visual format might be connected to the frequency change. It may be possible that this different visual look also has some different properties when it comes to the analytical part - might be even broken signals not properly encrypted.

4.4.2 Interference testing

PIR that was constantly using the same channel was detected with the URH spectrum analyzer and was tried to disturb with a 200kHz wide Gaussian noise signal.

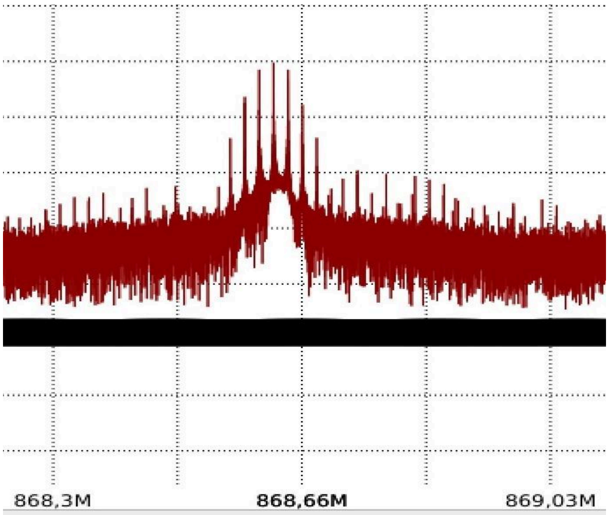
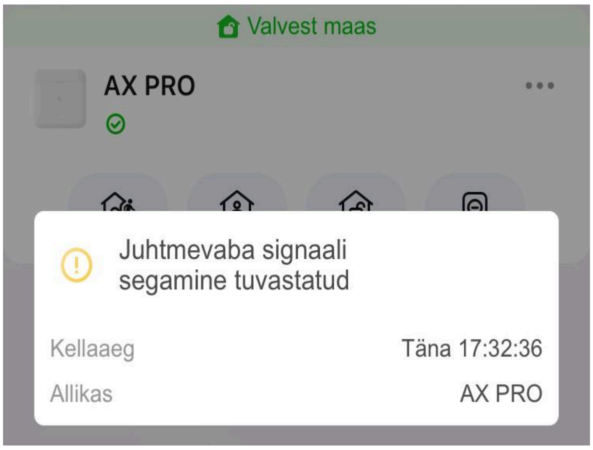


Figure 38. Hikvision PIR frequency channel changes were not detected in usual circumstances.

Interference signal was set on 868,6MHz with 200kHz channel width according to Figure 38, but it was not working as PIR continued sending in alerts about detected movement. If at first PIR channel centre frequency was close to 868,6MHz, then after interference testing it used a channel with centre frequency close to 868,5MHz. That 200kHz signal was detected and reported as a jammer as can be seen in Figure 39. In case a wider 868MHz band was tried to disturb, then it was also detected within a few seconds. Similar situation was with a disturbance test on a Wi-Fi connection. Even when detection worked the peripherals were still out of reach.



Valvest maas

AX PRO

Juhtmevaba signaali segamine tuvastatud

Kellaaeg Täna 17:32:36

Allikas AX PRO

Figure 39. Wi-Fi interference was detected by Hikvision hub within seconds and notified in the application.

4.5 Chinese systems: Tecpeak; PGST; G-Homa

In total 7 different cheap Chinese wireless security alarm systems were tested. Some of them were from the same brand, but system description and general capabilities were different. Firmware and hardware was different, but software application used by mobile phone could be on PGST and Tecpeak systems the same for all the sets- applications called Tuya or Smart Life. These applications were available for both iOS and Android platforms. The G-Homa system had its own application named “G-Homa”. The iOS and Android versions were used to test the systems, but the other one was only tried when first did not function properly. As there are 7 quite similar systems it is not deeply elaborated on every single one while providing results, but focused more generally to forward the situation about Chinese cheap systems available in the Estonian market. Cheap can be defined by general comparison between prices as Ajax cost goes easily over 500€ but aforementioned Chinese systems were purchased mostly under 50€ per system. Nevertheless all cheap Chinese systems were tested separately with the same means like other brands. All Chinese systems used similar sensors and tags/tokens. Some of them were interchangeable. All the systems used a 433MHz band. There was no extra keypad included with the systems - all numbers could be entered straight on the main hub. Risks about allowing cheap Chinese systems with a microphone into your home Wi-Fi network and also installing control applications to your mobile, are left out of scope of this thesis.

4.5.1 G-Homa

G-Homa Wi-Fi alarm set was purchased on the second-hand market. It was chosen by picture where all information on boxing was written in German language. Also the manual is in German language meaning that the current product is originally designed for the German market. Price of the unit on the second-hand market was about 20 €.

System includes a control centre: EMW302WF-HS, 4 reed switch sensors RF302DA for doors and windows and one PIR RF302PIR. There is no keyfob or keypad. Also no other notification channel than Wi-Fi. System is controlled over G-Homa application version 3.0.25. Application build-up is poor and also had troubles connecting sensors to the central. With Android application there was even no proper push notification capability available. After an alarm it takes about 1 minute for the system to reset itself and then it is able to collect alarms once again. System sensors used frequency 433,93MHz as shown in Figure 40.

Replay attacks

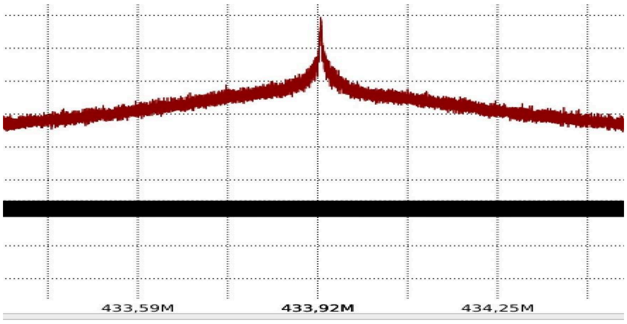
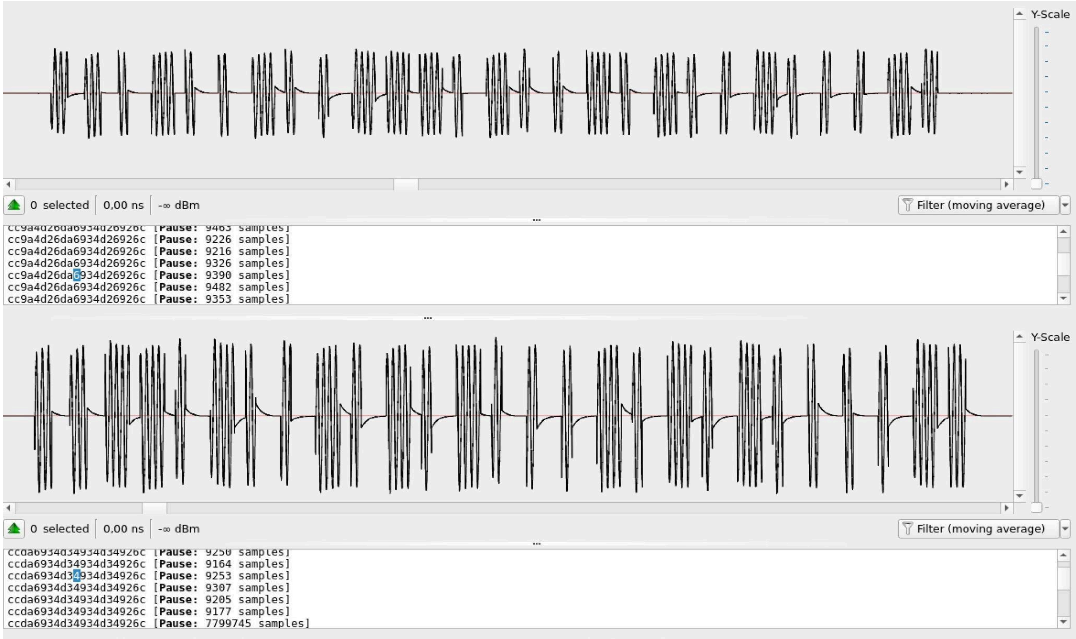


Figure 40. G-Homa frequency use.

Replayed PIR and reed switch signals were generating false alarms.



```
cc9a4d26da6934d26926c [Pause: 9463 samples]
cc9a4d26da6934d26926c [Pause: 9226 samples]
cc9a4d26da6934d26926c [Pause: 9216 samples]
cc9a4d26da6934d26926c [Pause: 9326 samples]
cc9a4d26da6934d26926c [Pause: 9390 samples]
cc9a4d26da6934d26926c [Pause: 9482 samples]
cc9a4d26da6934d26926c [Pause: 9353 samples]
```

```
ccda6934d34934d34926c [Pause: 9250 samples]
ccda6934d34934d34926c [Pause: 9164 samples]
ccda6934d34934d34926c [Pause: 9253 samples]
ccda6934d34934d34926c [Pause: 9307 samples]
ccda6934d34934d34926c [Pause: 9205 samples]
ccda6934d34934d34926c [Pause: 9177 samples]
ccda6934d34934d34926c [Pause: 7799745 samples]
```

Figure 41. Zoomed in view of G-Homa PIR and reed switch signals to get PWM code.

The PWM key was generated by using 700vs300 microseconds to get 1ms set equal to one bit. A total 27 bits long PWM message was used to address sensor signals. Bits were counted visually from Figure 41:

Reed switch PWM code: 110100100111010010100100011
PIR PWM code: 111101001010100010101000011

General RF channel and Wi-Fi channel for notification interference

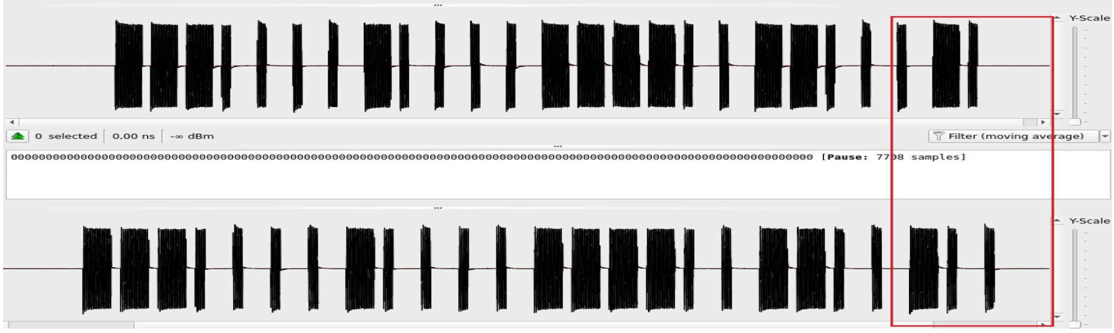
Usual GNU Radio disturbance signal setup was used and it was successful in blocking the signals generated by real sensors and keyfobs at 433,93MHz. Also 2.4GHz Wi-Fi interference was successful – commands from the application did not go through. As this system application had problems sending out proper notification to the mobile then our test with disturbing the notification channel was not possible to conduct properly as sometimes notifications were not sent even while there was no interference applied. In general the current system was the poorest set tested.

4.5.2 PGST PW150

When sensors were disabled from the switch while the system was armed no indication or alarm was raised by the hub. There is no built-in sensor check function. It is very important that in cases like that sensors would be properly installed and physically screwed down to avoid access to the on/off switch which is located behind the reed switch and PIR sensor. Reed switch had also a tamper switch behind the sensor so it would trigger an alarm if armed and tried to remove it. In general disarmed state only "24 hours Active" sensors like distress SOS button triggered an alarm, but tamper signals were not separately configurable and were disabled when the system was disarmed and sensor was not in 24 hours active regime. Also there was no sensor status checking before arming the system. It was possible to arm the system even if the magnet was away from the reed switch. In that case when a magnet was put back near to the reed switch then an alarm was generated. It was possible to change system settings while the system was under armed state including sensor regime. It was possible to delete a sensor while the system was in armed state and after deletion of that sensor, it was not triggering any alarm after the magnet was removed from the reed switch. At the same time when the sensor was tried to add while in an armed state, the system notified us of a need to disarm the system beforehand. If the alarm was triggered by a reed switch then the application only showed us this first alarm trigger – it was possible to move in front of PIR without getting a second sensor indication. If "Alarm Remove" was not pushed on the application, then nothing happened anymore. The whole system was on hold waiting for the application input. Only in case sensors were configured as "24 hours active" regime, then new data was accepted and with every trigger an alarm was raised. If sensors were in "Out arm active" regime then nothing happened. It was the same situation un-dependable of the first triggering unit. Also the system log file did not contain any information about PIR which was meanwhile triggered several times. If "Alarm remove" was pushed on the application then the system got automatically disarmed even though it was hoped that it stays in an armed state and only that one trigger will be ignored. In the application there is a possibility that the application itself is going to get notified if the system has been offline for more than 30 minutes. It works, but it is unknown if it works just through timer and ping or if there is a secret cloud service behind it. It must be verified by analyzing Wi-Fi traffic of the phone and system hub, but is considered as not too important and is left out of the scope. Offline notification is only once after the first 30 minutes. All system arming and disarming and alarms data is forwarded to the application, but fortunately only dataset from time since being first connected is seen – no older data is visible. There is no notification if the device returns online. No two-way connection between hub and sensors is visible or seen over URH. PGST PW150 hub was not communicating with sensors over 433MHz. It only received a sensor signal but never sent anything out on that frequency.

Replay attacks

After recording some of the keyfob signals with URH it was clear that PGST used similar PWM coding as the G-Homa system. It was noticed that signals look like a pulse width modulated and ASK or PSK or FSK demodulation was not adequate. When looked closer, most of the working arming and disarming signals had the same similar PWM outfit. When measured the ¾ filled part was 1,25ms and paused part 420us. The ¼ filled part was vice versa 420us and pause was 1,25ms. It gives us the following when estimated that ¾ part is 1 and ¼ is 0. For keyfob 1 Figure 42 is describing the PWM coded signals.



```
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 [Pause: 7708 samples]
```

Figure 42: PWM coding difference between arming and disarming signals for PGST PW150 keyfob.

In time scale it gives us 41,75 milliseconds for 25 bit signal transfer.With similar means it was determined PWM encoded data sent for other signals also:

PIR:	1000011111000011001101100
Reed switch:	0100010011011011100001100
SOS button:	0110111011010001000101100
Keyfob 1 arm:	1110000100001111001100**010**
Keyfob 1 disarm:	1110000100001111001100**100**

Reed switch tamper switch was generating exactly the same alarm message as removing the magnet from the switch. It is probably the same message and two triggers are just connected to the same reed switch signaling output.

General RF channel and Wi-Fi channel for notification interference

System was easily disturbed with the signal generated in URH over 433,93MHz. Keyfob worked only against the hub to arm or disarm the system. While in armed status no sensor activity nor SOS button or keyfob (from distance) was able to influence the system. No jamming detection was noted.

Our Wi-Fi network was on channel 4 (2416–2438MHz) having a centre frequency of 2427MHz. An interference signal created with GNU Radio shown in Figure 9, was successful in disturbing our own channel that was used by PGST PW150 to connect to the internet. No notifications arrived to the application while interference was present. If interference was disabled then notification that first generated the alarm was received with current moment timestamp together with a note for arming and disarming in the same moment. When the system was disturbed and the reed switch was triggered during that time, plus power was removed from the hub and put back and the interference signal turned off, then the system announced that Wi-Fi was connected; a red LED was rapidly blinking on the hub indicating an alarm, but no new notification was sent to the application. Meaning that in case attackers are jamming Wi-Fi signals and acting within a 30 minutes time frame before the application gives an offline notification, no triggered indications are sent for the owner over the notification channel -informing that something has happened. When coming home, people will disarm the system before entering premises and that disarm command will turn that blinking red LED again into green – so if hub is not visible from behind the front door for the user to see before entering premises that red LED is flashing, then no recording of any mishap will be never seen and owner thinks that everything is perfectly OK. Of course jamming only the communication channel will still activate local alarms in case local sensor communication is not jammed at the same time. Previous is also a relatively easy task to complete when buying a multiband jammer from China’s online stores [46]. With HackRF, it is mainly a question of getting adequate power level out of it. For real life positive action it will require an amplifier and possibly also a better antenna, depending on a frequency going to be influenced and a distance covered.

4.5.3 PGST PG-103

There are several added functions compared to PGST PW150: AC power failure and restored notification; 2G SIM card capability; microphone available in the system to store 20 seconds of voice in case of an alarm and call in function; internal battery; external signal bell and possibility to add wireless bell; tamper alarm switch on the back of the hub wall hook; screen and menu control possibility without an application; RFID tags and reader; possibility to control power sockets over the alarm system. System also has the possibility to control it over SMS. If the system mobile number is known and the default engineer password 6666 is unchanged, then the system replies from whatever mobile number the question is asked. For example sending SMS code *6666*62* will return system serial; language; engineer password (6666); user password; GSM cell signal quality; Wi-Fi network RSSI. For example if user code is 1234 then for arming a user code 1234#1 must be sent and 1234#2 can be used to disarm. Nevertheless the system also sends the same messages to the original programmed mobile number that has been used by the owner. As a positive security measure it may be noted that it was not possible to turn off the hub from the on/off switch while in an armed state. There was two-way communication as every time a signal set was transmitted from the main hub, after the keyfob had been pushed. It is intended for wireless alarm bell to squawk according to actions.

Replay attacks

All keyfobs were straightforward replay attackable and same was the situation with system sensors. It was verified in URH that similar PWM coding was used.

General RF channel and Wi-Fi channel for notification interference

Interference testing with 433MHz and Wi-Fi was similar to the PGST PW150 system. All sensors and communication channel were easily influenced. There is no jamming detection in general, only a notification from the application after a connection has been down for 30 minutes.

4.5.4 PGST PG-107

Added functions compared to PGST PW150 and PGST PG-103 were: system shows local temperature; humidity and PM2,5 level; was possible to attach 4 wired sensors.

It is possible to remove power from the main hub before it can send out SMS or call to the owner of the system, but usually the local Wi-Fi still captured the tamper message and sent it forward. It is quite hard to disable the power plug, detach the back tamper and turn off the battery switch all at the same time. That is where the jamming comes handy for the attacker but interfering with 2,4GHz and 433MHz bands is not enough as if any mobile signal reception passes by, then an alarm will be sent out by 2G modem (PGST also has systems with 3G and 4G capabilities available). Attackers still need to fight with the cellular coverage to be sure that notifications are not forwarded when tampering signals are detected. Nevertheless as the system does not have any 433MHz jamming detection it is usually enough to interfere only with that band unless the owner has not connected any wired sensors, which can be added to PGST PG-107.

When the system calls, it is possible to disarm the system by pressing number 2 on the phone keypad. It is also possible to monitor the room, or talk back to the room where the system is located. Numbers pushed on the phone: 1 to arm; 3 to monitor; 4 to talk. Our system tried to call us 3 times in case of an alarm. But it can be configured up to 255 times.

Replay attacks

In general all the sensors and keyfobs were the same as with PGST PW150 and PGST PG-103. General action was the same. URH capture of a keyfob signal was used the same way to visually determine PWM of the signal and tried to determine if this is somehow connected to the serial that was used inside the system for keyfobs registering.

Keyfob 1 PWM code from the URH signal by visual means:

Arm:	1000111010000111100000010
Disarm:	1000111010000111100000100

There was three keyfobs registered in system by serials:

0xc67820	110001100111100000100000
0x8e8780	100011101000011110000000

0x74b8c0 011101001011100011000000

It is possible to see from the upper yellow colour markings that added keyfobs work by their PWM code and it means that it is possible to generate an arm and disarm signals just by knowing the keyfob serial. Also as the difference between arming and disarming is in the end part, and only by bits 100 versus 010, then the first part of the message is 22 bits. A generated PWM code where 100 is in the end and the first 22 bits could be brute forced could be used to disarm any similar system. But if taken into account that time for 25 bits signal is equal to 41,75 milliseconds -determined while working on PGST PW150 signals- then it seems feasible, but as 2^{22} gives 4 194 304 combinations to try for 22 bits, and probably some small pauses are needed between different signals for the receiver to differentiate between different codes, then it still takes several days to try all the possibilities on a common laptop and HackRF. 4 194 304 x 41,74ms = 172 112,192s which is about 48,65 hours and that without taking into account pauses or system capability to send that kind of a stream out. This will be left for future works.

General RF channel and Wi-Fi channel for notification interference

Interference testing for sensors and Wi-Fi notification was successful. There was no jamming notification. Similarly, the mobile application was notifying the user if it had not seen the hub for 30 minutes.

4.5.5 Tecpeak A1

The smallest Tecpeak unit tested. It understood which sensor was added – reed switch or PIR. It acted with the Tuya application a bit better and had more setup possibilities within that application. It had only an internal signal bell. But it was able to call over 2G and send SMS. Very similar to other PGST Chinese versions.

PWM code for keyfob 1:

Disarm: 11000100000111110011000100
Arm: 11000100000111110011000010

Same first 22 bits need to be attacked to get all cheap Chinese sets in our selection disarmed.

Replay attacks

All conducted replay attacks were straightforward. There was no need to analyse any of the signals or figure out some coding or timing.

General RF channel and Wi-Fi channel for notification interference

Interference testing for sensors and Wi-Fi notification was successful. There was no jamming notification. Similarly, the mobile application was notifying the user if it had not seen the hub for 30 minutes.

4.5.6 Tecpeak A2

Replay attacks

As Tecpeak A2 is basically the same system as PGST PG-103 and PGST PG-107 then all the replay signals worked the same way as before with all other cheap Chinese products.

General RF channel and Wi-Fi channel for notification interference

All disturbance testing results were analogous to other cheap Chinese systems. There was no jamming detection built in - only indication from the mobile application if the system was 30 minutes offline.

4.5.7 Tecpeak A4

Tecpeak A4 is a bigger version and is a full analog of PGST PG-103 when it comes to visual look and capabilities. Keyfobs are visually different but still the same PWM 25 bit coding is in use with different three bit end for arming and disarming. Similar tests were conducted as with other systems and results were analogous. Frequencies from PIR and reed switch are 434,11MHz and keyfob is 433,95MHz and hub uses 434,12MHz. The reed switch does not react when under armed status closing the circuit – but reacts only when the magnet is removed. As there is no check of open or closed circuit before arming the system that can be a real problem in actual premises protection setup. It would be also nice if the doorbell signal would be sent as a notification to the user but it only beeps the control station. As the system was basically the same as others all the attacks one by one are not covered.

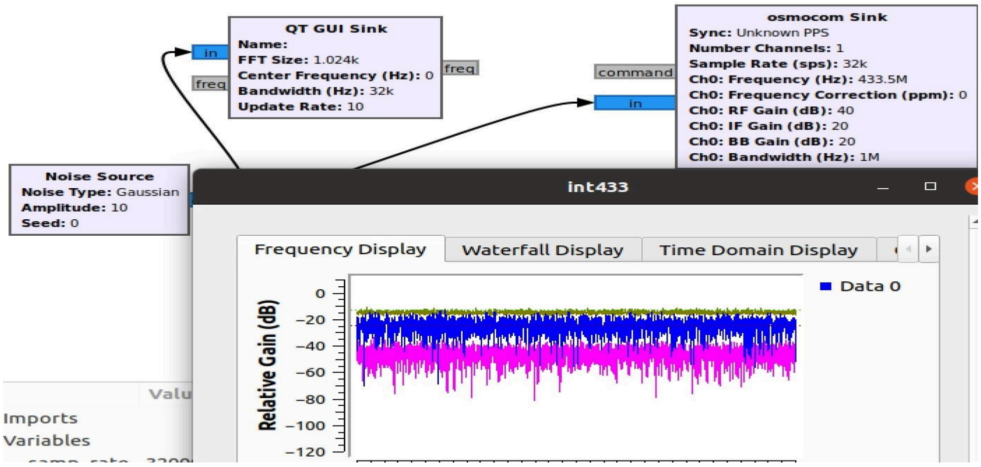
Replay attacks

All replay attacks worked straightforwardly. As it was just a simple store and replay attack then a big dataset was not recorded for later analyze and just noted here that it is possible to simply attack this kind of wireless alarm system with a use of URH and HackRF. Keyfob 2 PWM code was determined to see how much it is different from the previous ones and it is possible to see that still the same 3 bit ending difference is used between arming and disarming signal:

Keyfob 2 PWM code for arming : 1110100001110011000000010
And disarming: 1110100001110011000000100

General RF channel and Wi-Fi channel for notification interference

Figure 43 shows GNU Radio setup to disturb the 433MHz band. All disturbance testing was successful.



QT GUI Sink
Name:
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 32k
Update Rate: 10

osmocom Sink
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 32k
Ch0: Frequency (Hz): 433.5M
Ch0: Frequency Correction (ppm): 0
Ch0: RF Gain (dB): 40
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
Ch0: Bandwidth (Hz): 1M

Noise Source
Noise Type: Gaussian
Amplitude: 10
Seed: 0

Figure 43. Disturbing 433MHz Tecpeak A4 sensor connection was successful.

4.6 Yale IA331

This Yale system has an ASSA ABLOY Group product marking on it. Smart Hub 3.0 model: IA-HUB contained an internal battery 4,8V NIMH 600mAh that was holding power under a minute. There was no means to firmly install the unit to the wall and there was no tamper switch protecting against opening. Built in adequate signal bell. Hub had no Wi-Fi – only Ethernet connection to the internet to get connected to the Yale cloud. No keypad provided within the system.

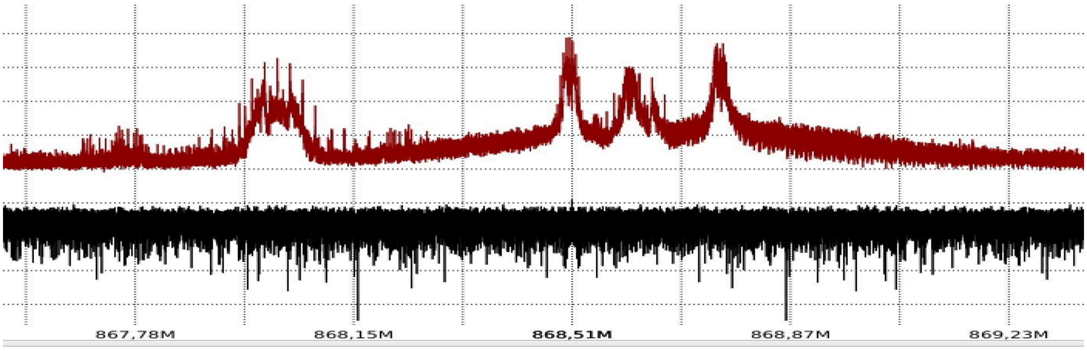


Figure 44. Yale using frequency hopping.

868MHz band was used, but different channels and frequency hopping was noticed as can be seen from Figure 44. Two-way signaling was noticed with sensors. The use of the following frequencies: 867,8 MHz; 868,0MHz; 868,5MHz; 868,6MHz; 868,8MHz was detected and possibly some other channels were in use by the system, but not used during our monitoring period. Channel width was about 200kHz. Tamper signals were more powerful, possibly narrower signals and wider signals usage is separated.

Battery connection is controlled with a separate switch on a side of the hub. If power is cut, and that button is turned off, then no alarm will be generated. Hub did not react on mains cut while under arm status. The Yale application had adequate setup instructions. It was a problem registering our second hand product as an error was received during registration: “Panel master user is max!”. As it turned out, our system was coming as a second hand product from Germany, and an old user had forgotten to delete this device from his application on the systems list. None of the notifications being sent from the hub to the mobile application could be monitored nor was it possible to change any settings ourselves. But as sensors were working and already connected, it was possible to test replay and sensor interference notification.

If it is not possible to even register the system, without someone else beforehand deleting their system, then it shows a way of security built in to prevent overtaking the system just by knowing the serial number of the station. It is a good security measure but in our situation it was just frustrating that Yale does not have some other built in reset button or other means to declare that system now belongs to a new user.

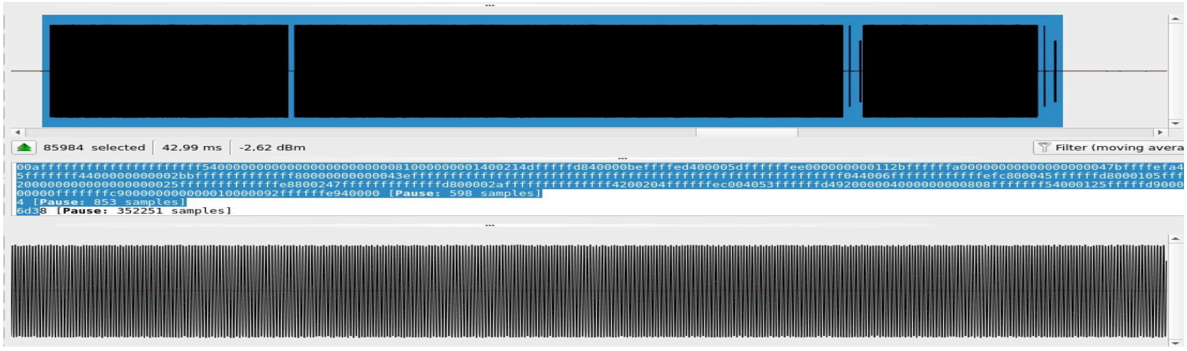
PIR is waking up only in an armed state. If PIR was triggered under armed status and then the system was disarmed by keyfob and armed again by keyfob then PIR went to sleep state after first trigger. Even though the system was armed again –there was no reaction from PIR to trigger an alarm while moving in front of it.

4.6.1 Replay attack

It must be noted that it was not possible to get positive feedback from PIR and reed switch signals recorded a month ago. Nevertheless if signals were freshly recorded then it was possible to work with them during the day. But keyfob replay worked also with a signal set that was a month old.

4.6.1.1 PIR

PIR trigger signal falsification was successful. Replay with PIR trigger signal raised a delay condition - that means that signal was accepted by the central hub and it will be possible to trigger a false alarm. Transmitting frequency must be 868,8MHz or 868,9MHz for properly functioning. One PIR trigger signal consisted of several parts and was more than 40 ms long - visible on Figure 45.



```
85984 selected | 42,99 ms | -2,62 dBm                                    Filter (moving avera
00afffffffffffffffffffffff5400000000000000000000000000810000000014002l4dfffffd840000beffffed400005dffffffee000000000112bffffffa0000000000000000000047bffffefa4
5fffffff440000000000002bbfffffffffffff80000000000000043efffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff044006fffffffffffefc800045fffffffd8000105fff
20000000000000000000025fffffffffffffe8800247fffffffffffffd800002affffffffffffffffffffffffff4200204ffffffec004053ffffffd4920000040000000000808fffffff54000125fffffd9000
00000ffffffc90000000000000010000092ffffffe940000 [Pause: 598 samples]
4 [Pause: 853 samples]
6d38 [Pause: 352251 samples]
```

Figure 45. Yale PIR trigger signal using FSK modulation.

4.6.1.2 Reed switch

Reed switch signals were possible to replay in the same way and falsified triggers could be generated. Sequence recorded is illustrated in Figure 46 and separated signal example in Figure 47.

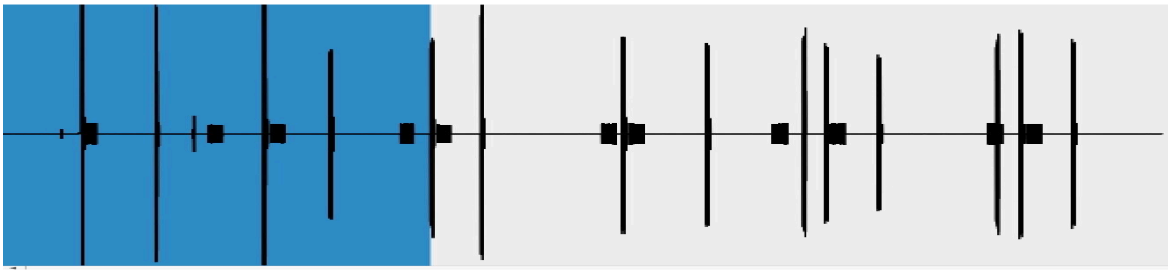
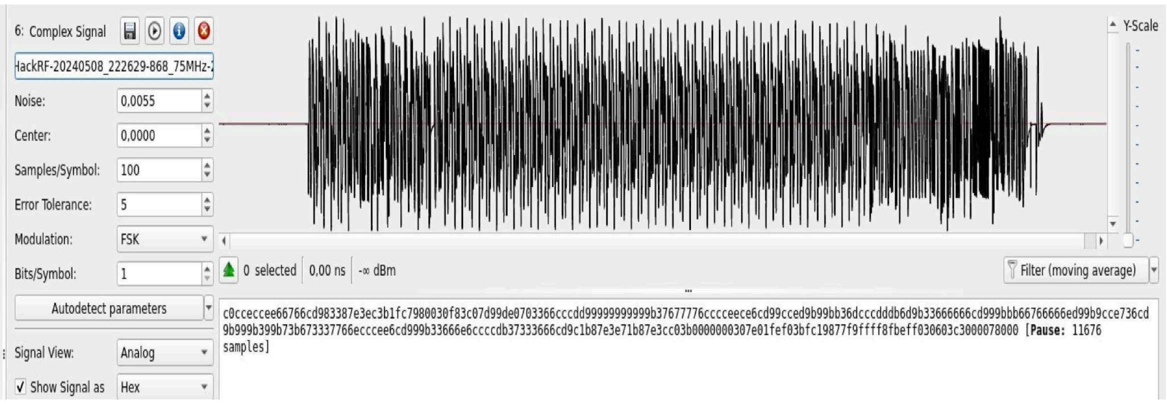


Figure 46. Yale reed switch trigger could be replayed when a sequence was used.



6: Complex Signal

HackRF-20240508_222629-868_75MHz-

Noise: 0,0055

Center: 0,0000

Samples/Symbol: 100

Error Tolerance: 5

Modulation: FSK

Bits/Symbol: 1

Signal View: Analog

☑ Show Signal as Hex

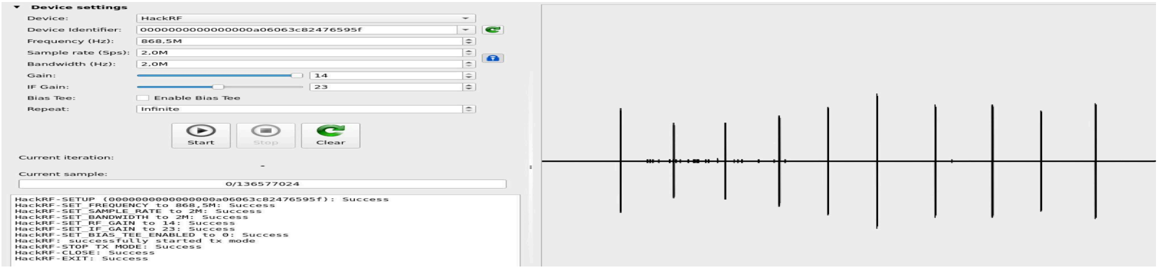
0 selected | 0,00 ns | -∞ dBm

```
c0cceccee66766cd983387e3ec3b1fc7980030f83c07d99de0703366cccdd99999999999b37677776cccceece6cd99cced9b99bb36dcccdddb6d9b33666666cd999bbb66766666ed99b9cce736cd
9b999b399b73b673337766ecccee6cd999b33666e6ccccdb37333666cd9c1b87e3e71b87e3cc03b0000000307e01fef03bfc19877f9ffff8fbeff030603c3000078000 [Pause: 11676
samples]
```

Figure 47. Yale reed switch signal example in URH.

4.6.1.3 Keyfob

Several keyfob disarm button push signals were collected and replayed while the hub was armed. Replay worked with a sequence of several pushes shown on Figure 48.



Device settings

Device: HackRF

Device Identifier: 0000000000000000a06063c82476595f

Frequency (Hz): 868,5M

Sample rate (Sps): 2,0M

Bandwidth (Hz): 2,0M

Gain: 14

IF Gain: 23

Bias Tee: □ Enable Bias Tee

Repeat: Infinite

Current iteration: -

Current sample: 0/136577024

```
HackRF-SETUP (0000000000000000a06063c82476595f): Success
HackRF-SET_FREQUENCY to 868,5M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 14: Success
HackRF-SET_IF_GAIN to 23: Success
HackRF-SET_BIAS_TEE_ENABLED to 0: Success
HackRF: successfully started tx mode
HackRF-STOP TX MODE: Success
HackRF-CLOSE: Success
HackRF-EXIT: Success
```

Figure 48. Yale keyfob disarming signals worked as replay.

Replay disarmed the hub, but it was noticed that it was not all the time working with every single set of recorded pushes. Sometimes push nr 3 disarmed the system, next time push nr 7 etc. There was some kind of loop built into the Yale system to protect for instant store and forward single push replays. Nevertheless our collected sample was able to disarm several times in a row. Even a month later after initial recording, it still worked perfectly. Correct frequency must be used while disarming the system with replay attack. 868,5MHz was suitable to get positive results. Deeper, bit level analyze was not done.

4.6.2 Interference testing

General RF channel for sensors

868MHz sensor signals were successfully disturbed from reaching the hub while interfering with a wider band signal covering all frequency hopping. It was not possible to test disturbance of the notification channel as access to the application was blocked and only ethernet connection was available. There was no possibility to measure the reaction of disturbed notification channel. Interfering sensors for a longer time did not raise any alarm state on the hub. It might be that the system was not programmed properly to react to the jamming attack, but on the other hand it describes how people are really using these systems. Otherwise the system itself was not just good enough to detect jamming, but this is unknown and without confirmation possibility.

4.7 Ajax Hub2 Plus Jeweller

On Ajax circuit boards it is written that the system is designed in Ukraine and its roots together with a factory are also there according to open source information [47]. This system is available in Estonia by different suppliers and is also used by G4S within the system provided as AIKO. AIKO has exactly the same hardware and firmware as the Ajax system. If this system is trusted by a big international company as G4S then there is a high chance that the system has been also tested by their own internal testers and got approval for use. According to the questionnaire, this system was suggested by 60% of the providers as the most secure one - the other 40% suggested wired systems. Mobile application in Android phone with version 3.1 (build #5766) was used to control and monitor the system during conducted testing.

4.7.1 Replay attack

As none of the replay attacks were successful, different sections about negative results are not going to be provided. The same attack architecture was used as before with all the other systems. An overview of things noticed during our testing with some examples is given.

4.7.1.1 PIR

"MotionCam Jeweller" with the firmware EU 5.54.15.2 was tested. Frequency use can be seen in Figure 49. PIR with camera uses two different protocols: Jeweller for alarms and Wings for picture data [48]. Inside the application it was possible to see signal levels together with temperature and battery status. Also tamper status for the sensor lid was shown and it was possible to configure detection sensitivity and picture settings. There was no success replying the signals.

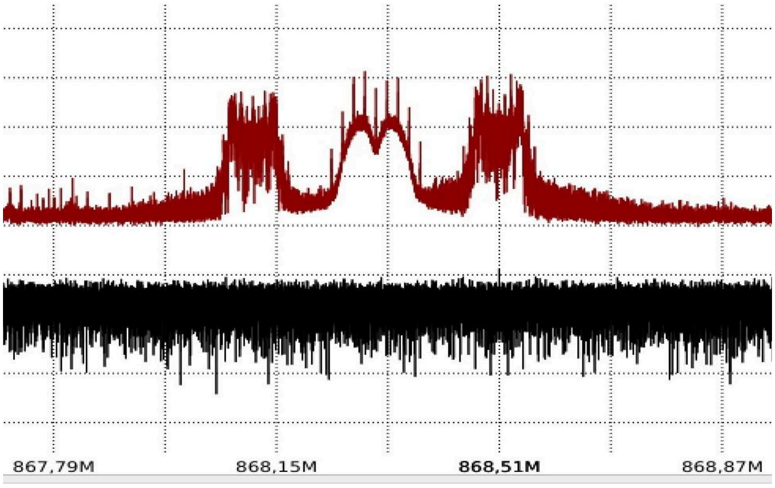
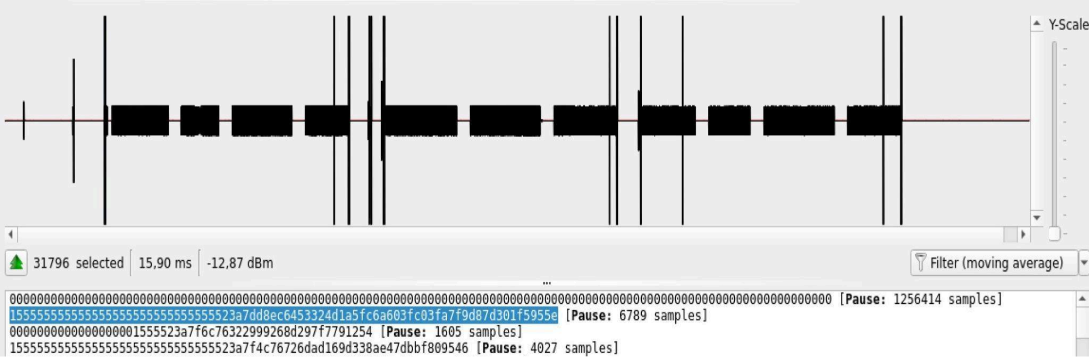


Figure 49. Ajax PIR Jeweller and Wings channels in spectrum while sending information.



```
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 [Pause: 1256414 samples]
155555555555555555555555555555555523a7dd8ec6453324d1a5fc6a603fc03fa7f9d87d301f5955e [Pause: 6789 samples]
0000000000000000001555523a7f6c76322999268d297f7791254 [Pause: 1605 samples]
155555555555555555555555555555555523a7f4c76726dad169d338ae47dbbf809546 [Pause: 4027 samples]
```

Figure 50. Ajax PIR sending pictures using Wings protocol and alarm using Jeweller protocol.

No connections to the peripherals' identification codes were noticed inside the data captured by URH. Pictures collected by PIR camera are sent using Wings protocol. Differences within strength and channel usage duration compared to Jeweller can be seen in Figure 50. The Jeweller works properly on top of the Wings. Wings is used for larger data amounts and Jeweller for quicker sessions and over longer distances. Deeper protocol analyze is left for the future works.

4.7.1.2 Reed switch

"Ajax DoorProtect Jeweller" reed switch signals were collected and tried to replay, but without success. Firmware of the reed switch was EU 5.57.0.39. When looking into the signals it was possible to see that the beginning of the signal was the same for addressing prefixes, but all the rest were different every time. Approximately 20 signals were collected and none of them was able to trigger the false alarm.

4.7.1.3 Keyfob

The Ajax keyfob "SpaceControl Jeweller" had four buttons and it was simple to use. It was possible to control some of the keyfob settings over mobile application like panic and accidental push protection. It used firmware EU 5.54.1.5. Ajax keyfob used two frequency channels: 868,065MHz - 868,165MHz and 868,465MHz - 868,565 MHz as shown in Figure 51. Channel bandwidth was 100kHz.

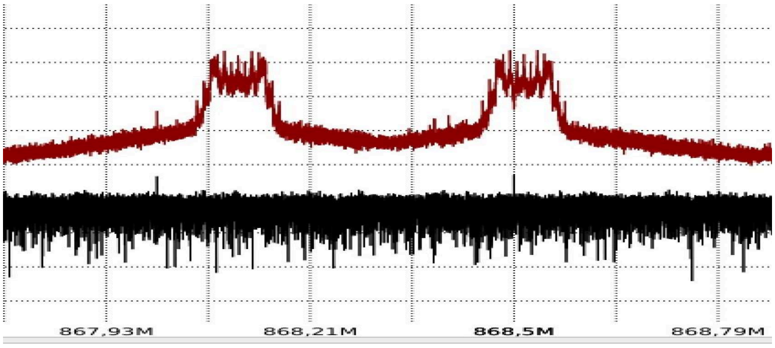
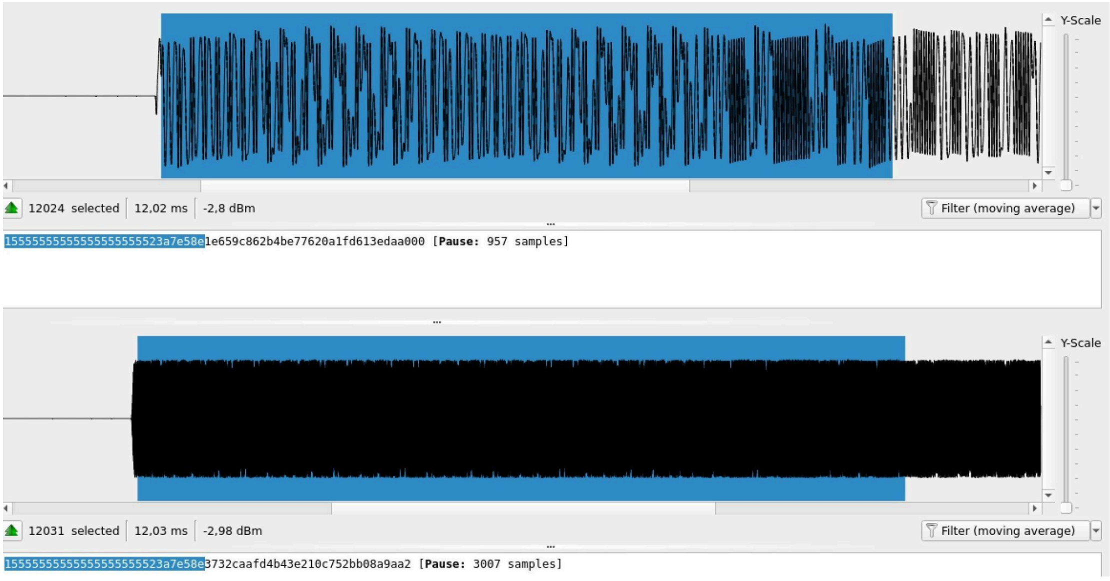


Figure 51. Ajax keyfob used only two frequency channels over 60 pushes tryout.

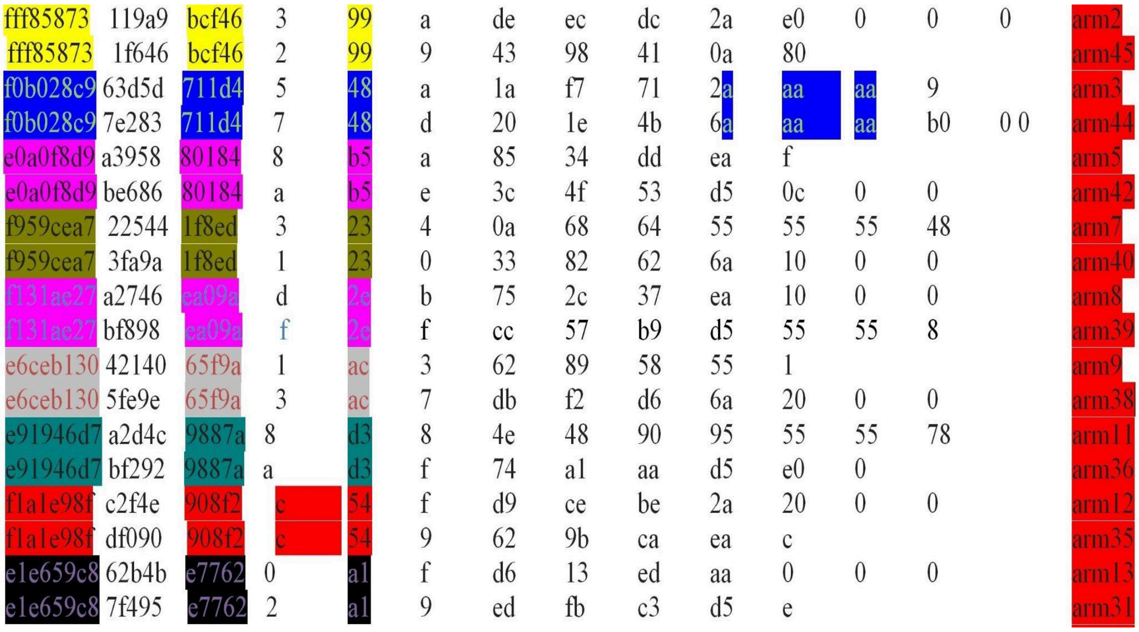
The keyfob was tested like all other ones with signal collection over HackRF and URH and looking at HEX format to simplify analysing, but as no visual indications of similarity occurred over several samples and the replay attack did not work, then more samples were collected. It was tried to see if there is any repetition at all or not. It was noticed that signals sent by keyfob were different from time to time - their length and modulation frequency seemed different, as can be seen from Figure 52 downwards.



```
12024  selected | 12,02 ms | -2,8 dBm
1555555555555555555555523a7e58e1e659c862b4be77620a1fd613edaa000 [Pause: 957 samples]

12031  selected | 12,03 ms | -2,98 dBm
1555555555555555555555523a7e58e3732caafd4b43e210c752bb08a9aa2 [Pause: 3007 samples]
```

Figure 52. Ajax keyfob arming using different style signaling with same start addressing according to URH.



fff85873	119a9	bcf46	3	99	a	de	ec	dc	2a	e0	0	0	0	arm2
fff85873	1f646	bcf46	2	99	9	43	98	41	0a	80				arm45
f0b028c9	63d5d	711d4	5	48	a	1a	f7	71	2a	aa	aa	9		arm3
f0b028c9	7e283	711d4	7	48	d	20	1e	4b	6a	aa	aa	b0	0 0	arm44
e0a0f8d9	a3958	80184	8	b5	a	85	34	dd	ea	f				arm5
e0a0f8d9	be686	80184	a	b5	e	3c	4f	53	d5	0c	0	0		arm42
f959cea7	22544	1f8ed	3	23	4	0a	68	64	55	55	55	48		arm7
f959cea7	3fa9a	1f8ed	1	23	0	33	82	62	6a	10	0	0		arm40
f131ae27	a2746	ea09a	d	2e	b	75	2c	37	ea	10	0	0		arm8
f131ae27	bf898	ea09a	f	2e	f	cc	57	b9	d5	55	55	8		arm39
e6ceb130	42140	65f9a	1	ac	3	62	89	58	55	1				arm9
e6ceb130	5fe9e	65f9a	3	ac	7	db	f2	d6	6a	20	0	0		arm38
e91946d7	a2d4c	9887a	8	d3	8	4e	48	90	95	55	55	78		arm11
e91946d7	bf292	9887a	a	d3	f	74	a1	aa	d5	e0	0			arm36
f1a1e98f	c2f4e	908f2	c	54	f	d9	ce	be	2a	20	0	0		arm12
f1a1e98f	df090	908f2	c	54	9	62	9b	ca	ea	c				arm35
e1e659c8	62b4b	e7762	0	a1	f	d6	13	ed	aa	0	0	0		arm13
e1e659c8	7f495	e7762	2	a1	9	ed	fb	c3	d5	e				arm31

Figure 53. Ajax keyfob arming signals similarities in HEX without prefix.

Some similarities found on keyfob arming signals can be seen on upper Figure 53. Strange repetition was found between signals collected in a way where arming signals arm1 vs arm46; arm2 vs arm45; arm3 vs arm44; arm5 vs arm42; arm7 vs arm40; arm8 vs arm39; arm9 vs arm38; arm11 vs arm36; arm12 vs arm35; arm13 vs arm 31 contained partly same information. It was possible to notice regularity from upper signal numbering. Between some samples like arm4 vs arm43 or arm10 vs arm37 to have logical order, we did not find similarities, but those were problematic samples detected within arm4 and arm10 signals.In total some similarity exists within a possible regular sequence, but even then about 20 HEX symbols are different, meaning no chance for actual bruteforce attack.

4.7.1.4 Keypad

"Ajax KeyPad Plus Jeweller" used firmware EU 5.57.4.9. In the application it was possible to switch on and off RFID reader, enable automatic locking when wrong code entered and use duress code. It showed temperature and battery level and lid status together with Jeweller signal level indication in the application. Ajax keypad signals were using FSK according to URH autodetect.

Code 3333 arming and disarming signals example in HEX format recorded by URH:

```
Arm7:     f5555555555555555555591d3 efc7  5aa79a91ad1ce3465ec4fdee00817dcb7cdf8
Disarm7:  f5555555555555555555591d3 efc7  9c9d266aee5e5d3e257abd93fb3e05af4b7f8
```

It was seen that signal length varied over samples and there are some similarities, but as with keyfob disarming signals, randomness is too big. At least 34 HEX symbols were changing with every signal. It takes a much bigger dataset combined with machine learning to analyse this more deeply.This is left out of scope of this thesis.

4.7.2 Interference testing

General RF channel for sensors

System detects high noise floor on Jewellers frequencies 868,0- 868,6 and informs over application. Also informs when the situation has been normalised. Notifications in application normally occur within 15-30 seconds after environment change. It is confirmed that the Ajax system can detect jamming and notifies the user within seconds.

Wi-Fi channel for notification

If a system's Wi-Fi channel is disturbed while only Wi-Fi being used to communicate with the server then the system notifies after a certain preset time that: “Central units connection with server over Wi-Fi has been disconnected” and “Central unit is not in network – control its Internet connection” (translation from Estonian language). After stopping disturbance, messages about reconnecting are received in application together with all the happenings meanwhile. But it is important that the timestamp on these messages is not the original one when action really happened but the minute when the info has reached the server. This means that if the connection has been cut then all messages lose their timestamp and it would be hard to verify when exactly something happened. Wi-Fi channel disturbance is detected in about 10 seconds from close range interference and about 40 seconds later application notifies from server side that connection has been dropped. Network returns within 3-4 seconds after the disturbance has been stopped. As the notification channel itself is problematic then it is vital to have a quick response from the cloud side. Compared to the cheap Chinese systems which were used with a “Smart Life” application which sent notification after half an hour the Ajax reacted still under a minute - giving less time for criminals and more time for people to react to the situation.

4.8 RFID cloning attacks

In Figure 54 tags from seven systems supporting RFID are represented together with a red MIFARE tag bought from LAB401 [44]. Three Tecpeak systems; two PGST systems; Ajax and Hikvision systems. DSC system software supported RFID tags but hardware was not available to us. Jablotron; Paradox; Yale; G-Homa and the PGST PW150 unit did not have native support for the RFID.

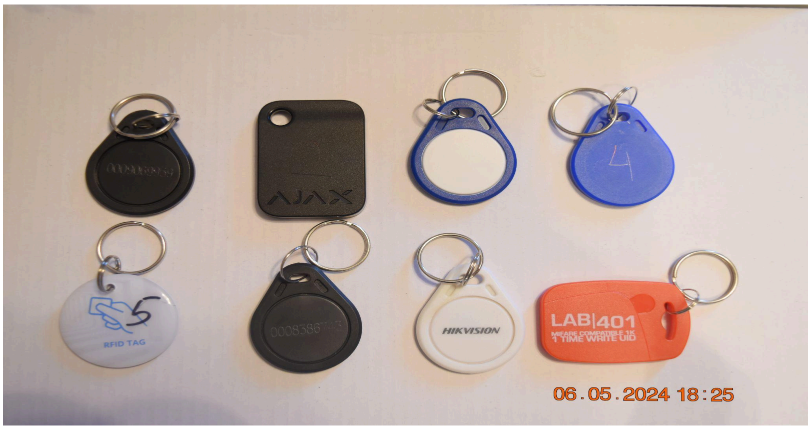
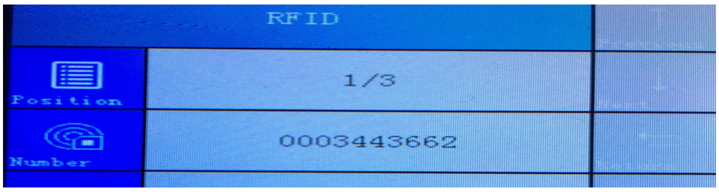


Figure 54. Tags used by alarm systems together with “MIFARE 1 TIME WRITE UID”.

PGST and Tecpeak systems used low frequency 125kHz tags. Hikvision used MIFARE Classic 1K high frequency tag and Ajax used DESFire EV1 2k high frequency tag.

Few of the tags used by PGST had a number on them that was used inside the system to register the tag. This was the decimal tag ID number from DEZ 10 field. But even the ones that did not have numbers written on them were using the same mechanism. Chinese systems provided open info about their tag numbering as seen in Figure 55.



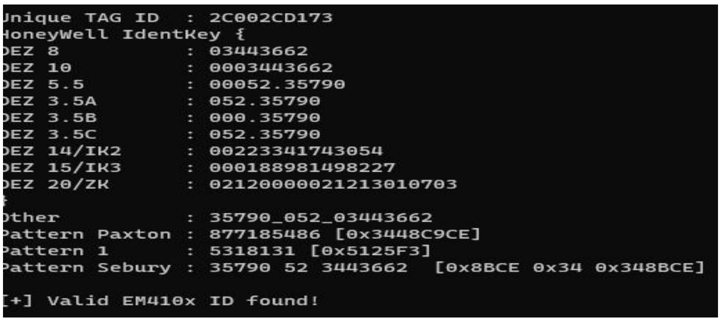
RFID

Position 1/3

Number 0003443662

Figure 55. Tag number reading from Tecpeak system RFID section.

Same tags were read with Proxmark3 to see if something extra will be found. Figure 56 shows a Proxmark3 terminal reading from the same tag as on upper Figure 55.



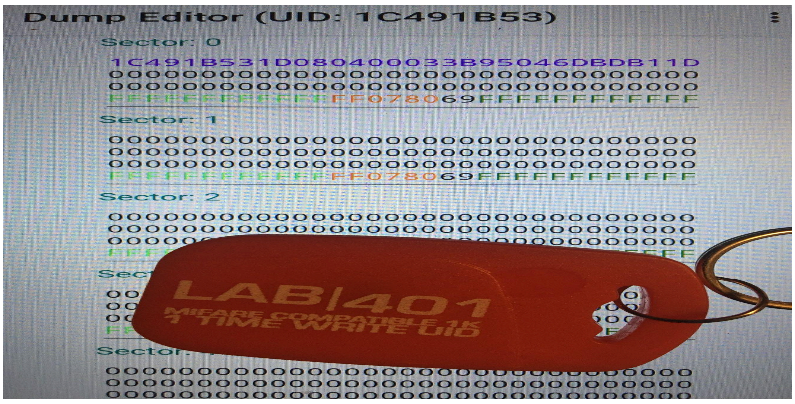
```
Unique TAG ID   : 2C002CD173
HoneyWell IdentKey {
DEZ 8           : 03443662
DEZ 10          : 0003443662
DEZ 5.5         : 00052.35790
DEZ 3.5A        : 052.35790
DEZ 3.5B        : 000.35790
DEZ 3.5C        : 052.35790
DEZ 14/IK2      : 00223341743054
DEZ 15/IK3      : 000188981498227
DEZ 20/ZK       : 02120000021213010703
}
Other           : 35790_052_03443662
Pattern Paxton  : 877185486 [0x3448C9CE]
Pattern 1       : 5318131 [0x5125F3]
Pattern Sebury  : 35790 52 3443662  [0x8BCE 0x34 0x348BCE]

[+] Valid EM410x ID found!
```

Figure 56. Tecpeak tag readout with Proxmark3 “lf search” command.

PGST and Tecpeak tags were tried to clone with ICopy-XS. It was possible to clone the tags and use the new clones with the systems.

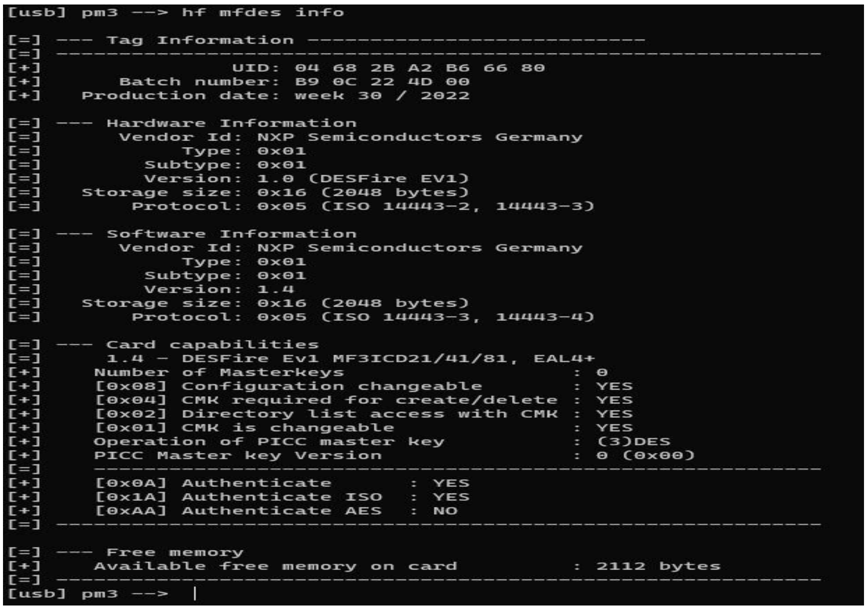
As Hikvision used MIFARE Classic 1k tag then it is known as a product that you may clone with proper tools. Products purchased from LAB401 were used in that test and with success. This shows clearly that the HIKVISION system is not secure to use when only a chip is used as an authentication measure to arm or disarm the system. It is necessary to use it with two level authentication where the system also asks for determined code assigned to that user together with that smart card or token. Nevertheless it might not be the case how people use the system. By default settings this two level authentication is not mandatory nor applied but seemingly as an extra measure to some bigger companies or extraordinary users who think that they need some extra level of protection. A MIFARE clone tag, shown in Figure 57, was created with one time write UID successfully and used without problems together with Hikvision keypad. An UID: 1C491B53 was read by Mifare Classic Tool - same as Hikvision original tag. All the keys for the Hikvision tag were filled with F's. No real keys were being used. All sectors from 1-16 were empty but sector 0 with UID. The Hikvision system used only UID info to verify tags in the system.



```
Dump Editor (UID: 1C491B53)
  Sector: 0
    1C491B531D080400033B95046DBDB11D
    00000000000000000000000000000000
    00000000000000000000000000000000
    FFFFFFFFFFFFFF078069FFFFFFFFFFFF
  Sector: 1
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    FFFFFFFFFFFFFF078069FFFFFFFFFFFF
  Sector: 2
    00000000000000000000000000000000
    00000000000000000000000000000000
```

Figure 57. Cloned UID from Hikvision tag.

Ajax tags are DESFire EV1. Tests to clone these tags successfully for the Ajax system to accept the clone were conducted with ICopy-XS but were not successful.



```
[usb] pm3 --> hf mfdes info

[=] --- Tag Information ---------------------------
[=] -------------------------------------------------------------
[+]                UID: 04 68 2B A2 B6 66 80
[+]       Batch number: B9 0C 22 4D 00
[+]    Production date: week 30 / 2022

[=] --- Hardware Information
[=]      Vendor Id: NXP Semiconductors Germany
[=]           Type: 0x01
[=]        Subtype: 0x01
[=]        Version: 1.0 (DESFire EV1)
[=]   Storage size: 0x16 (2048 bytes)
[=]       Protocol: 0x05 (ISO 14443-2, 14443-3)

[=] --- Software Information
[=]      Vendor Id: NXP Semiconductors Germany
[=]           Type: 0x01
[=]        Subtype: 0x01
[=]        Version: 1.4
[=]   Storage size: 0x16 (2048 bytes)
[=]       Protocol: 0x05 (ISO 14443-3, 14443-4)

[=] --- Card capabilities
[=]     1.4 - DESFire Ev1 MF3ICD21/41/81, EAL4+
[+]    Number of Masterkeys                    : 0
[+]    [0x08] Configuration changeable         : YES
[+]    [0x04] CMK required for create/delete   : YES
[+]    [0x02] Directory list access with CMK   : YES
[+]    [0x01] CMK is changeable                : YES
[+]    Operation of PICC master key            : (3)DES
[+]    PICC Master key Version                 : 0 (0x00)
[=]    ---------------------------------------------------------
[+]    [0x0A] Authenticate      : YES
[+]    [0x1A] Authenticate ISO  : YES
[+]    [0xAA] Authenticate AES  : NO
[=] -------------------------------------------------------------

[=] --- Free memory
[+]    Available free memory on card          : 2112 bytes
[=] -------------------------------------------------------------
[usb] pm3 -->  |
```

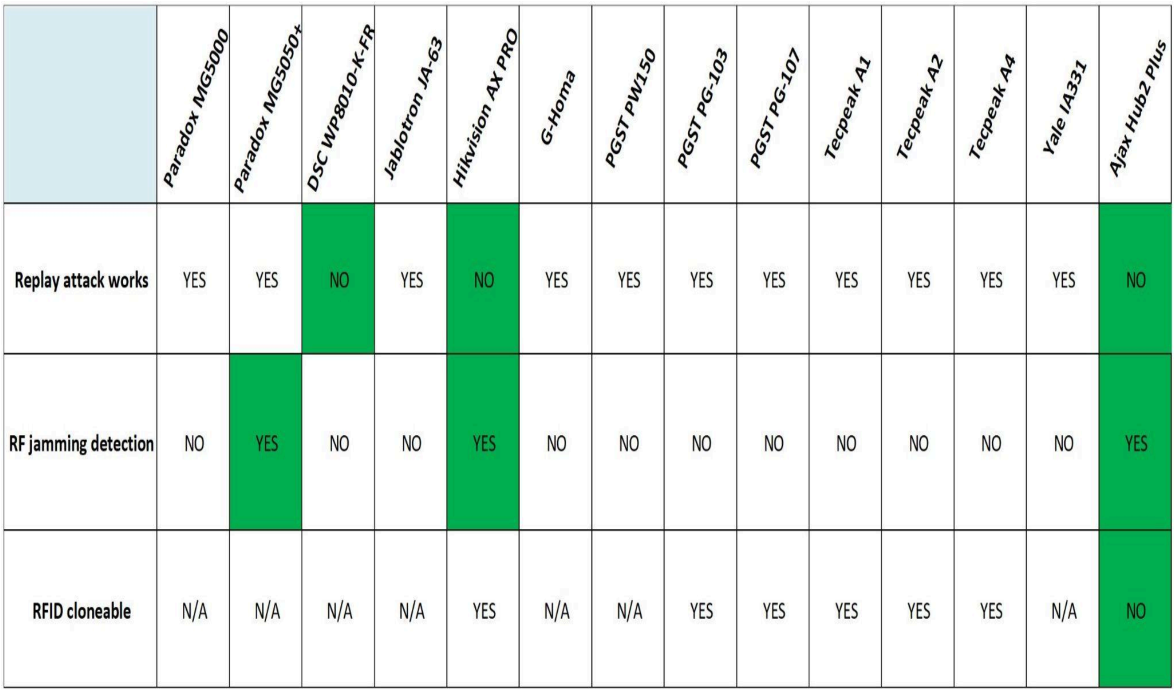
Figure 58. Ajax DESFire EV1 tag readout with Proxmark3.

It can be seen from Figure 58 that the tag is produced in week 30 of 2022 and AES is not in use. Also seems that the default factory master key is in use. If the same tag was read with Android smartphone application "NFC Taginfo by NXP" it was possible to see that there was 1 unknown DESFire application 0x4DA801in tag memory with ID 0x01A84D and with it the AES master key was actually used. As our goal was to test if these tags are quickly cloneable with commercial off-the-shelf tools openly available to everyone any deeper analyze was left out of the scope of this thesis.

5 Summary and recommendations

In this research 14 different wireless security alarm systems purchased from the Estonian market were tested and their responses to RF signal replay attacks; interference detection and RFID tags cloning were assessed.

Table 1. Summary of conducted tests results



	Paradox MG5000	Paradox MG5050+	DSC WP8010-K-FR	Jablotron JA-63	Hikvision AX PRO	G-Homa	PGST PW150	PGST PG-103	PGST PG-107	Tecpeak A1	Tecpeak A2	Tecpeak A4	Yale IA331	Ajax Hub2 Plus
Replay attack works	YES	YES	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES	NO
RF jamming detection	NO	YES	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO	YES
RFID cloneable	N/A	N/A	N/A	N/A	YES	N/A	N/A	YES	YES	YES	YES	YES	N/A	NO

As shown in Table 1, Ajax Hub2 Plus survived all our tests. Hikvision AX PRO was left in second place as it used simply cloneable RFID tags and identification based on UID only. Older and cheaper systems were suffering more problems and were quite easily attackable. We proved that many systems sold in Estonia suffer in lack of security themselves.

The Ajax and Hikvision systems were the most modern ones which both had good application and cloud support with regular online updates. Paradox MG5050+ with KL38 keypad was a disappointment in general as it was hoped that the replay attack problem that was detected in the older MG5000 version would have been addressed but unfortunately not. It was thought that cheap Chinese products cannot compete with expensive brand products but it was surprising how easy it was to attack them. It was proven that choosing cheap Chinese products is not the safest way to go.

As a result of our testing, it can be said that it is very important to understand vulnerabilities and weaknesses of wireless security alarm systems. Without understanding systems real capabilities, one can find systems not functioning properly at a critical moment. People answering the questionnaires also agreed that the subject is important and many were glad that they got a new perspective. Our goal to inform about possible threats was achieved.

The questionnaire gave logical and adequate feedback about the situation in Estonia concerning wireless security alarm systems. It clearly stated the importance of wireless technology used within security alarm systems. It was verified that almost half of the people are not familiar with replay, jamming and cloning attacks and most of the alarm system users are not sure if their system is secured against these attacks or not. Many system users would like to have consultation and are worried about their system security.

Same time, people not using alarm systems evaluate their security awareness above average most of the time and claim that they do not need an alarm system because they feel safe as they are. If all providers claimed that they always inform clients about vulnerabilities and weaknesses during the purchase process and 40% also said that they are also informing clients afterwards then 70% of people have not actually experienced any of that.

In total 20% of alarm system owners have had actual problems with intruders. In half cases the security alarm system was useful and in other half cases it did not stop burglary. It is obvious that people and situations are different and security alarm systems are purchased only if one feels the necessity. Questionnaire showed that a lot of systems are quite old and people do not know how to update them. Nevertheless it is wise to maintain and update or even upgrade the system once and a while if real protection and good security level is needed. Otherwise there is a high chance to become a member of that 10% club of the alarm system owners who later become victims of their own false sense of security.

If a specific question is raised about replay, jamming or cloning attacks then actual lack of knowledge and uncertainty was clear. Researchers should find a way how their knowledge could reach the general public in a better way to raise knowledge so that their work would have an even bigger effect.

In future other wireless systems are going to be added to our work and a bigger focus will be set also on Wi-Fi protocol parts to see if replays can be generated this way. Our goal in future would be to fool the cloud-server side so it would think that the security alarm is still up and running while it is actually offline.

From the manufacturing side it was interesting to notice how keeping dataset start and end far away from each other in time scale can make brute forcing attack impractical. From Paradox examples it was seen that obfuscation is not going to protect against replay attacks. Also simple 4 or 5 time sequencing of the code that was used with some keyfobs is not enough to protect replays. Frequency hopping is a good tool against simple replay attackers who cannot change transmitter frequency in a timely manner but it cannot be promoted as a measure to avoid jamming, because with a wider bandwidth interference signal all hopping is covered in these 433MHz and 868MHz narrow bands.

Recommendations

It is recommended that one should never buy a used alarm system. Alarm systems should be bought from a reliable vendor, comply with newest standards and installed by professionals. It is reasonable to have a security service contract. It is important to make sure that the system is not vulnerable and is tested accordingly and configured properly. Otherwise a simple few € tag can make a difference. It is vital to understand that the system cannot inform you about the situation when the notification channel is blocked. Even if systems can detect jamming then it is not enough if there is no other means of communicating while the only channel is already blocked. Wireless systems are and will most likely stay vulnerable to jamming attacks - so it is important to have many different notification channels and possibly also have a non wireless medium for transferring data. A cloud side reporting of an offline system and system sensors with memory are good properties to have. Security should be provided with many overlapping layers and the alarm system is only one part of it in general. It is always a good practice to have physically secure entrance points and an extra layer of video surveillance is also a good preventive measure.

References

1. Nisbet, A., & Kim, M. (2013). Security analyze and forensic investigation of home & commercial alarm systems in New Zealand: Current research findings. *Australian Digital Forensic Conference*. https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1123&context=adf

2. Lindeberg, A. (2021). Hacking into someone's home using radio waves: Ethical hacking of Securitas' alarm system (Master's thesis). https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1600180&dswid=-4196

3. Lamb, L. (2017). Home insecurity: No alarms, false alarms, and SIGINT. *Whitepaper*. https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEFCON-25-Logan-Lamb-Home-Insecurity-No-Alarms-False-Alarms-and-SIGINT-WP.pdf

4. Hamid, L. E., & Möller, S. (2020). How secure is Verisure's alarm system? (Degree project). https://www.diva-portal.org/smash/get/diva2:1556774/FULLTEXT01.pdf

5. Fabian, D. (2019). Examination of LUPUS-Electronics devices. *Embedded Lab Vienna for IoT & Security*. https://elvis.science/examination-of-lupus-electronics-devices

6. van Diermen, R. (2018). The internet of things: A privacy label for IoT products in a consumer market (Master's thesis). https://hdl.handle.net/1887/64571

7. Ringvall, L., & Ekholm, O. (2020). Penetration testing of GSM alarm: Using radio frequency communication (Bachelor's study). https://www.diva-portal.org/smash/get/diva2:1464511/FULLTEXT01.pdf

8. CTV News. (n.d.). A video from CTV News - a Canadian news broadcast story about vulnerable security alarm systems [Video]. YouTube. https://www.youtube.com/watch?v=d6dNUExl_d0

9. Washington TV Channels. (n.d.). A video on Washington TV channels about vulnerable security systems [Video]. YouTube. https://www.youtube.com/watch?v=poMdC22s6sE

10. Grigutytė, M. (2024, February 12). Ring hacked: Doorbell and camera security issues. *NordVPN*. https://nordvpn.com/blog/ring-doorbell-hack/

11. Fernández-Caramés, T. M., Fraga-Lamas, P., Suárez-Albela, M., & Castedo, L. (2017). Radio frequency identification. In *A methodology for evaluating security in commercial RFID systems*. IntechOpen. https://www.intechopen.com/chapters/52083

12. Morgan, D. M. (2017). Security of loyalty cards used in Estonia (Master's thesis). https://kodu.ut.ee/~arnis/loyalty_thesis.pdf

13. Pistorius, L., Polster, H., & Labudde, D. (2023). Relay station attacks on different RFID access systems. *2023 Smart Systems Integration Conference and Exhibition (SSI)*, Brugge, Belgium, 1-6. https://ieeexplore.ieee.org/document/10387965

14. Mackiewicz, A. (2020). What type of RFID cards can be easily cloned by hardware available on the market? (Master's thesis). National College of Ireland. https://norma.ncirl.ie/4524/1/andrzejmackiewicz.pdf

15. Postimees. (n.d.). Break-ins wave. Thieves are entering without signs. https://kodu.postimees.ee/7897839/sissemurdmiste-laine-vargad-sisenevad-jalgi-jatmata

16. Ministry of Justice. (2023). Statistics of thefts in Estonia. https://www.just.ee/kuritegevus2023/

17. Acumen Research and Consulting. (n.d.). Estimation of market growth for security alarm systems. https://www.acumenresearchandconsulting.com/home-security-system-market

18. Dun & Bradstreet. (2024, February 12). First research: Security system services industry profile. https://www.firstresearch.com/Industry-Research/Security-System-Services.html

19. KV.ee. (n.d.). New apartment sale advertisement. https://www.kv.ee/igal-neljapaeval-kell-11001300-on-maakler-majas-tu-3621097.html

20. Simply Psychology. (n.d.). Safety and security, in general, are on level 2 in Maslow's hierarchy of needs pyramid. https://www.simplypsychology.org/maslow.html

21. SDM Magazine. (2021, May). Overview of security companies annual revenue. https://www.sdmmag.com/ext/resources/Issues/2021/May/SDM-100/tables/SDM100-tables.pdf

22. Postimees. (n.d.). Break-in victim shop owner: Incomers do not need food and drinks - only money. https://jarvateataja.postimees.ee/7926410/sissemurdmiste-ohvriks-langenud-poepidaja-tulijatel-ei-ole-vaja-suua-juua-ainult-raha

23. ERR. (2024, March). Burglaries in Estonia, according to Police captain Inna Toater. Screenshot of Inna Toater's interview. *Terevisioon*. https://jupiter.err.ee/1609282535/terevisioon

24. Weidman, G. (2014). *Penetration testing: A hands-on introduction to hacking*. Google Books. https://books.google.com/books?id=rEFPDwAAQBAJ&pg=PP1

25. Guzman, A., & Gupta, A. (2017). *IoT penetration testing cookbook: Identify vulnerabilities and secure your smart devices*. Google Books. https://books.google.com/books?id=rEFPDwAAQBAJ&pg=PP1

26. OWASP Foundation. (2018). OWASP IoT top 10 - 2018. *Tech. Rep.* https://owasp.org/www-project-internet-of-things/OWASP-IoT-Top-10-2018-final.pdf

27. White, W. F. (1999). Plutonium Finishing Plant (PFP) criticality alarm system commercial grade item (CGI) critical characteristics. https://www.iaea.org/sites/default/files/34009270.pdf

28. YouTube. (n.d.). Top 5 BEST home security systems of 2023 [Video]. https://www.youtube.com/watch?v=h0aP_xeVvm0

29. Sunvis Store. (n.d.). Typical home security alarm system (Figure 3). https://www.sunvisstore.co.uk/ring-12pc-alarm-starter-kit-including-outdoor-siren-with-indoor-camera-5253-p.asp

30. Activate Me Tech. (n.d.). Hikvision AX PRO's typical components (Figure 4). https://www.activateme.tech/shop/hikvision-64-zone-wireless-alarm-control-panel/

31. Schneier, B. (1999). Attack tree. https://www.schneier.com/academic/archives/1999/12/attack_trees.html

32. Megateh.ee. (n.d.). AIKO starter kit at Megateh.ee webshop. https://www.megateh.ee/tooted/ajax-juhtmevaba-valvesusteem-ja-targakodu-susteemid-starterkit/ajax-black-starterkit-plus-hub-plus-motion-door-space

33. G4S Estonia. (n.d.). AIKO service with Ajax kit by G4S in Estonia. https://kampaania.g4s.ee/aiko/et

34. Estonian Government. (n.d.). Estonian Radio Frequency Plan. https://www.riigiteataja.ee/aktilisa/1011/2202/3008/MKM_m65_lisa1.pdf

35. Estonian Government. (2019). Conditions for the use of radio frequencies and technical requirements for radio equipment exempted from frequency licence. https://www.riigiteataja.ee/akt/126022019014?leiaKehtiv

36. Estonian Government. (2020). Estonian Electronic Communication Law. https://www.riigiteataja.ee/akt/120052020034?leiaKehtiv

37. Estonian Government. (2020). Limiting radio communications. https://www.riigiteataja.ee/akt/126052020007

38. Estonian Government. (2024). Estonian Penal Code. https://www.riigiteataja.ee/en/eli/508042024002/consolide

39. Alibaba. (n.d.). 12 channels wifi GSM CDMA 2G jammer. https://www.alibaba.com/product-detail/12-channels-wifi-GSM-CDMA-2G_1600692277888.html

40. YouTube. (n.d.). RF Jamming Demo video about using SDR. https://www.youtube.com/watch?v=LSURTmn_JLs

41. PentHertz. (n.d.). Modmobjam: A special tool for jamming mobile communications with SDR. https://github.com/PentHertz/Modmobjam

42. Jhonnybonny. (n.d.). CleverJAM: Github project. https://github.com/jhonnybonny/CleverJAM

43. Rantelon. (n.d.). Rantelon 20W per band KJ-CaseL jammer. https://rantelon.ee/wp-content/uploads/2021/12/KJ-CaseL.pdf

44. LAB401. (n.d.). LAB401 website. https://lab401.com/collections/all-products

45. BBC News. (2023). Hikvision spying in Western countries. https://www.bbc.com/news/world-asia-china-65307503

46. Alibaba. (n.d.). 433MHz jammer. https://www.alibaba.com/product-detail/OEM433MHZ-wireless-communication-transmission-drone-jammer_1600899250442.html

47. Ajax Systems. (n.d.). The Ajax factory location in Ukraine. https://ajax.systems/company-history/

48. Ajax Systems. (n.d.). Ajax Jeweller and Wings protocol. https://ajax.systems/radio-range/

Appendix I - Questionnaire questions

Questionnaire questions were written in capital letters to provide better readability.

I DO NOT USE SECURITY ALARM SYSTEM

https://s.surveyplanet.com/u3mvxcxd

1) WHAT IS YOUR AGE ?
2) IN WHICH COUNTY DO YOU LIVE?
3) DO YOU LIVE IN A CITY OR IN THE COUNTRYSIDE?
4) DO YOU LIVE IN AN APARTMENT OR IN A HOUSE?
5) HOW DO YOU ASSESS YOUR KNOWLEDGE ABOUT SECURITY IN GENERAL?
6) WHAT ARE THE REASONS WHY YOU DO NOT USE A SECURITY ALARM SYSTEM?
7) HOW DO YOU PROTECT YOUR HOME AND OFFICE?
8) CAN YOU SHARE AN IDEA HOW TO BE PROTECTED AND SAFE WITHOUT HAVING A SECURITY ALARM SYSTEM OR PAID SERVICE?
9) DO YOU THINK THAT HAVING A SECURITY ALARM SYSTEM WOULD RAISE YOUR SENSE OF SECURITY?
10) HAVE YOU EVER CONSIDERED OF PURCHASING A MODERN SECURITY ALARM SYSTEM?
11) ARE YOU AWARE OF DIFFERENT NEW SECURITY SOLUTIONS AVAILABLE ON THE MARKET?
12) PLEASE MARK WHAT ALARM SYSTEM PROPERTIES SEEM IMPORTANT TO HAVE?
13) WOULD YOU CARE WHERE THE SYSTEM HAS BEEN MANUFACTURED?
14) WOULD YOU PURCHASE AND INSTALL THE SYSTEM YOURSELF OR WOULD YOU TRUST PROFESSIONALS TO HANDLE IT?
15) HOW MUCH ARE YOU WILLING TO PAY FOR SECURITY COMPANY SERVICE MONTHLY(€) ?
16) HOW MUCH ARE YOU WILLING TO SPEND ON A SECURITY ALARM SYSTEM (€)?
17) HAVE YOU HEARD ABOUT WIRELESS SECURITY ALARM SYSTEMS ?
18) IF/WHEN YOU GET A NEW SECURITY ALARM SYSTEM WOULD YOU PREFER WIRELESS OR WIRED ONE?
19) WOULD YOU LIKE TO USE YOUR SMARTPHONE TO CONTROL YOUR SECURITY ALARM SYSTEM?
20) DO YOU USE A CHIP CARD OR PHYSICAL TOKEN TO GET ACCESS TO PREMISES?
21) ARE YOU AWARE OF DIFFERENT ATTACKS AGAINST SECURITY ALARM SYSTEMS?
22) HAVE YOU EVER HEARD ABOUT REPLAY ATTACKS?
23) HAVE YOU EVER HEARD ABOUT RADIO JAMMING ATTACKS?
24) HAVE YOU EVER HEARD ABOUT CHIP CARD OR TOKEN CLONING ATTACKS?
25) HAVE YOU EVER HAD AN INCIDENT THAT COULD HAVE BEEN POSSIBLY AVOIDED IF A PROPER SECURITY ALARM SYSTEM HAD BEEN IN PLACE?
26) COMMENT FREELY CURRENT SURVEY!

WIRELESS ALARM SYSTEMS SECURITY (USER VERSION)

https://s.surveyplanet.com/nuqy3c1i

1) WHAT IS YOUR AGE?
2) IN WHICH COUNTY IS YOUR ALARM SYSTEM LOCATED?
3) DO YOU LIVE IN A CITY OR IN THE COUNTRYSIDE?
4) DO YOU LIVE IN AN APARTMENT OR IN A HOUSE?
5) HAVE YOU NOTICED AN INCREASE IN WIRELESS PRODUCTS AROUND YOU DURING LAST YEARS?
6) WHAT KIND OF SECURITY ALARM SYSTEM DO YOU USE?
7) MY SYSTEM HAS: (different functions and options to choose from)
8) HOW OLD IS YOUR SYSTEM?
9) DO YOU USE SERVICE PROVIDER SYSTEM AND HAVE ACTIVE CONTRACT OR DO YOU MANAGE SYSTEM INDEPENDENTLY?
10) HOW OFTEN DO YOU MAINTAIN OR SERVICE YOUR SYSTEM?
11) DO YOU KNOW WHERE YOUR SECURITY ALARM SYSTEM IS MANUFACTURED?
12) WHAT INFLUENCED YOUR DECISION WHILE CHOOSING SECURITY ALARM SYSTEM?
13) HAVE YOU EVER THOUGHT ABOUT THE SECURITY OF THE ALARM SYSTEM ITSELF?

14) HOW DO YOU ASSESS YOUR KNOWLEDGE ABOUT ALARM SYSTEMS SECURITY?
15) ARE YOU AWARE OF THE SECURITY LEVEL OR GRADE OF YOUR ALARM SYSTEM?
16) DO YOU THINK THE MORE EXPENSIVE BRAND SYSTEMS BETTER SECURITY LEVEL IS REALLY PERCEIVED COMPARED TO CHEAP CHINESE ONES?
17) DO YOU USE A SMARTPHONE APP TO CONTROL THE ALARM SYSTEM?
18) DO YOU USE SMS MESSAGES OR MOBILE PHONE CALLS TO CONTROL YOUR ALARM SYSTEM?
19) DO YOU THINK THAT CLOUD SOLUTIONS INCREASE OR DECREASE ALARM SYSTEMS SECURITY?
20) IS YOUR ALARM SYSTEM CONNECTED TO SOME OTHER INTERNET DEVICE? FOR EXAMPLE WITH SOME SMART HOME CENTER OR AMAZON ECHO, ALEXA OR WITH OTHER SIMILAR “IoT” DEVICE?
21) IN YOUR OPINION ARE WIRELESS SECURITY ALARM SYSTEMS EASIER TO ATTACK OR NOT?
22) WHAT ALARM NOTIFICATION CHANNEL IS USED BY YOUR ALARM SYSTEM?
23) HOW IS YOUR ALARM SYSTEM FIRMWARE AND SOFTWARE UPDATING ORGANIZED?
24) HAS MANUFACTURER OR SERVICE PROVIDER EVER INFORMED YOU ABOUT YOUR SYSTEM VULNERABILITIES OR WEAKNESSES?
25) IS YOUR SYSTEM PROTECTED AGAINST REPLAY ATTACKS?
26) IS YOUR SYSTEM PROTECTED AGAINST RADIO JAMMING ATTACKS?
27) IS YOUR SYSTEM PROTECTED AGAINST CHIPCARD OR TOKEN CLONING ATTACKS?
28) HAVE YOU EVER EXPERIENCED ALARM SYSTEM ANOMALIES? FOR EXAMPLE RADIO INTERFERENCE OR OTHER NOT UNDERSTANDABLE UNUSUAL SITUATIONS?
29) HOW DO YOU USUALLY ACT IN CASE OF ANOMALY OR SYSTEM FAILURE?
30) WOULD YOU PURCHASE SOME OTHER SECURITY ALARM SYSTEM INSTEAD IF YOU COULD?
31) HAVE YOU EVER HAD AN INCIDENT WHERE SECURITY ALARM SYSTEM HAS PROVEN ITS VALUE IN PRACTICE?
32) ARE YOU CONVINCED THAT YOUR SECURITY ALARM SYSTEM IS ACTUALLY SECURE?
33) COMMENT FREELY CURRENT SURVEY!

WIRELESS ALARM SYSTEMS SECURITY (PROVIDER VERSION)

https://s.surveyplanet.com/hhib73t5

1) HAVE YOU NOTICED AN INCREASE OF WIRELESS PRODUCTS IN SECURITY ALARM SYSTEMS MARKET IN THE LAST FEW YEARS?
2) HAVE YOU NOTICED THE GROWTH OF CHEAP “MADE IN CHINA” SYSTEMS IN THE MARKET IN RECENT YEARS?
3) NAME THE MOST POPULAR WIRELESS SECURITY ALARM SYSTEM YOU PROVIDE?
4) WHAT MAKES THIS SYSTEM PREFERRED BY CLIENTS?
5) WHAT IS THE MARKET SHARE % OF WIRELESS SECURITY ALARM SYSTEMS COMPARED TO WIRE-BASED SYSTEMS?
6) ARE THE WIRELESS SECURITY ALARM SYSTEMS YOU PROVIDE MORE EXPENSIVE THAN THE WIRED ONES OR VICE VERSA?
7) WHICH SOLUTION WOULD YOU RECOMMEND TO YOUR CUSTOMERS AS THE MOST SECURE CHOICE OF ALL THE SECURITY ALARM SYSTEMS YOU PROVIDE TODAY?
8) DO YOU THINK THE MORE EXPENSIVE BRAND SYSTEMS BETTER SECURITY LEVEL IS REALLY PERCEIVED COMPARED TO CHEAP CHINESE ONES?
9) HOW DO YOU ASSESS YOUR CUSTOMERS AWARENESS REGARDING ALARM SYSTEMS SECURITY?
10) ARE YOU AWARE OF THE SECURITY LEVEL OF THE WIRELESS SECURITY ALARM SYSTEMS PROVIDED BY YOU?
11) WHAT SECURITY STANDARDS ARE APPLIED TO THE WIRELESS SECURITY SYSTEMS YOU PROVIDE?
12) DO YOU PROVIDE SECURITY ALARM SYSTEMS WITHOUT SMARTPHONE APP SUPPORT?
13) DO CLOUD SOLUTIONS INCREASE OR DECREASE SECURITY?
14) DO YOU PROVIDE SYSTEMS THAT ARE COMPATIBLE WITH OTHER INTERNET DEVICES? FOR EXAMPLE CONTROLLED BY USING SOME SMART-HOME HUB OR AMAZON ECHO, ALEXA OR A SIMILAR “IoT” PRODUCT?
15) DO YOU PROVIDE SYSTEMS WHAT CAN BE CONTROLLED BY SMS OR OVER MOBILE-PHONE CALL?
16) ARE CUSTOMERS USUALLY AWARE OF DIFFERENT ALARM NOTIFICATION CHANNELS?

17) ARE CUSTOMERS ASKING FOR SYSTEMS THAT SUPPORT SEVERAL DIFFERENT ALARM TRANSMISSION CHANNELS AT THE SAME TIME?
18) PLEASE SELECT MOST USED ALARM NOTIFICATION CHANNELS.
19) HOW ARE UPDATES OF FIRMWARE AND SOFTWARE ORGANIZED FOR THE SYSTEMS YOU PROVIDE?
20) HOW DO YOU VERIFY THE SECURITY OF PROVIDED SYSTEMS?
21) DO YOU INFORM THE CLIENT OF SYSTEM VULNERABILITIES/WEAKNESSES?
22) ARE WIRELESS SECURITY ALARM SYSTEMS EASIER TO ATTACK?
23) HAVE YOU NOTED OR HAVE CUSTOMERS EVER INFORMED YOU OF INCIDENTS OF RADIO INTERFERENCE IN WIRELESS SECURITY ALARM SYSTEMS?
24) ARE SYSTEMS YOU PROVIDE PROTECTED AGAINST REPLAY ATTACKS?
25) ARE SYSTEMS YOU PROVIDE PROTECTED AGAINST JAMMING ATTACKS?
26) DO THE SECURITY ALARM SYSTEMS PROVIDED BY YOU ALLOW THE USE OF A CHIP CARD OR TOKEN FOR AUTHENTICATION?
27) ARE YOU AWARE OF CHIP CLONING ATTACKS AND INFORM YOUR CLIENTS ABOUT IT?
28) ARE THE SYSTEMS PROVIDED BY YOU PROTECTED AGAINST CHIP CARD CLONING?
29) HOW MANY SECURITY ALARM SYSTEMS DO YOU APPROXIMATELY SELL IN A YEAR?
30) HOW MANY CUSTOMERS RELY ON SECURITY SERVICE PROVIDED BY YOU?
31) FEEL FREE TO COMMENT CURRENT SURVEY!

Estonian versions of questionnaires:

MA EI KASUTA VALVESÜSTEEMI: https://s.surveyplanet.com/cmhr4pf7

JUHTMEVABADE VALVESÜSTEEMIDE TURVALISUS (KASUTAJA VERSIOON): https://s.surveyplanet.com/48jhpg5v

JUHTMEVABADE VALVESÜSTEEMIDE TURVALISUS (TEENUSEPAKKUJA VERSIOON): https://s.surveyplanet.com/szkvwd5e

Appendix II - Information about tested systems parameters

“XX“ are for last numbers not shown here for privacy reasons – will be provided upon request if it gets important for some next research.

PARADOX:
Alarm system 1: Paradox Magellan MG5000 FW: V4.72 (4.72.072 on Babyware); Production date 05/2011; SN: 20168FXX
Alarm system 2: Paradox Magellan MG5050+ FW: V1.22.005 (01.28.001 on Babyware); Production date 01/2023 SN: 21308BXX FCC ID: KDYMG5050PLUS
Standards: EN 50136-1; EN 50136-2 SP4; EN50131-1; EN50131-3 Grade 2 Class II
Wired keypad: Paradox KL32LCD+; SN: 1D50E4XX
PCS 200 GSM 2G modem with VDMP3 module + wired DG55 PIR sensors were attached to the system. Babyware 5.5.23 was used to program and monitor the aforementioned Paradox alarm systems.
Wireless keypad 1: Paradox K37 433MHz FW: v1.16 Production week 39/2011
Wireless keypad 2: Paradox K37 433MHz FW: V1.16 Production week 39 2011
Wireless keypad 3: Paradox K38 433MHz FW: V1.01.004 Production date 08/09/2023
Wireless motion sensor PMD1P 433MHz FW: V2.02 Production week 38/2012 SN: 1270XX
Wireless reed switch DCTXP2 433MHz FW: V3.00 Production week 39/2012 SN: 0461XX
Keyfob 1: Paradox REM25 433MHz FW: V1.02 Production date: unknown SN: 0622XX
Keyfob 2: Paradox REM25 433MHz FW: V3.00 Production date: after 2019 SN: 2090XX
Paradox MG5050+ board and KL38 discounted price in total: 150€
Manual:
https://www.paradox.com/Products/default.asp?CATID=4&SUBCATID=43&PRD=1585

DSC WP8010-K-FR:
Central: (868-3:ANY) P/N:90-208142 Panel ID: 19B80E ; FW:I18.415; Product release date: 09.07.2017. Hub SN: 27173312XX. Keypad: WK141 (868-3:037) ;P/N:90-206891 Grade 2/Class2
PIR: PG8904 (868-3:012) Grade2/Class2. Reed switch: PG8945 (868-3:010) Grade2/Class2
Keyfob: PG8929 (868-3:030) Grade2/Class2.
Price for the unit and keypad with 50% discount: 203,10€
Manual:
https://www.fsm.fi/downloads/products/t/turvapakettid/DSC-10_ENG_kayttoohje.pdf

Jablotron JA-63
Hub: JA-63K,B,MB 5700_503; GK61009
Keyfob: RC-44 (3600_501)
Keypad: JA-60F-EN 0708701-001 / FF61009
PIR: JA-60P,T1 (4700_501); DR61021
2G modem. System was supplied years ago as part of the “GSMvalve koduvalve”
Price in auction: 69€
Manuals:https://manualzz.com/doc/62012906/jablotron-ja-63-%E2%80%9Eprofi%E2%80%9C-user-manual#p8

Hikvision AX PRO DS-PWA96-M-WE
Serial: Q127XXXXX
Version: V1.2.9 build 240412

Keypad: Model: DS-PK1-LT-WE; SN: Q273XXXXX - dated 08/2023.Standards:EN50131-1:2600 +A1+A2+A3; EN 50131-3:2009; SG2 ECII; EN50131-5-3:2017; EN 50131-6:2017+A1
PIR: DS-PDP15P-EG2-WE
Keyfob: DS-PKF1-WE
Reed switch: DS-PDMC-EG2-WE
Price for the system: 392,63€
Manual:
https://www.hikvision.com/content/dam/hikvision/products/S000000001/S000000601/S000000937/S000000938/OFR001810/M000034331/User_Manual/UD25814B_Baseline_AX-PRO-_User-Manual_v1.2.7_202209.pdf

G-Homa:
Hub: EMW302WF-HS
Reed switch: RF302DA
PIR: RF302PIR.
Price in auction: 15€
Manual: https://www.manualslib.com/manual/1308832/G-Homa-Emw302wf-Hs.html

PGST PW150:
PIR: 433M/1527 V2.3
Keyfob: 2238 V1.5 dated 2019 05 31
Reed switch: V1.4 dated 2022 02 17
Hub: PW150
Price in auction: 65€
Manual: https://fccid.io/2AIT9-PW150/User-Manual/User-Manual-5529214

PGST PG-103
Model: GSM+Wi-Fi Alarm host
RF:433M/1527/330K
Wi-Fi Module: T
Server: International
Language: ENG
Hub: PG-103 SN: 760200 ; Firmware: v1.23.03.n5
Price in auction: 22€
Manual: https://www.cn-pgst.com/downloads

PGST PG-107:
Firmware: v1.23.02.hf
Hub: PG-107 SN: 880686
2G modem + Wi-Fi.
Price in auction: 50,50€
Manual: http://it.cn-pgst.com/Content/upload/pdf/202237816/PG-107.pdf

Tecpeak A1:
Cellular+Wi-Fi-12-4Q
Hub A1; SN: 111527
Price in auction: 14,50€
Manual: **https://www.tecpeak.it/en/pages/faq**

Tecpeak A2:
Name : Alarm system
RF: 433MHz/1527/330K
GSM:850/900/1800/1900MHz
Server: International
Hub SN: 196198; Cellular+Wi-Fi -30-4.1.9.
Price in auction: 25€
Manual: **https://www.tecpeak.it/en/pages/faq**

Tecpeak A4:
Hub: A4 ; FW: v1.22.09.n5 ; SN 761958
Server: Global
Wi-Fi and 2G modem
Price in auction: 28€
Manual: **https://www.tecpeak.it/en/pages/faq**

Yale IA331
Serial: 15954785XX
Version 1.0 A1904 Made in Taiwan
Reed Switch: Yale smart Living AC-DC 1904 made in Taiwan
PIR: Yale smart Living AC-PETPIR 1904 made in Taiwan (contained a separate Tamper switch)
Keyfob: Yale smart Living AC-KF 1904 made in Taiwan – three button version.
Price in auction: 33€
Manual not found online - paper available with the system.

Ajax Hub2 Plus:
Hub hardware version was 82.2.9.10.3.5.1.0 and firmware EU 2.19.0.
PIR: "MotionCam Jeweller" with firmware EU 5.54.15.2.
Reed switch: "Ajax DoorProtect Jeweller" with firmware EU 5.57.0.39
Keyfob: "SpaceControl Jeweller" with firmware EU 5.54.1.5
Keypad: "KeyPad Plus Jeweller" with firmware EU 5.57.4.9
Manual: https://support.ajax.systems/en/manuals/hub-2-plus/

Appendix III - Paradox keypad signals analyze (raw data example)

In following part a typical arming session with code 0000 between wireless keypad (A- as Alice) and MG5000 hub (B - as Bob) is presented in HEX format where at least some similarities are tried to mark with different colouring to illustrate data repetitions and illustrate amount of data being exchanged during one session:

```
1A   53f36aaaaaa9f9b4d36924da49a49a69369b490
2B   f5555554fcd26934926924db4db69b4d248
3B   db69b5a69a6db4db6db6d26db6da6d249248
4A   553f369b4d246da69369a69a49a69
5B   f5555554fcdb6d34926d249b6d24da6da6db4d
6A   f5555554fcda6d3491b69a4da68d34934d2
7A   f5555554fcda6934926d269a6d24db6db6d36d24d34da4d36db6d24d348   - - - contains the code
8B   f5555554fcd26934926924db4db69b4d248
9B   f5555554fcdb6d34936d26db6d24da6da4db4da6db6d269b6da6d24d248
10A f5555554fcda6d34936d349b4d34d24d348
11B 9b4926db424da4936da49b4db4db69b4db6da4db6db6da49a49
12A f5555554fcda6d34936d349b4d34d24d348
13B f5555554fcda69b49a6d24db6d24d34da4d36d26da6da69a6da69b4d248
14A f5555554fcda6d34936d349b4d34d24d348
15B f5555554fcdb6d34926d249b6d24da6da6db4da6db6d26db6db6d24d248
16A f5555554fcdada6926da69369a69a49a69
17B f5555554fcda69349a6d34db6d24d36db4d36d26da6da69a6da69b4da48
18A 9b69a4da69a69269a4
19B f5555554fcdb6d34926d249b6d24da6da6db4da6db6d26db6db6d24d248
20A f5555554fcda369a49b69a4da69a69269a4
21B f5555554fcda69b49a6924db6d24d34db4d36d26db2da6d26da69b4d248
22A f5555554fcda6c
23B 926d249b6d4936924db6926d36d36da6d36db6936db6db6926924
24A 4d34935369a69a49a688
25B f5555554fad26934926d24db6d24d34db6d36d26da6da69b6da69b4d248
26A f5555554fcda6d3496da69369a69a49a690
```

```
27B f5555554fcdb6d34926d249b6d24da6da6db4da6db6d26db6db6d24d248
28A f5555554fcda6d34a6da69369a69a49ad2
29B f5555554fcda69b49a6924db6d24d34db4d36d2
30B 248
31A f5555554fcda6d34936d349b4d34d24d348
32B f5555554fcdb6d34926d249b6d24da6da6db4da6db6d26db6db6d24d248
33A f5555554fcda6d34936d349b4d34d24d348
```

MESSAGES OF ARMING AND DISARMING WITH CODE 0000 IN HEX FORMAT ORDERED BY VISUAL SIMILARITY:

```
Alog11 8A: f5555554fcda6934926d26    9a6d24d    b6    db    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d3        42
Alog15 7A: f5555554fcda6934926d26    9a6d24d    b6    db    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d3        42
Alog16 7A: f5555554fcda6934926d26    9a6d24d    b6    db    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d3        42
Alog18 8A: f5555554fcda6934926d26    9a6d24d    b6    db    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d3        41
Alog26 8A: f5555554fcda6934926d26    9a6d24d    b6    db    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d3        42
Alog28 7A:f5555554fcda6934926d26     9a6d24d    b6    db    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d3        42
Alog30 7A: f5555554fcda6934926d26    9a6d24d    b6    db    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d3        41
Alog31 3A: f5555554fcda6934926d26    9a6d24d    b6    db    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d3        42
Alog06 7A: f5555554fcda6934926d26    9a6d24d    b6    db    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d3        42
Alog07 6A: f5555554fcda6934926d26    9a6d24d    b6    db    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d3        42
Alog08 6A: f5555554fcda6934926d26    9a6d24d    b6    db    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d3        42
Dlog12 8A: f5555554fcda6d34926d36    9a6d24d    a6    da    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d2        41
Dlog18 8A: f5555554fcda6d34926d36    9a6d24d    a6    da    6d    36    d2    4d    34    da    4d    36    db    6d
      24        d2        42
```

```
Dlog24 5A: f5555554fcda6d34926d36    9a6d24d    a6    da    6d    36    d2    4d    34    da    4d    36    db    6d
      24       d2       42
Dlog26 1A: f5555554fcda6d34926d36    9a6d24d    a6    da    6d    36    d2    4d    34    da    4d    36    db    6d
      24       d2       42
Dlog33 8A: f5555554fcda6d34926d36    9a6d24d    a6    da    6d    36    d2    4d    34    da    4d    36    db    6d
      24       d2       42
Dlog08 7A: f5555554fcda6d34926d36    9a6d24d    a6    da    6d    36    d2    4d    34    da    4d    36    db    6d
      24       d2       42
```

Not all messages for arming and disarming are the same according to the analyze made in URH. Also it is possible that some of the messages have fluctuations within timings or amplitude level and can be misread in the URH analyze window by built-in automatic function (for example upper marked 41's). As manual reading of these messages is time consuming we exclude it and concentrate on the messages that seem to be readable and analyzable.

Samples of some probable misread code 0000 messages:

```
Alog37 5A: f5555554fcda6934926d26    9a6d24d     b6    db    6d    6d    a4    9a    69    b4    9a    6d    b6    da
      24       d3       42
Dlog06 6A: f5555554fcda6d34926d36    9a6d24d     a6    da    6d    36    d2    4d    34    da    4d    6d    b6    da
      49       a4       90
Dlog32 7A:  4d249f9b4da6924da6d34    da49b  4d   b4    da    6d    a4    9a    69    b4    9a    6d    b6    da    49
      a4       90
Dlog36 6A: b4aaa9f9b4da6924da6d34    da49b  4d   b4    da    6d    a4    9a    69    b4    9a    6d    b6    da    49
      a4       90
Dlog40 7A: f5555554fcda6d34926d36    9a6d24d  a3  6d    36    9b    69    26    9a    6d    26    9b    6d    b6    92
      69       24
Dlog35 5A: f5555554fcda6d34926d36    9a6d126  d3  6d    36    9b    69    26    9a    6d    26    9b    6d    b6    92
      69       22
log09 6A: 4fcda6d34927e6d369a 49369b4d36926      d3    6d    36    9b    69    26    9a    6d    26    9b    6d    b6
      92       69       22
Dlog19 8A: f5555554fcda6d34 49369b   4d36926      d3    6d    36    9b    69    26    9a    6d    26    9b    6d    b6
      92       69       22
Dlog13 6A: f5555554fcda6d34 49369b   4d36926      d3    6d    36    9b    69    23    4d    36    93    4d    b6    db
      49       34       91
```

```
log09 6A: f5555554fcda6934926d26        8d36913   6d    b6    db    4d    b4    93    4d    36    93    4d    b6    db
      49    34    d2
Dlog21 6A: fcda6d34927e6d369a 49369b 469b493      69    b6    9b    4d    b4    93    4d    36    93    4d    b6    db
      49    34    92
```

MESSAGES OF ARMING AND DISARMING WITH CODE 1111 IN HEX FORMAT ORDERED BY VISUAL SIMILARITY:

```
AR6Ak3:  f5555554fcda6934936d249a6d24d   a6    9b    69    b4    9a    69    b6    92    6d    b4    db    6d    24
      92    42
AR5Ak6:  f5555554fcda6934936d249a6d24d   a6    9b    69    b4    9a    69    b6    92    6d    b4    db    6d    24
      92    42
AR6Ak4:  f5555554fcda6934936d249a6d24d   a6    9b    69    b4    b4    d3    6d    24    db    69    b6    da    49
      24    90
AR7Ak7:  f5555554fcda6934936d248d36926   d3    4d    b4    da    4d    34    db    49    36    da    6d    b6    92
      49    22
AR7Ak10: f5555554fcda6934936d249a6d25    b4    d3    6d    36    93    4d    36    d2    4d    b6    9b    6d    a4
      92    49
6A k4dis:  f5555554fcda6d34936d34      9a6d24d     b6    9a    69    b4    9a    69    b6    92    6d    b4    db    6d
      24    93    44
8A k1dis:  f5555554fcda6d34936d34      9a6d24d     b6    9a    69    b4    9a    69    b6    92    6d    b4    db    6d
      24    93    41
8A k2dis: f5555554fcda6d34936d34       9a6d24d     b6    9a    69    b4    9a    69    b6    92    6d    b4    db    6d
      24    93    42
9A k7dis: f5555554fcda6d34936d34       9a6d24d     b6    9a    69    b4    9a    69    b6    92    6d    b4    db    6d
      24    4b    42
8A k9dis: f5555554fcda6d34936d34       9a6d24d     b6    9a    69    b4    9a    69    b6    92    6d    b4    db    6d
      24    93    42
```

It is possible to notice that arming and disarming with code 0000 and 1111 contains similarities that can be used for further extraction to get more knowledge about how the messages for arming and disarming are built up.

```
AR6Ak3:    f5555554fcda6934936d24    9a6d24d     a6    9b    69    b4    9a    69    b6    92    6d    b4    db    6d
      24    92    42
AR5Ak6:    f5555554fcda6934936d24    9a6d24d     a6    9b    69    b4    9a    69    b6    92    6d    b4    db    6d
      24    92    42
8A k2dis:   f5555554fcda6d34936d34    9a6d24d     b6    9a    69    b4    9a    69    b6    92    6d    b4    db    6d
      24    93    42
```

```
8A k9dis:    f5555554fcda6d34936d34   9a6d24d   b6   9a   69   b4   9a   69   b6   92   6d   b4   db   6d
     24      93      42
Alog08 6A:  f5555554fcda6934926d26   9a6d24d   b6   db   6d   36   d2   4d   34   da   4d   36   db   6d
     24      d3      42
Dlog18 8A:  f5555554fcda6d34926d36   9a6d24d   a6   da   6d   36   d2   4d   34   da   4d   36   db   6d
     24      d2      42
```

After seeing how these messages are similar in HEX we also wanted to see what is changing in binary:

Message arming with code 0000 log08 6A :

```
1111010101010101010101010101010011111100110110100110100100110100100100100110110100100110100110100110110100100100110
1101101101101101101101101001101101101001001001101001101001101101001001101001101101101101101101001001001101001101
0010
```

Message arming with code 1111 katse3 6A:

```
1111010101010101010101010101010011111100110110100110100100110100100100110110110100100100100110100110110100100100110
1101001101001101101101001101101001001101001101001101101101001001001101101101101001101101101101101001001001001001001
0010
```

Message disarming with code 0000 log18 8A:

```
1111010101010101010101010101010011111100110110100110110100110100100100100110110100110110100110100110110100100100110
1101001101101101001101101001101101101001001001101001101001101101001001101001101101101101101101001001001101001001
0010
```

Message disarming with code 1111 katse2 8A:

```
1111010101010101010101010101010011111100110110100110110100110100100100110110110100110100100110100110110100100100110
1101101101001101001101001101101001001101001101001101101101001001001101101101101001101101101101101001001001001001101
0010
```

For easier visibility we compared the bits line by line:
ARMING log08 6A first part as first line and arming katse3 6A first part as second line followed by second part of both messages:

11110101010101010101010101010100111111001101101001101001001101001001001**0**01101101001001**1**0100110100110110100100100110
1101**1**01101**1**01101101101**1**
11110101010101010101010101010100111111001101101001101001001101001001001**1**01101101001001**0**0100110100110110100100100110
1101**0**01101**0**01101101101**0**

01**0**01101**1**01**1**01**0**01001**0**01**1**01**0**01101**0**01**1**01**1**01001**0**01101**0**01101**1**01101101101101101001001001**1**01001**1**010010
01**1**01101**0**01**0**01**1**01001**1**01**0**01**1**01101**1**01**0**01**0**01001**1**01101**1**01101**0**01101101101101101001001001**0**01001**0**010010

In total it shows 20 bits are different.

DISARMING log18 8A first part as first line and katse2 6A first part as second line followed by second parts of both messages:

11110101010101010101010101010100111111001101101001101101001101001001001**0**01101101001101**1**0100110100110110100100100110
1101**0**01101**1**01101001101**1**
11110101010101010101010101010100111111001101101001101101001101001001001**1**01101101001101**0**0100110100110110100100100110
1101**1**01101**0**01101001101**0**

01**0**01101**1**01**1**01**0**01001**0**01**1**01**0**01101**0**01**1**01**1**01001**0**01101**0**01101**1**01101101101101101001001001**1**01001**0**010010
01**1**01101**0**01**0**01**1**01001**1**01**0**01**1**01101**1**01**0**01**0**01001**1**01101**1**01101**0**01101101101101101001001001**0**01001**1**010010

In total it shows 20 bits are different.

We also tried to separate different bits with arming and disarming with the same code to see more clearly what is changing in message bit level. In real practical tests it shows that it does not matter for the current Paradox unit if we send out an arming or disarming message as it arms and disarms after getting the same message repeatedly. That means these bits which are changing only to claim arming or disarming information being transmitted will not matter to actually defeat the system. So we can probably exclude their deeper inspection if only code based brute force attack tools are considered, and therefore it is still good to know which bits are responsible for that information transmission. As it also raises problems with brute force to get MG5050+ jamming detection to activate if “funny” signals occur repeatedly.

Getting arming-disarming informative bits separated:

138 bits in the first row and 96 bits in the second row equals 234 bit message length!

Arming log08 6A first part as first line and disarming log18 8A first part as second line followed by second parts of both messages:

11110101010101010101010101010100111111001101101001101**0**01001101001001001001101101001**0**0110100110100110110100100100110
1101**1**01101101101**1**011011
11110101010101010101010101010100111111001101101001101**1**01001101001001001001101101001**1**0110100110100110110100100100110
1101**0**01101101101**0**011011

01001101101101001001001101001101001101101001001101001101101101101101101001001001101001**1**010010
01001101101101001001001101001101001101101001001101001101101101101101101001001001101001**0**010010

In total 5 bits are different. Bits 54; 84; 120; 132; 228

Arming katse3 6A first part as first line and disarming katse2 6A first part as second line followed by second parts of both messages:

```
1111010101010101010101010101010100111111001101101001101001001101001001001101101101001001001001101001101101001001001101
11010011010011011011010
1111010101010101010101010101010100111111001101101001101101001101001001001101101101001101001001101001101101001001001101
11011011010011010011010

0110110100100110100110100110110110100100100110110110110100110110110110100100100100100010010
0110110100100110100110100110110110100100100110110110110100110110110110100100100100101010010
```

In total 5 bits are different.

We can see that from these set of 5 different bits for arming and disarming there is also a difference in accordance with code usage for arming/disarming. We can notice that from these different bits third and fifth one are vice versa for arming and disarming. Observing the same messages in HEX format will visualize it better. It raises some questions but at the moment we leave them out of our scope and concentrate more on the bits that seem to be responsible for the code transmission part.

Bits marked with yellow are responsible for arming/disarming transmission part on log08 6A and katse3 6A arming messages:

ARMING log08 6A first part as first line and arming katse3 6A first part as second line followed by second part of both messages:

```
1111010101010101010101010101010100111111001101101001101001001101001001000101101101001001110100110100110110100100100110
11011011011011011011011
1111010101010101010101010101010100111111001101101001101001001101001001001101101101001001000100110100110110100100100110
11010011010011011011010

0100110110110100100100110100110100110110100100110100110110110110110110100100100110100110010010
0110110100100110100110100110110110100100100110110110110100110110110110100100100100100010010
```

As it is possible to see bits nr 120 and nr 228 overlap with bits being changed with code change.

Bits marked with yellow are responsible for arming/disarming transmission part on log18 8A and katse2 6A disarming messages:

DISARMING log18 8A first part as first line and katse2 6A first part as second line followed by second parts of both messages:

111101010101010101010101010101010011111100110110100110110100110100100100100110110100110110100110100110110100100100110110100011011011010011011011
111101010101010101010101010101010011111100110110100110110100110100100100110110110100110100100110100110110100100100110110110110100011010011010

0100110110110100100100110100110100110110100100110100110110110110110110100100100110100100010010
0110110100100110100110100110110110100100100110110110110100110110110110100100100100100110010010

As it is possible to see bits nr 120 and nr 228 overlap with bits being changed with code change also with disarming messages.
According to that we assume that these overlapping bits number 120 and 228 change their value according to the arming and disarming message state but as we determined beforehand it seems irrelevant in our attack scenario so we can at least in the beginning exclude these bits from code breaking attack.

So from that it is derived that bits number 72; 87; 126; 138; 141; 147; 150; 153; 159; 162; 165; 171; 174; 177; 183; 189; 195; 222 are related to code change from 0000 to 1111.

To see if these bits are randomly changed or there is a certain recurrence we look more deeply into messages with different codes used.

Arming 2222 against 0000 and 1111

111101010101010101010101010101010011111100110110110110100100110100100100110110110100100100010011010011011010010010011011011011010001101101101101
111101010101010101010101010101010011111100110110100110100100110100100100100110110100100100110100110100110110100100100110110110110110110110110111
111101010101010101010101010101010011111100110110100110100100110100100100110110110100100100100100110100110110100100100110110100011010011011011010

0100110100110100100110110100110110110100110110110110110110110110100100100100100110010010 ----2222
0100110110110100100100110100110100110110100100110100110110110110110110100100100110100110010010 ----0000
0110110100100110100110100110110110100100100110110110110100110110110110100100100100100100010010 ----1111

Code 2222: f5555554fcdb6934936d249a6d24d   b6   9b   6d   34   d2   6d   36   da   6d   b6   db   6d   24
93   42

Alog08 6A: f5555554fcda69349 26d269a6d24d b6 db 6d 36 d2 4d 34 da 4d 36 db 6d 24 d3 42
AR6Ak3: f5555554fcda69349 36d249a6d24d a6 9b 69 b4 9a 69 b6 92 6d b4 db 6d 24 92 42

If beforehand we thought that bits 120 and 228 are only related to arming/disarming informative value then here we can see that HEX values 93 and 92 what were before seen as different value describing arming and disarming together with d3 and d2 are now represented in either way only in arming messages. At current moment it might be that bits 120 and 228 are connected so if bit 120 = 1 (giving 1011 as b) then on the same time bit 228 = 0 (giving 0011 as 3) and if bit 120=0 (giving 1010 as a) then on the same time bit 228=0 (giving 0010 as 2).

It is possible to see that most of the places with different bits occur in the same places at bit numbers: 72; 87; 126; 138; 141; 147; 150; 153; 159; 162; 165; 171; 174; 177; 183; 189; 195; 222 (120 and 228 left out from the list here). Only bit 48 is added to differing bits. That is in HEX the FCDB instead of FCDA like log08 6A and katse3 6A have.

In total it seems that 21 bits can change their value when code is changed. But when looking at hex and taking into account that messages have different parts for different purposes and not all of these bits are following each other then possibilities are narrowed down. 2 in order of 21 = 2 097 152 different possibilities. 21 bit key in real world cryptography cannot be thought of as a high level of security, rather it is insecure and can be broken on a student laptop but what was noticed with 2222 was that the changed bit position was also different. So if bits are randomly changed in random positions then it makes it really hard to figure out where the actual code is hidden.

Comparing code 3333 to code 0000 with using 4 bits chunk as HEX symbol describer:

11110101010101010101010101010101001111110011010010011010010011010010011010001101101001101000100110100110110100100100110
10011010011011011011010010110110100011010
11110101010101010101010101010101001111110011011010011010010011010010010010001101101001001101001101001101101001001001 10
11011011011011011011011010011011011010010

011010010010010110100100100110100110110100110110100110100110110100110100100010010 ----3333
010001101001101001101101001001101001101101101101101101101001001001101001101010010 ----0000

We notice 22 changes but 2 are inside the same 4 bit row making 21 HEX symbols differences between these two.

When all combined together we can see that a lot more HEX symbols are influenced in total by numbers change.

1111010101010101010101010101010100111111001101001001101001001101001001101001101101001110100100110100110110100100100110
1001110100110110110110100110110110100110100111010
1111010101010101010101010101010100111111001101101101101001001101001001001101101101001000100100110100110110100100100110
11011011010011011011011010011010011010010
1111010101010101010101010101010100111111001101101001101001001101001001001001101101001001101001101001101101001001 00110
11011011011011011011011010011011011010010
1111010101010101010101010101010100111111001101101001101001001101001001001101101101001001001001101001101101001001001 10
11010011010011011011010011011010010011010

011010010010011010010010011010011011010011011010011010011011010011010010010010 ----3333
011011010011011011011011010011011011011011011011011011011011010010010010010011010010 ----2222
010011010011010011011010010011010011011011011011011011011010010010011010011010010 ----0000
011010011011011010010010011011011011010011011011011011011010010010010010010010010 ----1111

Here we can see that with 3333 we have plus 6 differences in HEX symbols change and in total 27 symbols are in play now. It is adding more complexity to our task and we can estimate that the system will get even more complex if we add other code numbering captures to the analyze. We also tested the second keypad and saw that serial change basically changed also other bits that were initially thought of carrying the code info. As another 7 bits were overlapping with the ones changing when code changed with the first keypad we decided to stop current analyze. The serial number is itself somehow also used together with code while obfuscating signals.

Appendix IV - DSC keyfob signals analyze (raw data example)

Keyfob disarming signals URH HEX values ordered according similarities:

```
1)   d55555550f9a8f9af  3f    009b3 eee  5063  b707b93   58   490bf2          ccc134           fa953  50d568d673dbb
4)   d55555550f9a8f9af  3f    009b3 dee  5063  b646126   e8   b8ad79          23391b                  936e8  73cecbb33e08b0
19)  d15555550f9a8f9af  3f    009b3 dee  5063  b279615   cb   8c3c3c          2176b2                  ccb81  60d98b533fda48
5)   d45555550f9a8f9af  3f    009b3 c6e  20c7  6978588   35   07a0a1          b2a91d           24c6f  e275d7867700f
27)  d55555550f9a8f9af  5f    009b3 c6e  5063  b242dcd   c3   1b26d9                  512f7e          a45d3  6d106
27)  d55555550f9a8f9af  5f    009b3 c6e  5063  b242dcd   c3   1b26d9                  512f7e          a45d3  6d106
-redundant inside same session
1)   d55555550f9a8f9af  5f    009b3 d6e  5063  b3db32a   9a   2aab50          a9ea47           15b93  69a9b0
8)   d45555550f9a8f9af  5f    009b3 d6e  20c7  64e3893   43   ecad5f          80cde1           8
24)  d55555550f9a8f9af  57    009b3 d6e  4063  b4ffd62        4d      8910a9          eaaf24          e9f01  38694988
22)  d55555550f9a8f9af  57    009b3 fee  4063  b31df24   a8   6575b3                  b16a5b          f215a  50d2683
9)   d55555550f9a8f9af  77    009b3 e6e  59a5  2259647   62   77cbe9          b955be           dd938
18)  d55555550f9a8f9af  77    009b3 e6e  59a5  2259647   68   77cbe9          b955be           d7338
1)   d55555550f9a8f9af  77    009b3 e6e  59a5  255de0f   c3   8b4bee          b955be           aa718
25)  d55555550f9a8f9af  77    009b3 e6e  59a5  26a194b   c6   adcbe3          b955be           be958
6)   d551555287cc8f9af  77    009b3 cee  59a5  255de0f   c6   8b4bee          b955be           87098
6)   d55555550f9a8f9af  77    009b3 cee  59a5  26a194b   d7   5b97c7          72ab7d           0d5b
23)  d55555550f9a8f9af  77    009b3 cee  59a5  2259647   76   77cbe9          b955be           e0fb8
29)  d55555550f9a8f9af  77    009b3 cee  59a5  2259647   7f   77cbe9          b955be           e96b8
29)  d55555550f9a8f9af  77    009b3 cee  59a5  26a194b   c9   adcbe3          b955be           994d8
2)   d55555550f9a8f9af  77    009b3 cee  59a5  2259647   1a   774be9          b955be
2)   d55555550f9a8f9af  77    009b3 cee  59a5  26a194b   ac   ad4be3          b955be           861c0
2)   d55555550f9a8f9af  77    009b3 cee  59a5  21bb67a   a8   f0cbe0          b955be           b0398
7)   d55555550f9a8f9af  77    009b3 fee  59a5  255de0f   c7   8b4bee          b955be           f6280
24)  d55555550f9a8f9af  77    009b3 fee  59a5  24e2669   97   ec4be8          b9557d                  0589
3)   d55555550f9a8f9af  77    009b3 fee  59a5  2259647   65   77cbe9          b955be           82f80
25)  d55555550f9a8f9af  77    009b3 e5c  b34a  44b2c8e   e0   ef97d3          72ab7d           9d67
19)  d55555550f8a8f9af  77    009b3 d6e  598a  44b2c8e   d4   ef97d3          72a37d           4a44
20)  d15555550f9a8f9af  77    009b3 d6e  334a  44b2c8c   d5   df2f45          caadf7           de9c
27)  d55555550f9a8f9af  77    009b3 d6e  59a5  20803f5   86   b64be2          b955be           d7108
4)   d55555550f9a8f9af  77    009b3 d6e  59a5  2259647   67   77cbe9          b955be           e8f38
```

```
5)  d55515550f9a8f9af  77  009b3 dee  59a5  2259647  66  77cbe9  b955be    e1eb8
15) d55555550f9a8f9af  77  009b3 c6e  59a5  24e2669  9b  ec4be8  b955be    f63d0
15) d55555550f9a8f9af  77  009b3 c6e  59a5  20803f5  89  b64be2  b955be    88f10
22) d55555550f9a8f9af  77  009b3 c6e  59a5  2259647  77  77cbe9  b955be    e9e38
28) d55555550f9a8f9af  77  009b3 c6e  59a5  2259647  7c  77cbe9  b955be    a2520
28) d55555550f9a8f9af  77  009b3 c6e  59a5  26a194b  ca  adcbe3  b955be    d2740
11) d55555550f9a8f9af  77  009b3 c6e  59a5  2259647  6c  77c9e9  b955be    f3538
11) d55555550f9a8f9af  77  009b3 c6e  59a5  255de07  e5  c5a5f7  5caadf    4168c
11) d55555450f9a8f9af  77  009b3 c6e  59a5  26a194b  da  adcbe3  b955be    83758
11) d55555550f9a8f9af  77  009b3 c6e  59a5  21bb67a  de  f04be0  b955be    b5100
13) d55555550f9a8f9af  77  009b3 f6e  59a5  2785d4a  6d  f84bed  b955be    e3980
13) d45555550f9a8f9af  77  009b3 f6e  59a5  24e2669  88  ec4be8  b955be    943c8
13) d45555550f9a8f9af  77  009b3 f6e  59a5  24e2669  88  ec4be8  b955be    943c8 - - - redundant inside
same session
3)  d55555550f9a8f9af  9f  009b3 f6e  4063  a0027be  63  3830f5  8
5)  d55555550f9a8f9af  9f  009b3 f6e  4063  a20aa77  61  b85b7e  8
16) d55555550f9a8f9af  9f  009b3 f6e  4063  a5aed2a  23  386970        0
26) d55555550f9a8f9af  9f  009b3 f6e  4063  a05f11e  2d  b866cd  0
26) d55555550f9a8f9af  77  009b3 eee  59a5  2785d4a  70  f84bed  b955be    e7500
18) d15555550f9a8f9af  9f  009b3 edc  80c7  4beb6be  95  70c67a
21) d52a91550f9a87cd7  77  009b3 c6e  5f85  255de0f  d3  8b4bee  b955be    8b418
21) d45555550f9a8f98f  3f  009b3 cee  5063  b29c472  20  416f2b  b4825d          313ec
93e758b67da33
```

These signals in HEX format are probably not always correctly demodulated. Sometimes only changing the error tolerance factor from 4 to 5 or 3 to 2 can totally change the result. Some part of it can be put on a not maximum quality received radio signal. As we used URH and mainly rely on autodetection functionality then in this case it did not work properly and we had to manually adjust the parameters to fix the detection errors as much as we could.

LOOKING MORE DEEPER:

```
2)  d55555550f9a8f9af  77  009b3 cee  59a5  2259647  1a  774be9  b955be ---- Error?
3)  d55555550f9a8f9af  77  009b3 fee  59a5  2259647  65  77cbe9  b955be    82f80
4)  d55555550f9a8f9af  77  009b3 d6e  59a5  2259647  67  77cbe9  b955be    e8f38
5)  d55515550f9a8f9af  77  009b3 dee  59a5  2259647  66  77cbe9  b955be    e1eb8
9)  d55555550f9a8f9af  77  009b3 e6e  59a5  2259647  62  77cbe9  b955be    dd938
11) d55555550f9a8f9af  77  009b3 c6e  59a5  2259647  6c  77c9e9  b955be    f3538
```

18)	d55555550f9a8f9af	77	009b3	e6e	59a5	2259647	68	77cbe9	b955be	d7338
22)	d55555550f9a8f9af	77	009b3	c6e	59a5	2259647	77	77cbe9	b955be	e9e38
23)	d55555550f9a8f9af	77	009b3	cee	59a5	2259647	76	77cbe9	b955be	e0fb8
28)	d55555550f9a8f9af	77	009b3	c6e	59a5	2259647	7c	77cbe9	b955be	a2520
29)	d55555550f9a8f9af	77	009b3	cee	59a5	2259647	7f	77cbe9	b955be	e96b8

Changing part inside the signal:

3) fe 65 82f 80
4) d6 67 e8f 38
5) de 66 e1e b8

9) e6 62 dd9 38
11) c6 6c f35 38
18) e6 68 d73 38

22) c6 77 e9e 38
23) ce 76 e0f b8
28) c6 7c a25 20
29) ce 7f e96 b8

1)	d55555550f9a8f9af	77	009b3	e6e	59a5	255de0f	c3	8b4bee	b955be	aa718
6)	d551555287cc8f9af	77	009b3	cee	59a5	255de0f	c6	8b4bee	b955be	87098
7)	d55555550f9a8f9af	77	009b3	fee	59a5	255de0f	c7	8b4bee	b955be	f6280

Changing part inside signal (assuming that first part in signal6 is an error):

1) 2e6 c3 aa718
6) ce c6 87098
7) fe c7 f6280

2)	d55555550f9a8f9af	77	009b3	cee	59a5	26a194b	ac	ad4be3	b955be	861c0	----4 is an error?
6)	d55555550f9a8f9af	77	009b3	cee	59a5	26a194b	d7	5b97c7	72ab7d	0d5b	----Error ???
11)	d55555450f9a8f9af	77	009b3	c6e	59a5	26a194b	da	adcbe3	b955be	83758	
25)	d55555550f9a8f9af	77	009b3	e6e	59a5	26a194b	c6	adcbe3	b955be	be958	
28)	d55555550f9a8f9af	77	009b3	c6e	59a5	26a194b	ca	adcbe3	b955be	d2740	
29)	d55555550f9a8f9af	77	009b3	cee	59a5	26a194b	c9	adcbe3	b955be	994d8	

Changing part:

2) ce ac 861c0
11) c6 da 83758
25) e6 c6 be958

28) c6 ca d2740
29) ce c9 994d8

2)	d55555550f9a8f9af	77	009b3	cee	59a5	21bb67a	a8	f0cbe0	b955be	b0398
11)	d55555550f9a8f9af	77	009b3	c6e	59a5	21bb67a	de	f04be0	b955be	b5100

Changing part:

2) ce a8 c b0389
11) c6 de 4 b5100

13)	d45555550f9a8f9af	77	009b3	f6e	59a5	24e2669	88	ec4be8	b955be	943c8	----first 4 error?
15)	d55555550f9a8f9af	77	009b3	c6e	59a5	24e2669	9b	ec4be8	b955be	f63d0	
24)	d55555550f9a8f9af	77	009b3	fee	59a5	24e2669	97	ec4be8	b9557d	0589	---7d error???

Changing part:
13) f6 88 943c8
15) c6 9b f63d0
24) fe 97 0589

15)	d55555550f9a8f9af	77	009b3	c6e	59a5	20803f5	89	b64be2	b955be	88f10
27)	d55555550f9a8f9af	77	009b3	d6e	59a5	20803f5	86	b64be2	b955be	d7108

Changing part:
15) c6 89 88f10
27) d6 86 d7108

13)	d55555550f9a8f9af	77	009b3	f6e	59a5	2785d4a	6d	f84bed	b955be	e3980
26)	d55555550f9a8f9af	77	009b3	eee	59a5	2785d4a	70	f84bed	b955be	e7500

Changing part:
13) f6 6d e3980
26) ee 70 e7500

From the upper it is possible to see that on similar signals sent out by keyfob mainly only a small part of information is changing. Nevertheless we cannot estimate what kind of signal or message is going to be sent next or which exact messages will be combined in one session. We also cannot see the rolling code part at the moment yet. It would need a conversion between HEX and Decimal value of certain parts of the changing part. It is left out of scope at the moment and is going to be done in later works.

BY SESSION:

1	d55555550f9a8f9af	3f	009b3	eee	5063	b707b93	58	490bf2	ccc134	fa953	50d568d673dbb
1	d55555550f9a8f9af	5f	009b3	d6e	5063	b3db32a	9a	2aab50	a9ea47	15b93	69a9b0
1	d55555550f9a8f9af	77	009b3	e6e	59a5	255de0f	c3	8b4bee	b955be	aa718	
2	d55555550f9a8f9af	77	009b3	cee	59a5	2259647	1a	774be9	b955be		
2	d55555550f9a8f9af	77	009b3	cee	59a5	26a194b	ac	ad4be3	b955be	861c0	
2	d55555550f9a8f9af	77	009b3	cee	59a5	21bb67a	a8	f0cbe0	b955be	b0398	
3	d55555550f9a8f9af	77	009b3	fee	59a5	2259647	65	77cbe9	b955be	82f80	
3	d55555550f9a8f9af	9f	009b3	f6e	4063	a0027be	63	3830f5	8		
4	d55555550f9a8f9af	3f	009b3	dee	5063	b646126	e8	b8ad79	23391b	936e8	73cecbb33e08b0
4	d55555550f9a8f9af	77	009b3	d6e	59a5	2259647	67	77cbe9	b955be	e8f38	
5	d45555550f9a8f9af	3f	009b3	c6e	20c7	6978588	35	07a0a1	b2a91d	24c6f	e275d7867700f
5	d55555550f9a8f9af	9f	009b3	f6e	4063	a20aa77	61	b85b7e	8		
6	d551555287cc8f9af	77	009b3	cee	59a5	255de0f	c6	8b4bee	b955be	87098	
6	d55555550f9a8f9af	77	009b3	cee	59a5	26a194b	d7	5b97c7	72ab7d	0d5b	
7	d55555550f9a8f9af	77	009b3	fee	59a5	255de0f	c7	8b4bee	b955be	f6280	
8	d45555550f9a8f9af	5f	009b3	d6e	20c7	64e3893	43	ecad5f	80cde1	8	
9	d55555550f9a8f9af	77	009b3	e6e	59a5	2259647	62	77cbe9	b955be	dd938	
11	d55555550f9a8f9af	77	009b3	c6e	59a5	2259647	6c	77c9e9	b955be	f3538	
11	d55555550f9a8f9af	77	009b3	c6e	59a5	255de07	e5	c5a5f7	5caadf	4168c	
11	d55555450f9a8f9af	77	009b3	c6e	59a5	26a194b	da	adcbe3	b955be	83758	
11	d55555550f9a8f9af	77	009b3	c6e	59a5	21bb67a	de	f04be0	b955be	b5100	
13	d55555550f9a8f9af	77	009b3	f6e	59a5	2785d4a	6d	f84bed	b955be	e3980	
13	d45555550f9a8f9af	77	009b3	f6e	59a5	24e2669	88	ec4be8	b955be	943c8	
15	d55555550f9a8f9af	77	009b3	c6e	59a5	24e2669	9b	ec4be8	b955be	f63d0	
15	d55555550f9a8f9af	77	009b3	c6e	59a5	20803f5	89	b64be2	b955be	88f10	
16	d55555550f9a8f9af	9f	009b3	f6e	4063	a5aed2a	23	386970	0		
18	d55555550f9a8f9af	77	009b3	e6e	59a5	2259647	68	77cbe9	b955be	d7338	
18	d15555550f9a8f9af	9f	009b3	edc	80c7	4beb6be	95	70c67a			
19	d15555550f9a8f9af	3f	009b3	dee	5063	b279615	cb	8c3c3c	2176b2	ccb81	60d98b533fda48

19	d55555550f8a8f9af	77	009b3	d6e	598a	44b2c8e	d4	ef97d3	72a37d	4a44	
20	d15555550f9a8f9af	77	009b3	d6e	334a	44b2c8c	d5	df2f45	caadf7	de9c	
21	d52a91550f9a87cd7	77	009b3	c6e	5f85	255de0f	d3	8b4bee	b955be	8b418	
21	d45555550f9a8f98f	3f	009b3	cee	5063	b29c472	20	416f2b	b4825d	313ec	93e758b67da33
22	d55555550f9a8f9af	57	009b3	fee	4063	b31df24	a8	6575b3	b16a5b	f215a	50d2683
22	d55555550f9a8f9af	77	009b3	c6e	59a5	2259647	77	77cbe9	b955be	e9e38	
23	d55555550f9a8f9af	77	009b3	cee	59a5	2259647	76	77cbe9	b955be	e0fb8	
24	d55555550f9a8f9af	57	009b3	d6e	4063	b4ffd62	4d	8910a9	eaaf24	e9f01	38694988
24	d55555550f9a8f9af	77	009b3	fee	59a5	24e2669	97	ec4be8	b9557d		0589
25	d55555550f9a8f9af	77	009b3	e6e	59a5	26a194b	c6	adcbe3	b955be	be958	
25	d55555550f9a8f9af	77	009b3	e5c	b34a	44b2c8e	e0	ef97d3	72ab7d	9d67	
26	d55555550f9a8f9af	9f	009b3	f6e	4063	a05f11e	2d	b866cd	0		
26	d55555550f9a8f9af	77	009b3	eee	59a5	2785d4a	70	f84bed	b955be	e7500	
27	d55555550f9a8f9af	5f	009b3	c6e	5063	b242dcd	c3	1b26d9	512f7e	a45d3	6d106
27	d55555550f9a8f9af	77	009b3	d6e	59a5	20803f5	86	b64be2	b955be	d7108	
28	d55555550f9a8f9af	77	009b3	c6e	59a5	2259647	7c	77cbe9	b955be	a2520	
28	d55555550f9a8f9af	77	009b3	c6e	59a5	26a194b	ca	adcbe3	b955be	d2740	
29	d55555550f9a8f9af	77	009b3	cee	59a5	2259647	7f	77cbe9	b955be	e96b8	
29	d55555550f9a8f9af	77	009b3	cee	59a5	26a194b	c9	adcbe3	b955be	994d8	

When looking at session 2 and 11 and 28 and 29:

2	d55555550f9a8f9af	77	009b3	cee	59a5	2259647	1a	774be9	b955be	
2	d55555550f9a8f9af	77	009b3	cee	59a5	26a194b	ac	ad4be3	b955be	861c0
2	d55555550f9a8f9af	77	009b3	cee	59a5	21bb67a	a8	f0cbe0	b955be	b0398
11	d55555550f9a8f9af	77	009b3	c6e	59a5	2259647	6c	77c9e9	b955be	f3538
11	d55555550f9a8f9af	77	009b3	c6e	59a5	255de07	e5	c5a5f7	5caadf	4168c
11	d55555450f9a8f9af	77	009b3	c6e	59a5	26a194b	da	adcbe3	b955be	83758
11	d55555550f9a8f9af	77	009b3	c6e	59a5	21bb67a	de	f04be0	b955be	b5100
28	d55555550f9a8f9af	77	009b3	c6e	59a5	2259647	7c	77cbe9	b955be	a2520
28	d55555550f9a8f9af	77	009b3	c6e	59a5	26a194b	ca	adcbe3	b955be	d2740
29	d55555550f9a8f9af	77	009b3	cee	59a5	2259647	7f	77cbe9	b955be	e96b8
29	d55555550f9a8f9af	77	009b3	cee	59a5	26a194b	c9	adcbe3	b955be	994d8

Pink - blue -grey or at least pink - blue are in order.

Appendix V - Attack tree

OUR GOAL: Secretly enter premises protected by security alarm system (burglar version)

1) Using the code to disarm the system (OR)

1.1) Get code from the user (OR)

1.1.1) Threaten user to reveal the code (OR)

1.1.2) Blackmail or bribe user to give the code (OR)

1.1.3) Ask for the code with a trick- play a repairman/phishing etc. (OR)

1.1.4) Infiltrate into staff to get access to the code

1.2) Observe visually while the code is being entered (OR)

1.2.1) Over the shoulder (OR)

1.2.2) From the distance with zoomed in camera

1.3) Get the code by eavesdropping communication (OR)

1.3.1) Eavesdrop mobile communication (SMS) to get the code (OR)

1.3.1.1) Listen in to the BTS tower communication link channels (OR)

1.3.1.2) Capture used mobile phone traffic by MITM attack

1.3.2) Eavesdrop Wi-Fi communication to get the code (OR)

1.3.2.1) Decrypt Wi-Fi packets to reveal the code (OR)

1.3.2.2) Replay packets known to disarm the system

1.3.3) Eavesdrop wireless keypad radio channel on 433MHz or 868MHz to get the code (OR)

1.3.3.1) Decrypt or decipher the code from sent messages (OR)

1.3.3.2) Replay recorded messages known to disarm the system

1.3.4) Eavesdrop signals in caballing to get the code

1.3.4.1) Listen in to the keypad/hub cables (OR)

1.3.4.2) Listen in to the LAN cables

1.4) Brute force the code over keypad signaling channels (OR)

1.5) Get the code by having access to the mobile phone application (OR)

1.5.1) Lend or borrow the phone (OR)

1.5.2) Steal the phone (OR)

1.5.3) Infect the phone with a rootkit (OR)

1.5.4) Get access to the user account over the cloud service

1.6) Get the code from installer

1.6.1) Get a job in alarm service company (OR)

1.6.2) Hack the service provider database (OR)

1.6.3) Bribe Individual worker having access to codes

1.6.3.1) Bribe account holder (OR)

1.6.3.2) Bribe instalment workers

2) Using the keyfob to disarm the system (OR)

2.1) Get the physical keyfob

2.1.1) Steal the working keyfob from user (OR)

2.1.2) Clone the keyfob from original one (OR)

2.1.3) Clone keyfob OTA (OR)

2.1.4) Conduct replay attack using recorded keyfob signals

3) Using a token to disarm the system (OR)

3.1) Get the physical token

3.1.1) Clone the token physically from original (OR)

3.1.2) Clone token secretly OTA (OR)

3.1.3) Generate our own token based on known system specs (OR)

3.1.4) Steal the token

4) Avoid alarm system getting activated

4.1) Avoid triggering sensors while entering or moving inside premises (OR)

4.1.1) Fooling reed switches with strong magnets (OR)

4.1.2) Fooling PIR sensors with heat shielding cover

4.2) Jam the communication between sensors and hub (OR)

4.3) Jam the communication channel between system and user or service provider (OR)

4.4) Break down the alarm system (OR)

4.4.1) Physically brake it while unarmed (OR)

4.4.1.1) Brake main unit during prearranged accident (OR)

4.4.1.2) Disable/block/manipulate sensors

4.4.2) Physically brake it while armed

4.4.2.1) Cut power and drain battery (OR)

4.4.2.2) Inject overvoltage to power lines

4.5) Avoid system to get armed (OR)

4.5.1) Jam wireless keypad/keyfob frequencies (OR)

4.5.2) Manipulate with original token so it would not work (OR)

4.5.3) Jam Wi-Fi or mobile communications (OR)

4.5.4) Generate a flaw that disallows arming (OR)

4.5.5) Generate immense load of false alarms so user would not arm the system

4.6) Manipulate with alarm system over network

4.6.1) Hack system main control unit over Internet (OR)

4.6.2) DOS attack (OR)

4.6.3) De-authenticate attack for cutting Wi-Fi connection (OR)

4.6.4) Send fake status messages over the Internet to the cloud service

Appendix VI - Licence

Non-exclusive licence to reproduce the thesis and make the thesis public

I, Alar Paas,

1. grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright, my thesis

   “Testing Wireless Security Alarm Systems from the Estonian Market”,

   supervised by Danielle Melissa Morgan.

2. I grant the University of Tartu a permit to make the thesis specified in point 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 4.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in points 1 and 2.

4. I confirm that granting the non-exclusive licence does not infringe other persons’ intellectual property rights or rights arising from the personal data protection legislation.

Alar Paas

15/05/2024