A. Muñoz, C. Fernandez-Gago, and R. Lopez-villa, "A Test Environment for Wireless Hacking in Domestic IoT Scenarios", *Mobile Networks and Applications*, 2022.
http://doi.org/10.1007/s11036-022-02046-x
NICS Lab. Publications: https://www.nicslab.es/publications

Mobile Networks and Applications
https://doi.org/10.1007/s11036-022-02046-x

A Test Environment for Wireless Hacking in Domestic IoT Scenarios

Antonio Muñoz[1] · **Carmen Fernández-Gago**[1] · **Roberto López-Villa**[2]

Accepted: 23 May 2022
© The Author(s) 2022

Abstract
Security is gaining importance in the daily life of every citizen. The advent of Internet of Things devices in our lives is changing our conception of being connected through a single device to a multiple connection in which the centre of connection is becoming the devices themselves. This conveys the attack vector for a potential attacker is exponentially increased. This paper presents how the concatenation of several attacks on communication protocols (WiFi, Bluetooth LE, GPS, 433 Mhz and NFC) can lead to undesired situations in a domestic environment. A comprehensive analysis of the protocols with the identification of their weaknesses is provided. Some relevant aspects of the whole attacking procedure have been presented to provide some relevant tips and countermeasures.

Keywords IoT security · Domestic security · Network security · Hacking the IoT

1 Introduction

Nowadays, wireless protocols constitute an important part of the communication systems being used globally. They are fundamental parts on a wide variety of devices, from customer products like TV sets or smartphones, to professional and military equipment, including industrial machinery. Those devices and their wireless applications often transfer information that can be sensitive. Sometimes, these devices' integrity and availability depend direct or indirectly on these protocols.

Therefore, the protection against malicious (or unintended) attacks is significantly valuable and must be always considered. Most standard protocols implement cybersecurity methods, but their potential protection is not always the best. Bluetooth technology has been the subject of study in the face of many attacks. Mutchukota et al. [40] implement a Man-In-The-Middle attack based on the pairing weaknesses, Iqbal et al. [24] reveal some security gaps in Bluetooth architecture implementing a Denial of Service attack, others based on cracking [43] and mining and analyzing curve [2] while other studies focus on particular protocols such as the one used for Bluetooth mouse privacy filtering in [46]. GPS spoofing attacks were firstly reported by Warner et al. [64] followed by a long list of works based on software attacks [27, 66], creating false alarms [25] among others. In the case of Near Field Communication (NFC), it provides secured transaction between cell phones, which store data safely, and other NFC equipped devices. However, many security methods can be breached performing different versions of NFC wormhole attacks [13] exploiting software vulnerabilities [37, 39] or tampering tags [39], implementing URI obfuscation [38], as a consequence of not having any NFC message time-stamping method implemented, relay attacks may occur [22, 23] or corrupting data [16]. Pereira et al. [48] present RFID vulnerabilities by hacking the Authentication System of a University Campus on a Budget. In [59] how to intercept the Sector Sweep to Launch Man-in-the-Middle Attacks on Wireless IEEE 802.11ad Networks is reported. In [52] authors present injection attacks in 802.11n MAC frame aggregation. Other works [61, 69] exploit WSN (Wireless Sensor Networks) security issues or physical layer identification [7].

In order to validate that the performance of these protection methods is in line with the security requirements, they must be analysed and tested in detail. For that purpose,

✉ Antonio Muñoz
amunoz@lcc.uma.es

Carmen Fernández-Gago
mcgago@lcc.uma.es

Roberto López-Villa
roblopvil@uma.es

[1] Network, Information and Computer Security (NICS) Lab, University of Malaga, Street, Malaga 29001, Spain

[2] Testing & Certification S.A.U., Dekra, Street, Malaga, Spain

Published online: 14 October 2022

several tools are available. However, the main issue with these tools is that in most cases, they are standalone and used for a single specific protocol. Thus, this problem raises the need for a unified system that is able to perform different types of testing on at least, the most relevant protocols.

This work is based on implementing attacks to different wireless transmission technologies in a domestic scenario. In order to show this approach, a home scenario, in which certain number of IoT devices are connected, is provided. Further on, an analysis of the protocols and their weaknesses are analysed from a cybersecurity point of view. Further on, a description of the implementation of different attacks is provided. A brief description of the installation and configuration is given for their proper performance. Finally, a demonstration test suite is delivered including possible real-world applications, taken as ethical hacking attacks within our particular scenario.

Among the most outstanding contributions of the work presented in this paper, the following should be highlighted:

- The description of a real use case scenario with Internet of Things (IoT) devices, which intends to demonstrate the lack of security mechanisms for the protection of sensitive user data. Showing some of the weaknesses, as far as security is concerned, of certain devices that are currently traded.
- To demonstrate the existence of these weaknesses, a series of attacks have been implemented for each of the IoT devices involved in the previously described scenario.
- A thorough study of each of the attacks has been carried out together with their planning and implementation for the sake of the reproducibility of the implemented experiment.
- Finally, a series of countermeasures are proposed to mitigate or reduce the possible impact of each of the described attacks.

The rest of the paper is structured as follows. Section 2 presents the most relevant related work. Section 3 described the test environment scenario, the methodology and the most relevant protocol foundations and details for every attack. Some countermeasures and Discussion are given in Section 4. Section 5 concludes the paper and outlines the future work.

2 Related Work

IoT security has been a hot topic in recent years, as evidenced by the number of papers devoted to surveys and reviews of the state of the art of IoT security.

Some papers offer a more general overview, such as Sicari et al. [58]. On the other hand, there are other works that are more specialised in particular aspects of IoT, such as Roman et al. [53] and Weber and Studer in 2016 [65]. More recent works, such as that of Hypponen et al. [20] highlights the wide range of potential IoT-related challenges for consumers connecting to other traditional networks. An analysis of IoT security issues and an overview of the current and future trends in this area is presented in [53].

The research community seems to agree that the seemingly most important security challenge facing the IoT is what is known as 'cradle to grave'. That is, tracking from the development of secure IoT devices in terms of hardware and software, to the secure cooperation of heterogeneous IoT platforms and ecosystems. Nevertheless, this is not the only one, there are aspects such as the continuous integration of better security mechanisms in the most used IoT protocols, the definition of a more granular and user-friendly AAA infrastructure, incorporating mechanisms to facilitate the self-management of devices (detecting anomalies) among many others. There is a large body of work on hacking IoT devices. For example, Seralanthan et al. [57] present all the steps for hacking a connected webcam.

There are works such as Roberts et al. [51] that present a series of practical tips for finding vulnerabilities in IoT devices. Authentication among IoT devices is one of the most recurring security issues. To this end, radio frequency identification (RFID) technology has played an important role in providing efficient and secure identity security authentication services for IoT devices. The operation of RFID is based on tags that store information related to identities, these tags are read by readers that check and verify their identity against a database. All this can lead to various information leaks. This can lead to the possibility of different types of attacks on RFID, some of which are physical attack [9], eavesdropping attack [4, 28], and brute force attacks to read RFID tag information [4, 28, 54]. Traditional authentication schemes use non-volatile memory (NVM) [30] for key storage with the consequent problems of loss data [33]. There are different proposals to address this problem mainly based on hardware encryption such as Physical Unclonable Functions (PUFs). These make use of the random differences of the integrated circuits in the fabrication process to generate unique vital information [21] this introduces changes in the physical process, temperature gradients among other factors that make these functions unclonable. In such a way that in the face of different challenge inputs the PUF is able to map an unpredictable and unique response [18]. There are also others focused on blockchain security, such as [56] as well as a proposed mutual authentication protocol between RFIDs that eradicates the need for a trusted third party based on blockchain technology [63]. This work focused on domestic scenarios such as the one

discussed in this paper, as is the case of [14], which focuses on access control. This work describes the vulnerabilities found and proposes some possible countermeasures. However, this work dates from 2014, with the consequent technological evolution and focuses only on weaknesses identified in access control without proposing how to attack other vectors or carry out a whole reproducible process.

Others such as [36] look at how to map the attack surface of IoT devices following a series of steps. There are specific works for healthcare applications, such as [6], which provides a complete review of the most relevant aspects of security and privacy of IoT devices in these ecosystems. However, there are other works that carry out this type of more generic studies, such as [11].

Despite different approaches, most studies agree that for the development of security mechanisms, the specific characteristics of IoT (physicality, limitations, heterogeneity, connectivity, scalability) create challenges for the development of security mechanisms. However, as Roman et al. [53] argue, in some cases they are also new opportunities. There are different factors, such as the predictability of physical processes and the existence of neighbouring things, which analogously to social engineering mechanisms used to extract information and enforce security. They can be used to implement more optimal security mechanisms, with good results on issues such as anomaly detection through physical behaviour analysis and local watchdogs.

Other works describe a whole methodology with concrete cases. A manual for hacking IoT devices is presented in [47]. Gupta [15] presents a whole handbook for practical hacking of different devices.

There are also works focused on hacking particular protocols, such as in [34], which presents vulnerabilities in the Bluetooth protocol. Others are based on attacking devices, as is the case of [70] in which the security analysis of a smartphone is carried out to attack the domestic environment in which it is used as a controller of the IoT ecosystem.

Neshenko et al. [41] highlight the security assumed for commercial IoT devices due to the fact that they are marketed in embedded form. Notra et al. [44] show the patent shortcomings of security mechanisms of certain IoT devices on the market by hacking various household devices such as an alarm, a smart switch, and a smart light bulb. Other authors have reported studies on possible attacks on Internet of Medical Things (IoMTs) as Yang et al. suggests [68] (on devices such as defibrillator, pacemakers, insulin pumps and gastric electrical stimulator). Others detected weaknesses in the communication link between different implantable devices [31, 67]. Daniluk et al. [8] identified a possible attack based on cloning device identities. A number of security issues in what are known as implantable cardiac defibrillator devices were reported in [19]. Among the different problems detected, the loss of capacity of the device's own battery can cause unexpected failures or premature stops [3]. This could lead to serious consequences for the patient. Another problem is the possibility of modifications to the firmware of the device itself by possible attackers. Derived from the fact that a large part of medical devices can be controlled by other devices such as smartphones or personal computers, vulnerabilities in the latter could be exploited [50]. As an example of this, a recent case described by SweynTooth [12] in which up to a total of 12 flaws in the Bluetooth protocol have been identified. These can affect up to 450 different devices ranging from fitness devices to medical tools and implants, among others. While it is true that one has to question how real all of this is, Hassija et al. [17] provide insight into how realistic all of these attacks are, as well as their feasibility in real implementation cases.

After analyzing a certain number of studies on security challenges and mechanisms in a smart home, we can state that there are three main security and privacy issues: communication issues, device issues, and service issues [5]. There are different proposals to address the issue. In [60], a tiered framework at different levels (cloud, utility, third party and user interface) is proposed. Others focused on preserving user privacy [1, 29]. Security models for authentication and preserving the integrity of all transmitted messages [35]. Solutions oriented to provide security in the use of cell phones in wireless networks [32]. There are also solutions that focus on protecting the appliances involved in a smart home by proposing an enhanced security framework [26].

3 Test Environment

This section includes the complete test environment. First of all, we introduce the description of the scenario we have worked on, justifying with a potential real case the relevance of the implemented attacks. Secondly, the methodology implemented during all the experiments is presented. Finally, a description of the most important aspects of each of the attacks is given.

3.1 Application Scenario

Figure 1 depicts the scenario on which this study is based. This scenario describes a real world situation with which a large number of people can be identified. Different ordinary situations are presented with the aim of showing the impact that any of the attacks presented in this work can have on our daily lives. Firstly, users drive their car, which is equipped with a Movistar GPS system that allows the vehicle to be located at any time. Making use of the garage door opening system that makes use of the 433Mhz UHF protocol, they open the door and get ready to leave with the vehicle. They arrive at their destination and park the vehicle in a

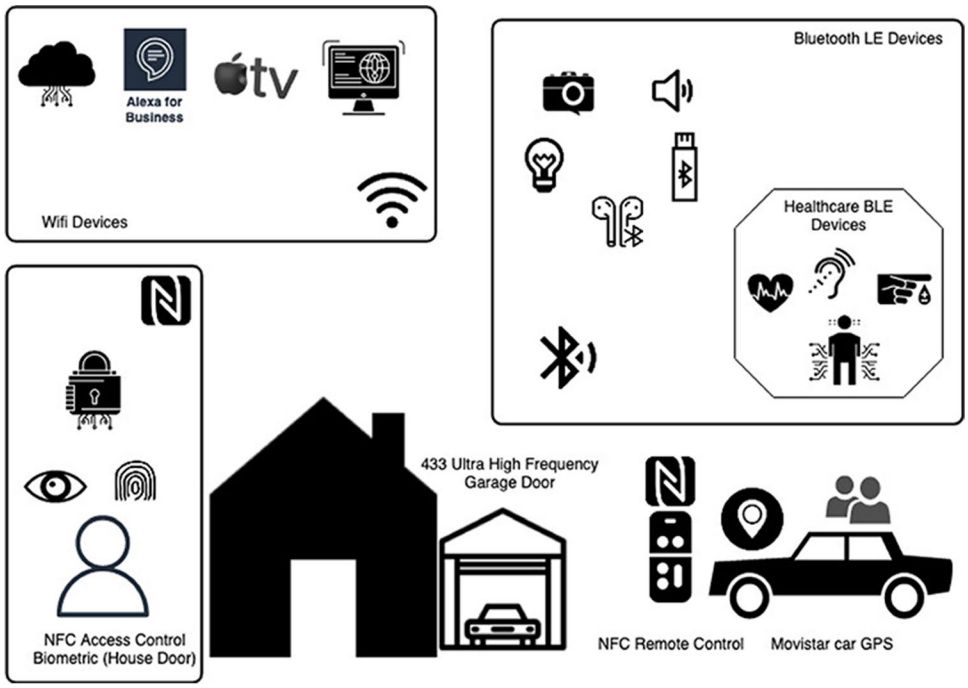

Fig. 1 Application scenario

designated area. From this moment on, two compromising situations arise. If an attacker is skilled to attack the protocol that controls the opening of the garage door, which is implementable by following the steps proposed below, the intruder would have access to the garage. Users do not worry that their car may be stolen since it is equipped with a GPS monitoring system for its location. They neglect to check thoroughly that all doors and windows were properly closed at the time of parking. In fact, they left one window half-opened, allowing skilled car thieves to gain access to the passenger compartment. They realize that the car is equipped with a GPS tracking system. However, the advanced skills of the thieves allow them to launch an attack on the GPS system in order to bypass the vehicle's monitoring system.

The home is provided with home automation equipment based on IoT devices that make use of different protocols. Access to the home is through a biometric device that works with both retina and fingerprint of each of the users residing in the house. This access control device works with the use of the NFC protocol. If an attacker is able to crack the protocol, this would allow them to gain access to the home. The box at the top left depicts different devices that work with wifi network access. If an attacker manages to gain control of the home wifi network, he would have access to all shared resources on the web (Alexa, pay TV subscription, internet, cloud accounts, etc.). And finally, we focus on a number of devices that work with the Bluetooth Low Energy protocol. The situation is as follows in this case, a neighbor as a joke intends to take over the controls of certain Bluetooth devices in this smart home as activating and deactivating a BLE speaker, as well as a BLE headset, plays with the on and off flashing of a BLE bulb and even sniffs photographs stored in a BLE equipped camera and a USB-BLE memory stick. We may think that the BLE attack by accessing all these devices is serious enough, but the issue is even trickier since the residents in the house wear some BLE healthcare devices. Indeed, it is a "joke in very bad taste" playing with a person's BLE hearing aid while it is operating. Although the situation gets worse when the prankster neighbor pretends to play with unknown BLE devices. Given that these are heartbeat monitoring and another blood sugar monitoring devices, it can be really dangerous. Once the complete scenario has been set out, we will show how the different attacks on the proposed protocols have been implemented. We proceed to the description of the methodology used in this study.

3.2 Methodology

Once the scenario is presented, different connection devices and the implementation protocols are selected as target to attacks. Let us introduce the protocols attacked WiFi, Bluetooth LE, GPS, NFC and 433 MHz RF (referred as 433 throughout the document). Every protocol has its main features and security structure, which is compromised together with the developed attacks. The selection criteria for the included protocols consist in its relevance and how generalised is its use and are used by devices in the daily life of any citizen. Attack to every protocol has been accomplished, including the driver and tools installation and configuration for that, and real world demonstrations to prove the attacks are completed. However, a detailed guide for the attacks

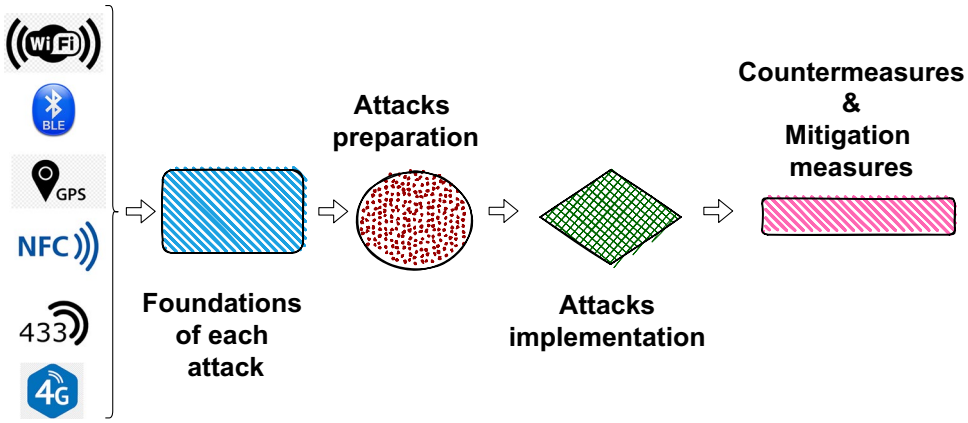

Fig. 2 Methodology workflow

reproduction is out of the scope of this paper, but the most relevant points have been outlined.

Figure 2 shows the methodology used for each of the protocols attacked. First of all, a detailed study of each of the protocols was carried out to identify possible weaknesses. Next, each of the attacks was prepared with the necessary instrumentation (Wireshark, Inspectrum, proxmark, srsLTE, nRF, etc.) for its implementation. Finally, we suggest a series of countermeasures and mitigation measures for the possible threats identified with some mechanisms that significantly reduce the possible risks.

Once the methodology is described, let us introduce the foundations of every protocol to proceed with the actual implementation of them.

3.3 Home Scenario Attacks

This section focuses on real-world security test cases that may be useful in order to understand how the attacks were implemented.

The target of our attack is a 433MHz garage door remote. For this purpose, NESDR Smart and GNU Radio Companion were used to capture the data sent by the remote. Then, a flow graph that graphically shows the signals and saves them in an output 'audio' file was built. The signal is captured by a running script on Arduino and also replies same sniffed sequence emitted byte, implementing a 'Replay Attack'.

The initial setup for this demonstration consists of the following hardware requirements: NESDR Smart, Arduino Nano with the 433 MHz RF emitter module, and a 433 MHz garage door remote. Then, connecting the NESDR Smart to any USB in the main system and signal is captured. The signal is analyzed and cloned as an essential step of this attack. Only modifying the bit stream inside the 'mySwitch. send' function allows coding other signals. Clicking the Upload button to load this code inside the Arduino board. Henceforth, this Arduino once powered on sends the raw bit stream. Finally, in less than 2 seconds the door was open.

The next attack objective is a MIFARE Classic 1K[1] card from a that stores money data for vending machines. It has a weak protection technology, so our Proxmark 3 can initiate a Nested Attack to obtain the keys. Also, the Courtois Dark Side Attack [42] can be executed, but it will not be covered in this test. After the keys are obtained, we dump all the information in the card and restoring it on one Chinese Magic backdoor tag. Also, the original UID will be inserted on the Magic card to complete the cloning. In particular, a Proxmark 3 EASY (or any other model), a MIFARE Classic 1K Chinese Magic backdoor tag, a target MIFARE Classic 1K tag, and a target MIFARE Classic 1K reader were used. The most relevant steps of the attack is once read starts, checking the top 18 default keys to decrypt the data sectors in the next step. We notice that four out of the total 32 sectors do not use any of the default keys. To reveal these keys, the Nested Attack script is launched. Then, all the keys for this card are printed inside the 'dump- keys.bin' file. By applying reverse engineering and comparing data from different amounts of money in the same card, it is possible to obtain how the money is coded, and then forge it. Finally the card is cloned.

The next step is attacking IoT WiFi light bulb from TP-Link, in particular, the LB130 model. For this purpose, a rogue access point(AP) is installed to read non-encrypted messages from devices connected to our AP in order to replicate packets. The message 'encryption' protocol that protects the data between the LB130 and the device that controls it (normally an iOS or Android device) is weak and therefore it was exploited. This protocol consists on a per-byte XOR function with a hard-coded value, so that knowing this value, any packet can be decrypted. This allowed the reverse engineering processes to know the previously

[1] MIFARE Classic Tool®. Google Play Store - IKARUS Projects. 2020. https://play.google.com/store/apps/details?id=de.syss.MifareClassicTool

mentioned ciphering method. Henceforth, we proceed downloading the same APK from APKMirror and installing it on the Android device. This old version also will prevent the LB130's firmware to be updated, and the vulnerability would likely be fixed. It is an indispensable step to enable the installation of apps from unknown sources in Android settings. Traffic is sniffed and analyzed using Wireshark tool until login credentials are identified. This allows the connection of the android device to the AP and plug the LB130 light bulb or turn it off.

The kitchen light bulb is the next target of attack. As already mentioned, it connects via bluetooth. The attack on BLE starts searching for near Bluetooth devices that are available, and it will allow to sniff a specified listed device. First, note the name that was automatically assigned to the light bulb inside the Magic Blue app. This is a hint of the light bulb's MAC address. Close the Android Magic Blue app and disable the Bluetooth from Android Settings to force a disconnection to the light bulb. The light bulb should appear on the list. Thus, a sniffer app is launched. Several dots will appear on the terminal indicating the data being captured. After pairing the app, try performing commands like turning on and off the light bulb. This process is usually unsuccessful, so you may need to try again disabling the Bluetooth, scanning on the sniffer and enabling the Bluetooth to once more select the light bulb on the terminal and the app. A successful capture should keep outputting dots to the terminal. Wireshark is used for packet injection. The packets should show more data than before, like the Source and Destination addresses. And merely using a new Command Line Interface (CLI) will render with the gatttool environment. Then, input 'connect' to let our system connect to the peripheral. The terminal should output the 'Connection successful' message that indicates that the pairing has, in fact, succeeded. To know the possible GATT handles for this peripheral, execute 'primary'. If the light bulb was turned on, the previous command should have turned it off. A message notifying the write was successful should be output. Then, let us open again the sniffed capture.

Finally, attacking Global Positioning System (GPS) implies generating GPS signals that include false location data, and their further emission using the LimeSDR Mini. Finally, a device with a GPS receiver obtains this data and the given false information is shown .

The initial setup for this demonstration test has three hardware requirements previously described. For the purpose of generating false GPS signals, we are using a sample list of locations bundled with one of the repositories.[2] These locations correspond to a sample Japanese rocket simulator. The different input location formats are detailed in the main repository.[3]

Once SDR is calibrated and ready to emit, let us start receiving GPS signals. Next step is opening GNU Radio Companion from the Ubuntu App Menu or by executing in a terminal gnuradio-companion, which from a File source (the one we generated with gps-sdr-sim) converts to complex numbers output, and finally input it into an sink. This sink is in charge of transferring the GPS signal information. Then, GPS spoofing takes place and starts to emit rogue GPS signals. In our test, the first fake location found is one of the Japanese Rocket Launch site in the Uchinoura Space Center, close to the Kimotsuki city.

4 Countermeasures and Discussion

Subsequently,a list of countermeasures to mitigate the risk of being target of most of the attacks is presented as well as a discussion intended to improve the security of the protocols themselves.

General GPS: the suggested countermeasure is to always use alternative geo-location methods to complement the GPS signal. One of the examples is the previously mentioned 'Bluetooth and WiFi Scanning' that comes implemented in Android. This will help mitigating the possible location errors related to fake GPS signals. However, this options may not be present in specific types of devices.

Movistar Car and other car GPS modules: while configuring the mobile app required to operate the auxiliary module, enable Engine Turn On, Engine Turn Off, Towed and Impact mobile notifications. These will notify each major event occurring in the car. Additionally, from the mobile OS perspective, configure mobile app notifications to always notify with sound, even when Do Not Disturb mode is enabled.

WiFi Lightbulb: as a general WiFi advice, always secure local WiFi connections by using WPA2 PSK AES only with secure (Upper/lowercase alphanumerical + symbols, 12+ characters) custom passwords. For critical environments, i.e. usage of WiFi cameras, the MAC address filtering should be applied, although it could be unsuccessful against MAC cloning attacks. Additionally, always check and update WiFi IoT devices and their apps to the latest firmware version and use custom passphrases if the option is available. Furthermore, always avoid operating WiFi IoT devices that send and/or receive weakly ciphered sensitive data.

BLE: if unsecured BLE lightbulbs are used, they might be only intended for non-critical house zones and secondary lights. An attacker could deny all access to the lightbulb

[2] bladeGPS:GitHub - OSQZSS. 2020. https://github.com/osqzss/bladeGPS

[3] GPS Signal Simulator. GitHub - OSQZSS. 2020. https://github.com/osqzss/gps-sdr-sim

functioning. Update app and lightbulb to latest firmware version and use custom passphrases if the option is available. Nonetheless, these kind of unsecured BLE devices are rarely updated to comply a higher security standard. As it is mentioned in the BLE Security subsection, there are safer encryption methods like Out-Of-Band and Passkey present in a wide variety of devices. Additionally, lower, if possible, the BLE range in order to only be able to manage it in the current room.

NFC: if the house door lock has a numpad for pin input, configure an additional 4/6-pin code which will pose a harder challenge for a possible attacker, as this works when the NFC tag has been sniffed. Use known to be safe tags like MIFARE Classic 1K EV1 or the newer MIFARE DESFire EV2.

433: one possible solution could be to lower the antenna range of the remote door opener in order to only be able to open the door within 3-4 meters, lowering the risk of 433 signal being sniffed. Also, an update to a more secure 866 Rolling Code system as explained in the 433 Security Structure subsection would improve greatly the odds of being sniffed.

Furthermore, we also consider a list of countermeasures that consist of the combination and interdependence of different protocols to strengthen the overall system security:

- We could improve the 433 garage door using a switch controlled by a Bluetooth LE beacon. The BLE beacon(s) could measure the distance between the user smartphone and the door within a short range of 2-3 meters. If the smartphone is not present or further from the maximum distance, manual/physical door activation should be needed, making the malicious access of an attacker harder to perform.
- For the NFC door lock, the use of a smartphone linked tag instead of physical tag could mitigate the chances of the NFC tag being cloned. Furthermore, the NFC reader could require a dynamic passkey given to the smartphone with the connection to a local WiFi API, to comply a Two Factor Auth. (2FA)-like method.

Pinto et al. [49] propose that software-based approaches could be applied for security purposes. Nevertheless, these methods are not sufficient. In this line, we believe that those methods need an enhancement using security-oriented technologies that promote hardware as the root of trust (Trusted Computing, Trusted Execution Environment, etc.). Indeed, as a challenge is proposed, a further study of using OPTIGA Trust X technologies[4] within different IoT devices from proposed scenario.

Some lines are identified as ongoing works. A final configuration for 4G, due to the mentioned technical issues, a successful testing environment for this protocol has been impossible and the manufactured is expected to release a new firmware version that mitigates the driver problem. Also, we are working on the support for additional IoT related protocols such as ZigBee, as one of the most implemented protocols in IoT devices; WiFi 5GHz: similar to the WiFi included in our guide, offering a significantly higher speeds; Thread based on IPv6 and 6LoWPAN, it is known as Google's ZigBee; And 2G: ancient mobile communication system that is still in use until further notice because it is offered as the fallback band for protocols like 4G and 5G.

Also, we have identified the limitations of current software. We believe that updating and developing new software that can cover the pertinent evaluation needs is an open research line. Since new vulnerabilities can be discovered and it is possible that our current environment could not be able to exploit them. To that purpose, new and more powerful tools that are able to execute more attacks could be found. In the case of our AR150 for the WiFi environment, the installation of many other modules that can exploit other vulnerabilities is allowed by default.

The development of an unified graphical interface where the tools can be set up and launched. This environment could serve to facilitate the evaluation labours, with the insertion of default templates and parameters modification.

At the same time, work is being done to make this guide available on an interactive web page, so that it can be presented for simple and open use on the web. The implementation of a web service for the collection of the methods presented in this Guide that integrates the possibility of adding new installation and test instructions for other protocols is being considered.

Studying extended approaches that makes use of security-oriented technologies promoting hardware as RoT. Evaluating the possible use of TEE or TC by implementing solutions in our scenario. Results can provide hopefully results. Also a further study of TC vs TEE for IoT is a ongoing work.

Finally, an automation software development for testing purposes is implemented. Some tests could be autonomously executed to test different attacks, such as Bluetooth, where it is possible to sequentially exploit every detected device by the antenna.

5 Conclusion

In this paper we have analysed the current situation and forward-thinking of security in presented technologies, and other ones like ZigBee and 5G. The chosen system media allows a total portability to be able to perform the mentioned tests in local domains, such as a research laboratory; or from a product

[4] https://www.infineon.com/dgdl/Infineon-OPTIGA%20TRUST%20X%20SLS%2032AIA-DS-v02_60-EN.pdf?fileId=5546d462602a9dc801606f1c2ebb7fe9

testing perspective, to be able of performing the tests directly on the client premises. The presented and detailed demonstration tests in this paper are real-world evaluations and respond to common weaknesses and vulnerabilities present in a surprisingly large amount of devices. Hence, they can be reproduced in research and development projects. Indeed, tests and attacks performed demonstrate the chosen protocols, when being erroneously implemented or using weak protection methods, may be totally vulnerable. Some examples are the WiFi or the NFC, where the devices do not verify the identity of the devices they connect to. As mentioned throughout the paper, options for security and hardening for each one of the protocols exist. However, if the manufacturers do not implement these new features, we will continue having the same weaknesses in the devices we use everyday. On the other hand, after the 4G protocol analysis, the found vulnerabilities were considerably less important, since their implementation is not trivial and are hardly implementable. In fact, their set of initial requirement to fulfill can hardly be met in a real-world scenario. With regard to the research and implementation labours, the process has had certain adversities that have slowed down the final result achievement. In the case of the WiFi environment, knowing the AR150 device uses an unofficial modified firmware, it has been subjected to several issues, such as the memory internal management, the external antennas and custom modules. To achieve a successful result, different alternative methods have been tried, by searching in amateur forums and official firmware pages. Also, for the GPS environment, several configurations and libraries were tried. Related to the issues obtained with respect to the 4G environment, the LimeSDR Mini driver, LimeSuite, is in continuous development, and the latest versions have been proved not to be stable nor reliable for our board. At the research process beginning, the driver was not able to autonomously calibrate the board, and different versions and manual builds were tried to troubleshoot the issue. Finally, we could not continue with this test, until the manufacturer updated the driver version, so once updated, everything worked as expected. Finally, for the NFC environment, our Proxmark 3 board seemed to have manufacturing calibration faults, as many times it was impossible to detect the NFC tags. By trial and error, all the tags could be read and modified in order to execute our attacks.

Acknowledgements This work has been partially supported by the Spanish Ministry of Science and Innovation through the SecureEDGE project (PID2019-110565RB-I00), and by the by the Andalusian FEDER 2014-2020 Program through the SAVE project (PY18-3724).

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature. Funding for open access charge: Universidad de Málaga / CBUA

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Abdallah A, Shen XS (2016) A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. IEEE Transactions on Smart Grid 9(1):396–405
2. Babamir SM, Nowrouzi R, Naseri H (2010) Mining bluetooth attacks in smart phones. In: International conference on networked digital technologies. Springer, Berlin, Heidelberg, pp 241–253
3. Battery-powered medical devices: their failure modes and mitigation strategies alerts, knowledge, exponent. https://www.exponent.com/knowledge/alerts/2018/11/battery-powered-medical-devices (Online). [Accessed Jan 2022]
4. Blanco J, Garcia A, Pastor JM, Canas V (2017) A multi-purpose UHF RFID tag emulator for communication protocols testing. In: Smart SysTech 2017; European Conference on Smart Objects, Systems and Technologies. VDE pp. 1–7)
5. Bugeja J, Jacobsson A, Davidsson P (2016) On privacy and security challenges in smart connected homes. In: 2016 European Intelligence and Security Informatics Conference (EISIC). IEEE, pp 172–175
6. Chacko A, Hayajneh T (2018) Security and privacy issues with IoT in healthcare. EAI Endorsed Trans Pervasive Health Technol 4(14):e2–e2
7. Danev B, Luecken H, Capkun S, El Defrawy K (2010) Attacks on physical-layer identification. In: Proceedings of the third ACM conference on Wireless network security. pp 89–98
8. Daniluk K, Niewiadomska-Szynkiewicz E (2012) Energy-efficient security in implantable medical devices. In: 2012 federated conference on computer science and information systems (FedCSIS). IEEE, pp 773–778
9. Devadas S, Suh E, Paral S, Sowell R, Ziola T, Khandelwal V (2008) Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications. In: 2008 IEEE international conference on RFID. IEEE, pp 58–64
10. ESA Navipedia Contributors. Principles of Interoperability among GNSS. ESA (2020)
11. Farooq MU et al (2015) A critical analysis on the security concerns of internet of things (IoT). Int J Comput Appl 111:1–6
12. Garbelini ME, Wang C, Chattopadhyay S, Sumei S, Kurniawan E (2020) Sweyntooth: Unleashing mayhem over bluetooth low energy. In: 2020 USENIX annual technical conference (USENIX-ATC 20). pp 911–925
13. Giese D, Liu K, Sun M, Syed T, Zhang L (2019) Security analysis of near-field communication (NFC) payments. arXiv preprint arXiv:1904.10623
14. Godha R, Prateek S, Kataria N (2014) Home automation: Access control for IoT devices. International Journal of Scientific and Research Publications 4(10):1
15. Gupta A (2019) The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things. Apress
16. Haselsteiner E, Breitfuß K (2006) Security in near field communication: strengths and weaknesses. Philips Semiconductors, Gratkorn, Austria

17. Hassija V, Chamola V, Bajpai BC, Zeadally S (2021) Security issues in implantable medical devices: Fact or fiction? Sustainable Cities and Society 66:102552
18. He Z, Wan M, Deng J, Bai C, Dai K (2018) A reliable strong PUF based on switched- capacitor circuit. IEEE Transactions on Very Large Scale Integration (VLSI) Systems 26(6):1073–1083
19. Hosseini-Khayat S (2011) A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices. In: 2011 5th international symposium on medical information and communication technology. IEEE, pp 6–9
20. Hypponen M, Nyman L (2017) The Internet of (Vulnerable) Things. Technology Innovation Management Review 7(4):5–11
21. Igier M, Vaudenay S (2016) Distance Bounding based on PUF. In: International conference on cryptology and network security. Springer, Cham, pp 701–710
22. ISO, Near Field Communication Interface and Protocol (NFCIP-1), ISO/EIC 18092:2013 (2013)
23. ISO, Near Field Communication Interface and Protocol-2 (NFCIP-2), ISO/EIC 21481:2012 (2013)
24. Iqbal MMW, Kausar F, Wahla MA (2010) Attacks on Bluetooth security architecture and its countermeasures. In: International conference on information security and assurance. Springer, Berlin, Heidelberg, pp 190–197
25. Jiang X, Zhang J, Harding BJ, Makela JJ, Domınguez-Garcıa AD (2013) Spoofing GPS receiver clock offset of phasor measurement unit. IEEE Transactions on Power PP:1–10
26. Komninos N, Philippou E, Pitsillides A (2014) Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials 16(4):1933–1954
27. Larcom JA, Liu H (2013) GPS vulnerability analysis in surface transportation. UMass Dartmouth 19th Annual Sigma Xi Research Exhibit, Dartmouth, MA
28. Lee YC, Hsieh YC, You PS, Chen TC (2008) An improvement on RFID authentication protocol with privacy protection. In: 2008 Third international conference on convergence and hybrid information technology. IEEE, vol 2, pp 569–573
29. Lee S, Kim J, Shon T (2016) User privacy-enhanced security architecture for home area network of Smartgrid. Multimedia Tools and Applications 75(20):12749–12764
30. Li X, Niu J, Khan MK, Liao J (2013) An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications 36(5):1365–1371
31. Li C, Raghunathan A, Jha NK (2011) Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In: 2011 IEEE 13th international conference on e-health networking, applications and services. IEEE, pp 150–156
32. Li T, Ren J, Tang X (2012) Secure wireless monitoring and control systems for smart grid and smart home. IEEE Wireless Communications 19(3):66–73
33. Liang W, Fan Y, Li KC, Zhang D, Gaudiot JL (2020) Secure data storage and recovery in industrial blockchain network environments. IEEE Transactions on Industrial Informatics 16(10):6543–6552
34. Lonzetta AM, Cope P, Campbell J, Mohd BJ, Hayajneh T (2018) Security vulnerabilities in Bluetooth technology as used in IoT. Journal of Sensor and Actuator Networks 7(3):28
35. Mantoro T, Ayu MA, binti Mahmod SM (2014) Securing the authentication and message integrity for Smart Home using smart phone. In: 2014 International conference on multimedia computing and systems (ICMCS). IEEE, pp 985–989
36. Miessler D (2015) IoT attack surface mapping. Presentation at DEFCON. Accessed 29 Sept 2018
37. Miller C (2012) Exploring the NFC attack surface. presented at Black Hat, Las Vegas, USA
38. Mulliner C (2009) Vulnerability analysis and attacks on NFC-enabled mobile phones. Proceedings of International Conference on Availability, Reliability, and Security, 695–700
39. Mulliner C (2008) Attacking NFC mobile phones. presented at EUSecWest, London, UK
40. Mutchukota TR, Panigrahy SK, Jena SK (2011) Man-in-the-middle attack and its countermeasure in bluetooth secure simple pairing. International conference on information processing. Springer, Berlin, Heidelberg, pp 367–376
41. Neshenko N, Bou-Harb E, Crichigno J, Kaddoum G, Ghani N (2019) Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials 21(3):2702–2733
42. Courtois Nicolas T (2009) Card-Only Attacks on MiFareClassic. University College London, UK
43. Nilsson DK, Porras PA, Jonsson E (2007) How to secure bluetooth-based pico networks. In: International conference on computer safety, reliability, and security. Springer, Berlin, Heidelberg, pp 209–223
44. Notra S, Siddiqi M, Gharakheili HH, Sivaraman V, Boreli R (2014) An experimental study of security and privacy risks with emerging household appliances. In: 2014 IEEE conference on communications and network security. IEEE, pp 79–84
45. Padgette J, Bahr J, Batra M, Holtmann M, Smithbey R, Chen L, Scarfone K (2017) Guide to Bluetooth Security. National Institute of Standards and Technology
46. Pan X, Ling Z, Pingley A, Yu W, Zhang N, Fu X (2012) How privacy leaks from bluetooth mouse? In: Proceedings of the 2012 ACM conference on Computer and communications security. pp 1013–1015
47. Papp D, Tamás K, Buttyán L (2019) IoT hacking-a primer. Infocommunications Journal 11(2):2–13
48. Pereira H, Carreira R, Pinto P, Lopes SI (2020) Hacking the RFID-based authentication system of a university campus on a budget. In: 2020 15th Iberian conference on information systems and technologies (CISTI). IEEE, pp 1–5
49. Pinto S, Gomes T, Pereira J, Cabral J, Tavares A (2017) IIoTEED: an enhanced, trusted execution environment for industrial IoT edge devices. IEEE Internet Computing 21(1):40–47
50. Pycroft L, Aziz TZ (2018) Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. Expert Rev Med Devices 15(6):403–406. https://doi.org/10.1080/17434440.2018.1483235
51. Robberts C, Toft J (2019) Finding vulnerabilities in IoT devices: Ethical hacking of electronic locks
52. Robyns P, Quax P, Lamotte W (2015) Injection attacks on 802.11 n MAC frame aggregation. In: Proceedings of the 8th ACM conference on security & privacy in wireless and mobile networks. pp 1–11
53. Roman R, Lopez J, Gritzalis S (2018) Evolution and trends in the security of the internet of things. IEEE Computer 51(16–25):2018
54. Seis A, Saima SE, Rivest R (2004) Security and privacy aspects of low cost radio frequency identification system. In: Proceeding of the 1st international conference on security in pervasive computing. Springer, pp 201–212
55. Security contactless smartcard (2008) Digital Security group. Radboud University, Nederlands
56. Sengupta J, Ruj S, Bit SD (2020) A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications 149:102481
57. Seralathan Y, Oh TT, Jadhav S, Myers J, Jeong JP, Kim YH, Kim JN (2018) IoT security vulnerability: A case study of a Web camera. In: 2018 20th International conference on advanced communication technology (ICACT). IEEE, pp 172–177

58. Sicari S et al (2015) Security, privacy and trust in Internet of Things: The road a head. Computer Networks 76:146–164
59. Steinmetzer D, Yuan Y, Hollick M (2018) Beam-stealing: Intercepting the sector sweep to launch man-in-the-middle attacks on wireless IEEE 802.11 ad networks. In: Proceedings of the 11th ACM conference on security & privacy in wireless and mobile networks. pp 12–22
60. Stojkoska BLR, Trivodaliev KV (2017) A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production 140:1454–1464
61. Sun Y, Wang X, Zhou X (2011) Jamming attack in wsn: A spatial perspective. In: Proceedings of the 13th international conference on Ubiquitous computing, pp. 563–564
62. Vanhoef M, Piessens F (2017) Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. imec-DistriNet, KU Leuven. https://papers.mathyvanhoef.com/ccs2017.pdf
63. Wang S, Zhu S, Zhang Y (2018) Blockchain-based mutual authentication security protocol for distributed RFID systems. In: 2018 IEEE Symposium on computers and communications (ISCC). IEEE, pp 00074–00077
64. Warner JS, Johnston RG (2003) GPS spoofing countermeasures. Homeland. Security Journal 25(2):19–27
65. Weber RH, Studer E (2016) Cyber-security in the Internet of Things: Legal aspects. Computer Law & Security Review 32(5):715–728
66. Wesson K, Shepard D, Humphreys T (2012) Straight talk on anti-spoofing. GPS World, pp 32–63
67. Xu T, Wendt JB, Potkonjak M (2014) Matched digital PUFs for low power security in implantable medical devices. In: 2014 IEEE international conference on healthcare informatics. IEEE, pp 33–38
68. Yang Q, Mai S, Zhao Y, Wang Z, Zhang C, Wang Z An on-chip security guard based on zero-power authentication for implantable medical devices. In: 2014 IEEE 57th international midwest symposium on circuits and systems (MWSCAS). IEEE, pp 531–534
69. Yarbrough B, Wagner N (2018) Assessing security risk for wireless sensor networks under cyber attack. In: Proceedings of the annual simulation symposium. pp 1–12
70. Yoon S, Park H, Yoo HS (2015) Security issues on smarthome in IoT environment. In: Computer science and its applications. Springer, Berlin, Heidelberg, pp 691–696

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.