Source Summaries

Quintin Walters, Joshua Niemann, Connor Leavesley,
Daniel Capps, Jacob Ruud

April 5, 2020

Contents

1 Summary 1

1.1 Security Analysis of Bluetooth Technology

1.1.1 Group Member

Quintin Walters

1.1.2 Citation

Daniel Filizzola, Sean Fraser, and Nikita Samsonau. Security Analysis of Bluetooth Technology, 2018. URL `https://courses.csail.mit.edu/6.857/2018/project/Filizzola-Fraser-Samsonau-Bluetooth.pdf`

1.1.3 Main Idea

The authors detail the security methods used in Bluetooth versions 4.X, attempt to show attacks that bypass these methods, and describe ways to harden Bluetooth security against these attacks.

1.1.4 Theory

Game Theory is the primary theory being tested in this article. The authors attack various vulnerabilities in the Bluetooth protocol in order to determine methods to increase the relative security of the protocol.

1.1.5 Method

The researchers theorized and tested primary attacks against the Bluetooth security model: Active Eavesdropping and Passive Eavesdropping. Their attacks built upon the works by Da-Zhi Sun et al., Cope et a., Das et al., and Ryan. The assets used were a Raspberry Pi running Debian, an Ubertooth, TaoTronics TT-BH07 Bluetooth Headphones, a Logitech MX Master Mouse, and a Galazy S7 Edge. The authors modified existing Bluetooth utilities for their attacks and wrote some scripts of their own.

1.1.6 Findings

The authors managed to exploit their theorized vulnerabilities successfully. They found that the JustWorks authentication method used by headsets and headphones are insecure against active eavesdropping attacks with unsophisticated hardware. The researchers also discovered that, while difficult, passive eavesdropping is still successful against hardware running Bluetooth 4.1 and recommend moving to version 4.2 or greater. They also found that devices using LE Secure Connections or Secure Simple Pairings are secure against these specific attacks.

1.1.7 Future Directions

The future directions for Active Eavesdropping is to expand and cover more than JustWorks devices, this would include attacks against mice and keyboards. The next steps for Passive Easedropping is to use the extrapolated information to decrypt packets for further analysis and to attack other devices like keyboards and medical implants, this can be used to gather sensitive information like passwords and health data. They also stated that they could combine the two attack types to inject malicious packets or modify existing ones for other attacks against the devices. Finally, they could also do research on the vulnerabilities in Bluetooth 5.0.

1.2 Extracting the Security Features Implemented in a Bluetooth LE Connection

1.2.1 Group member

Joshua Niemann

1.2.2 Citation

A. M. Robles-Cordero, W. J. Zayas, and Y. K. Peker. Extracting the Security Features Implemented in a Bluetooth LE Connection. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 2559–2563, 2018. doi: 10.1109/BigData.2018.8622000

1.2.3 Main Idea

The authors detail the encryption and authentication standards found in the Bluetooth Low Energy Protocol, from Bluetooth 4.0 to Bluetooth 5.0. The researchers also look at several BLE devices to analyze their security models.

1.2.4 Theory

Game Theory is the primary theory being tested in this article. The authors examine various versions of the Bluetooth protocol to determine which versions have the best security measures in place. In addition, the authors analyze BLE devices in an effort to learn which devices and device manufacturers have the best security.

1.2.5 Method

The researchers found that many modern fitness trackers use older versions of Bluetooth low energy. They also found that these fitness trackers often do not enable optional features that make bluetooth much more secure. As a result, most of the encryption was trivial to decrypt. The researchers then created an app that uses the Bluetooth sniff log functionality present in the developer section in Android to extract the security features of a bluetooth low energy device.

1.2.6 Findings

The authors managed to exploit their theorized vulnerabilities successfully. They found that the JustWorks authentication method used by headsets and headphones are insecure against active eavesdropping attacks with unsophisticated hardware. The researchers also discovered that, while difficult, passive eavesdropping is still successful against hardware running Bluetooth 4.1 and recommend moving to version 4.2 or greater. They also found that devices using LE Secure Connections or Secure Simple Pairings are secure against these specific attacks.

1.2.7 Future Directions

The authors want to make their app much more usable to the average consumer. Right now it's very oriented toward technical-minded researchers.

1.3 Finding Vulnerabilities in IoT Devices: Ethical Hacking of Electronic Locks

1.3.1 Group Member

Connor Leavesley

1.3.2 Citation

Christopher Robberts and Joachim Toft. Finding Vulnerabilities in IoT Devices: Ethical Hacking of Electronic Locks, 2019. URL `https://pdfs.semanticscholar.org/3eb1/c453464f50c30b2dfb2aff705d45bfe7a6d1.pdf`

1.3.3 Main Idea

The authors outline how to approach attacking Bluetooth locks. They use well documented attacks to discover vulnerabilities in a Bluetooth low energy lock.

1.3.4 Theory

Game theory is being utilized to test the security of the lock and see where the vulnerabilities in the lock lie.

1.3.5 Method

The authors create a threat rating system following the DREAD model is to accurately represent the threat of the lock being successfully attacked. They make three threat models: unauthorized lock access, avoidance of logging, and denial of service. They use a Bluetooth man in the middle attack to gather information about the lock's Generic Attribute Profile (GATT), how the application connected to the lock, hosted services, and other characteristics of the lock. Using the GATT, an attacker could use a fake lock hosted on a Arduino board to connect to the application, and then forward all information to the actual lock. Next, the

authors test access permission edge cases to see when access could be abused by an attacker to bypass controls. The authors then reversed the app to gather further insight on how the app connected to the lock.

1.3.6 Findings

Not much was able to be done in the way of breaking into the lock. Some patterns were found in the communication scheme, but nothing to indicate how the application was encrypting the connection. The authors lauched a replay attack, but this was ineffective. Fuzzing was similarly ineffective. If the owner of the lock granted an attacker permission to access it, disconnects their internet, and then the attacker's permission was revoked, the attacker can still access the lock. In the app, a possible encryption key for a database was found, but not pursued.

1.3.7 Future Directions

The authors would like to see a more structured method developed to analyze the security of Bluetooth devices, as many of the approaches they took were very time consuming.

1.4 Security Evaluation and Exploitation of Bluetooth Low Energy Devices

1.4.1 Group Member

Connor Leavesley

1.4.2 Citation

Anthony J Rose. *SECURITY EVALUATION AND EXPLOITATION OF BLUETOOTH LOW ENERGY DEVICES*. PhD thesis, 2017. URL `https://apps.dtic.mil/dtic/tr/fulltext/u2/1054747.pdf`

1.4.3 Main Idea

In his thesis, Captian Rose attemps to provide the industry with a wholistic look on the security of the low energy bluetooth protocol. He uses four different methods in an attempt to cover a wide range of conigurations and scenarios to really put this protocol to the test.

1.4.4 Theory

Game Theory is the primary theory being tested in this article. Captain Rose proposes multiple different scenarios where the bluetooth protocol is vulnerable in order to better understand how to secure it in the future.

1.4.5 Method

Captain Rose and his supporters used multiple different methods to test the strength and security of the Bluetooth protocol. First, he used a benchmark open-source range-finding tool to determine the location of Bluetooth devices through a novel distance estimation method, increasing the state-of-the-art device location distance from 50 meters up to 1,000 meters. Second, he evaluated 17 individual Bluetooth Low Energy devices for vulnerabilities in their operating system. Thirdly, he used user behavior analytics to demonstrate how malicious actors can exploit vulnerabilities for unauthorized device access and obtain sensitive information

1.4.6 Findings

Captain Rose's research revealed that 13 out of 17 (75 percent) of the tested devices contained at least one vulnerability resulting in unauthorized access. However, he did find that countermeasures to BLE attacks already exist and most require minimum implementation and development by manufacturers. More complex mediation techniques exist for issues that are not solved by the initial mediation techniques.

1.4.7 Future Directions

Since Captain Rose's work was done on an outdated bluetooth protocol (4.1) he mentions that there is room for others or himself to do research on devices implementing the newest protocol. He also recommends research into newly release bluetooth devices such as Lockitron or Schlage. He also states that he did not do any work with the firmware of the devices he tested so there is room for others to continue his work there. Along with that, he states that no research was done on attempting to clone the devices that he was testing, so there is more work to be done there.

1.5 Security Vulnerabilities in Bluetooth Technology as used in IoT

1.5.1 Group Member

Daniel Capps

1.5.2 Citation

Angela M Lonzetta, Peter Cope, Joseph Campbell, Bassam J Mohd, and Thaier Hayajneh. Security vulnerabilities in bluetooth technology as used in iot. *Journal of Sensor and Actuator Networks*, 7(3):28, 2018. URL `https://www.mdpi.com/2224-2708/7/3/28`

1.5.3 Main Idea

This study is about understanding Bluetooth and Iot(Internet of Things) devices. They go in depth on the importance of understanding Bluetooth, the differet attacks possible against Bluetooth and IoT devices, and how to mitigate these attacks using different tequniques.

1.5.4 Theory

Game Theory is the primary theory being used in this article. The authors gathered information about many vulnerabilities and exploits in Bluetooth/Iot and determined different mitigation tequniques for each of them.

1.5.5 Method

The researchers explained the inner workings of IoT and Bluetooth and then gathered different information on attacks to Bluetooth and Iot. Then, by using the information they found they determined different risk mitigation tequniques for users of Bluetooth and IoT devices.

1.5.6 Findings

The authors presented multiple vulnerabilities and attacks against Bluetooth and IoT and risk mitigations to combat them, the most notable of them being more awareness from the user's perspective on security issue with bluetooth. The main attacks showcased here are PIN Cracking, Man-in-the-M(MITM), BlueJacking, BlueBorne, Fuzzing, Reflection/Relay, Backdoor, Denial of Service(DOS). Many more attacks are mention as well.

1.5.7 Future Directions

Can the analysis tequniques use here be used for any other wireless standard? Could there be an attack on BLE that has to do with power consumtion? What methods can we use to more properly inform users of the risks of IoT and Bluetooth so that they may mitigate said risks?

2 Summary 2

2.1 Analyzing the Security of Bluetooth Low Energy

2.1.1 Group Member

Connor Leavesley

2.1.2 Citation

Seth Sevier and Ali Tekeoglu. Analyzing the Security of Bluetooth Low Energy, 2019. URL https://www.researchgate.net/profile/Ali_Tekeoglu2/publication/333228988_Analyzing_the_Security_of_Bluetooth_Low_Energy/links/5de01b6a4585159aa4518887/Analyzing-the-Security-of-Bluetooth-Low-Energy.pdf

2.1.3 Main Idea

The authors aim to explain how Bluetooth LE protocol works and the cryptographic weaknesses in the protocol.

2.1.4 Theory

This paper is applying Game Theory. A successful cryptographic attack is a loss for the security of the protocol.

2.1.5 Method

The authors first sniffed the Bluetooth traffic with a Ubertooth using the BlueZ Bluetooth driver and associated Ubertooth drivers. Using the Blueooth handshake, the authors used Crackle to crack the Temporary Key due to its restricted key space. The Temporary Key was then used to gain access to the Long Term Key (LTK). The LTK was then used to decrypt any future communication traffic in Wireshark.

2.1.6 Findings

The authors found that the keyspace of the Temporary Key is very restricted, allowing for a very quick brute force attack. They also found that Bluetooth Low Energy was susceptible to a number of attacks due to the low power requirements: denial of service and replay attacks. It was also found that Ubertooth struggled to capture a complete pairing event. The authors suggest that the Ubertooth should be as close as possible to the source transceiver to mitigate this issue.

2.1.7 Future Directions

Many vendors likely do not implement the Bluetooth stack correctly. These vendors may also use the same stack across multiple devices. Areas of further research should focus on individual devices from the same vendor to attempt to find vulnerabilities that affect entire product lines.

2.2 Wiegand Protocol Access: A Decade of Decryption

2.2.1 Group Member

Quintin Walters

2.2.2 Citation

Brandon Chung. Wiegand Protocol Access: A Decade of Decryption, 2017. URL `http://www.cs.tufts.edu/comp/116/archive/fall2017/bchung.pdf`

2.2.3 Main Idea

Brandon Chung covers what the Wiegand Protocol is, the historic vulnerabilities and hacks, what vulnerabilities still exist, and how to protect yourself against them. He spends a large amount of time on the historic attacks because most of them are still applicable, the protocol has not been hardened against them and as a result it is still very easy to exploit.

2.2.4 Theory

Chung applies Game Theory in his work, he treats the security of the Wiegand Protocol as a zero sum game in which any method of bypass is a loss for the defenders. He highlights historic vulnerabilities of the protocol that are still in existence to reinforce this belief.

2.2.5 Method

The author primarily presents the findings of others, he does little original research of his own. However, he does use an Arduino device to attack an unnamed Wiegand RFID reader. He connects his Arduino device to the Wiegand DATA 0 and DATA 1 wires, then he uses monkeyboard's "Wiegand Protocol Library for Arduino" to verify that the inherent vulnerabilities in the protocol still exist. Chung provides instructions and sample code for readers to attempt this on their own devices. This attack is the basis of the attacks done by Bernard Mehl (2015) and Zac Franken (2007), two attacks that Chung wrote in depth about.

2.2.6 Findings

Brandon Chung found that Wiegand devices are still vulnerable to decade old attacks. These attacks have been extensively documented and Chung duplicated the early stages of them to prove that they would still work. Using an arduino device, or similar microcontroller, an attacker can intercept and then duplicate the signals sent by a Wiegand device to the

control server. This attack can capture and repeat and authorized card without needing to physically duplicate the card.

2.2.7 Future Directions

Chung lays out multiple methods for future implementation to secure Wiegand devices. He recommends that the protocol be adapted to allow for encrypted keycards and the rejection of keycards that are not properly encrypted, he also recommends that the actual readers implement hardware methods to detect when the device has been tampered with and to report that tampering immediately to the controller. Further upgrades include remote firmware detection and updates, Wiegand devices typically are not able to be updated without direct physical contact which disincentivizes updating the readers unless absolutely necessary.

2.3 Survey on Various Door Lock Access Control Mechanisms

2.3.1 Group Member

Joshua Niemann

2.3.2 Citation

R. S. Divya and M. Mathew. Survey on various door lock access control mechanisms. In *2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT)*, pages 1–3, April 2017. doi: 10.1109/ICCPCT.2017.8074187

2.3.3 Main Idea

The authors compare different types of door lock authentication measures and their overall security.

2.3.4 Theory

The authors are applying Game Theory by directly comparing each individual authentication method.

2.3.5 Method

The authors directly compare different authentication methods using different factors using characteristics that would matter to a user in addition to the overall security of the system. For user factors, factors considered include include battery life, ease of use and what happens if a credential is misplaced, stolen or forgotten. As for security, factors considered included the a user passing off a credential to an unauthorized party, the ability to spoof a credential, and the ease of bypass for a mechanical system.

2.3.6 Findings

The authors find that no one current system could be considered the most secure, and that each system has individual strengths. As each method does better in different ways, emphasis should be instead placed on ensuring the use of the lock that is most suited for the use case in which it is placed.

2.3.7 Future Directions

The authors suggest using the knowlege of authentication system problems in order to build a new system, taking in mind the strengths and weaknesses for each category of authentication.

2.4 Bluetooth Low Energy and Smartphones for Proximity-Based Automatic Door Locks

2.4.1 Group Member

Daniel Capps

2.4.2 Citation

Tim Andersson. Bluetooth low energy and smartphones for proximity-based automatic door locks, 2014. URL `http://www.diva-portal.org/smash/get/diva2:723899/FULLTEXT01.pdf`

2.4.3 Main Idea

The authors attempt to evaluate Bluetooth Low Energy as a technology by focusing on its use in door locks that automatically unlock based on the proximity of a smartphone.

2.4.4 Theory

Game theory. The authors try to determine ways to use the Proximity-based Automatic Door Locks with Bluetooth Low Energy without causing any adversaries to be able to exploit the locks.

2.4.5 Method

The author's main method for testing their hypothesis had two halfs. The first half was to implement an application for iOS that would be able to unlock/lock the door lock, and the second half was to measure the Received Signal Strength Indicator (RSSI) between the phone and the door lock in order to ensure that the door would only unlock if the phone was in close enough proximity, and otherwise would be locked.

2.4.6 Findings

The authors gained a lot of knowledge pertaining to how suitable Bluetooth Low Energy is for automatic door locks, including what restrictions and possibilities exist on the iOS platform for developing Bluetooth Low Energy applications. The authors primarily learned that using this method they determined that they couldn't differentiate between the two sides of the door the user was located on, that the applications effect on the battery life of the phone was negligible, the connection latency was sufficiently small for use in practice. The author's conclusion is that Bluetooth Low Energy is a suitable technology for proximity-based door locks.

2.4.7 Future Directions

Can you improve the implemented solution so that there is no limit on how many people can be in close proximity to the lock at once? Is there a better alternative to Bluetooth Low Energy in the case of Proximity-based door locks?

2.5 Security Vulnerabilities of Bluetooth Low Energy Technology (BLE)

2.5.1 Group Member

Jacob Ruud

2.5.2 Citation

Harry O'sullivan. Security vulnerabilities of bluetooth low energy technology (ble). URL `http://www.cs.tufts.edu/comp/116/archive/fall2015/hosullivan.pdf`

2.5.3 Main Idea

Author Harry O'Sullivan along with mentor Ming Chow attempt to analyze the security of bluetooth low energy technology. They focus specifically on how BLE devices communicate with each other and how the communication between devices could be exploited by attackers.

2.5.4 Theory

O'sullivan applies Game Theory in his work on BLE devices. Posing as an attacker he and attempts to simulate attack scenarios treating a compromise of sensitive information as a win.

2.5.5 Method

The author presents three different methods to compromise BLE as part of his research. The first method he attemps is an eavesdropping attack, during which he tries to capture information about a bluetooth host device using a sniffer. The second attack method he outlines is Man-in-the-middle, to explain which he refers to research done by lecturers at

Marthandam College. The third attack scenario he describes is denial of service. During his explaination he outlines work done by researchers at University of Utah, as well as an attack technique called fuzzing.

2.5.6 Findings

The main findings ot this paper present the vulnerabilities of the BD ADDR field which is present in all BLE communication. O'Sullivan found that an attacker could use bluetooth fuzzing to determine the master source of a bluetooth connection and potentially forge a connection to it. Not to mention the fact that BD ADDR's are not globally unique so an attacker could try to spoof their BD ADDR until packets start flowing in.

2.5.7 Future Directions

The author does not include any future directions at the end of his work. Bluetooth Low Energy has been tested extensively since its inception, and I can only assume that O'Sullivan believes that there is work out there testing every corner or bluetooth low energy. I do not necessarily agree with his thoughts but that is all there is to report with this paper.

3 Summary 3

3.1 Breaking Access Controls with BLEKey

3.1.1 Group Member

Quintin Walters

3.1.2 Citation

Mark Baseggio and Eric Evenchick. Breaking Access Controls with BLEKey, 2015. URL `https://www.blackhat.com/docs/us-15/materials/us-15-Evenchick-Breaking-Access-Controls-With-BLEKey-wp.pdf`

3.1.3 Main Idea

Mark Baseggio and Eric Evenchick outline the simplicity of the Wiegand protocol. They then explain the BLEKey, how they built it, and how it is used to attack Wiegand capable card readers. The authors indicate that similar research has been done in the past but they wished to improve upon it by implementing Bluetooth communications in order to reduce the risk of discovery by retrieval.

3.1.4 Theory

The theory applied by the authors is game theory, they demonstrate a vulnerability of the Wiegand protocol and then go about demonstrating a method to exploit it.

3.1.5 Method

Baseggio and Evenchick custom developed the hardware for the BLEKey using KiCad and a pre-built Bluetooth Low-Energy module. They then programmed it with the ARM GCC compiler and the Nordic Firmware updaters. The authors then attach the BLEKey to a Wiegand interface using hte insulation displacement connector on the tool.

3.1.6 Findings

The authors found that they could effectively intercept and store the card data as it is transmitted along the wires. They also found that they could remotely connect to the BLEKey to pull the card data from it, do a replay attack with a stored card, or play a custom card number. This can be used with great affect by penetration testers with even lower risk of discovery than prior devices.

3.1.7 Future Directions

Future research and development of the BLEKey can involve the addition of cellular radios, this can allow testers to use the device with even less risk of discovery along with adding the possibility of storing the card data off-site instead of on the BLEKey itself. Another path of future development can involve a method to tie the BLEKey into the card reader power supply so that it does not have to rely on a battery. This would allow testers to use it on longer term engagements without needing to risk discovery by replacing the battery.

3.2 Smart Locks: Lessons for Securing Commodity Internet of Things Devices

3.2.1 Group Member

Daniel Capps

3.2.2 Citation

Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security*, pages 461–472, 2016. URL `https://people.csail.mit.edu/dtl/pdf/ho-smartlocks.pdf`

3.2.3 Main Idea

The authors examine the security of smart locks and present three types of attacks against them. The authors also analyze five commercially used locks with their focus being how they fair against these attacks. The analysis the authors use revealed flaws in the design, implementation, and interaction models of existing locks can be exploited by multiple adversaries. Giving the adversaries capabilities from unauthorized passage to irrevocable control of the lock. The authors also propose several mitigation techniques for the attacks they present. The author's goal is informing people about the security challenges in the system design and functionality from new IoT systems.

3.2.4 Theory

Game Theory. The authors determine different types of attacks and mitigation techniques for smart locks against different types of adversaries.

3.2.5 Method

The authors use different tests for each attack vector using a specific environment. The three attack vectors described by the authors are State Consistency attacks, Unwanted Unlocking, and Privacy Leakage. The State Consistency attacks exploit the trust between the user's mobile application and the lock. Specifically where the lock needs the user to send data to the server for them and won't update their privileges if they're offline. This allows revoked users to gain access to a lock even if the owner changed their permissions on the server.

Unwanted Unlocking deals with certain conditions being met for unlocking the lock, but said conditions having edge cases where adversaries could unlock the door. An example of this is a Side-of-the-Door attack where an authorized user gets too close to the door from the inside and the lock either automatically unlocks or simply requires a touch from the adversary right outside the door in order to gain access. Privacy Leakage has to do with the server being able to see logs from houses unencrypted on the server side. Allowing any adversary with access to the server to see the logs of different people using those smart locks. The authors also tested different methods for mitigating these problems.

3.2.6 Findings

The authors implemented mitigation techniques for the attack vectors they found against smart locks. For State Consistency attacks, the authors used an access control list stored on the lock that would request updates and send log data each time an honest user was nearby. They also had the smart lock deny people access if they couldn't connect to the server and they were determined to be untrustworthy. For Privacy Leakage, the authors use a key generated on the lock that's sent to the user over BLE and upload the encrypted logs to the website. Allowing a user to see their logs over the internet without their logs being compromised. For Unwanted Unlocking, the authors used Vibrato. Which has the lock send a signal through a Body-Area Network(BAN) into the user's phone and then has the phone send an unlock message through BLE. Using a detection threshold of 2 x 10 to the 10th Hz they have the lock opening 100 percent of times it's touched and 0 percent of the time it's not touched. However, because the technology for BAN isn't in modern phones this solution wouldn't be able to be implemented for a while.

3.2.7 Future Directions

How could we more accurately triangulate a person's position to avoid Unwanted Unlocking without having to use BAN? Is it possible to make a smart lock immune to traditional lockpicking?

3.3 Testing Vulnerabilities in Bluetooth Low Energy

3.3.1 Group Member

Joshua Niemann

3.3.2 Citation

Thomas Willingham, Cody Henderson, Blair Kiel, Md Shariful Haque, and Travis Atkison. Testing vulnerabilities in bluetooth low energy. In *Proceedings of the ACMSE 2018 Conference*, ACMSE '18, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450356961. doi: 10.1145/3190645.3190693. URL `https://doi.org/10.1145/3190645.3190693`

3.3.3 Main Idea

The authors analyze common weaknesses in Bluetooth connections, and use open-source tools to attack Bluetooth Low Energy keyboards.

3.3.4 Theory

Game Theory. The authors directly attack the Bluetooth Low Energy protocol to gain the ability to read decrypted bluetooth packets from an attacker's perspective.

3.3.5 Method

The authors utilize a Bluetooth Low Energy keyboard in addition to a Ubertooth One and the CrackLE tool to decrypt packets from the keyboard. The authors captured the pairing sequence between the computer or phone and the keyboard using an ubertooth one.

3.3.6 Findings

The authors found that classical Bluetooth is still more secure for the time being. They also found that Bluetooth Low Energy is very possible to break, albeit very finnicky to get to work at times. Capturing a pairing sequence requires the Ubertooth to be on the right channel at the right time, which can be a challenge given Bluetooth Low Energy has multiple pairing channels, and an Ubertooth can only scan one at a time.

3.3.7 Future Directions

The authors next want to expand their device reach. The keyboard was picked because of it's ease of re-pairing the device. However, this same technique will work for other Bluetooth Low Energy devices, such as a smartwatch. The authors want to try different smartwatches and a few fitness trackers and see if the Ubertooth and Crackle can collectively decrypt the traffic.

3.4 GATTacking Bluetooth Smart Devices

3.4.1 Group Member

Connor Leavesley

3.4.2 Citation

Slawomir Jasek. Gattacking bluetooth smart devices. In *Blackhat 2016*, 2016. URL `https://paper.seebug.org/papers/Security%20Conf/Blackhat/2016/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool-wp.pdf`

3.4.3 Main Idea

The author summarized possible attacks against Bluetooth Low Energy (BLE) using the Generic Attribute Profile (GATT). The security features of BLE are also covered in detail.

3.4.4 Theory

This is Game Theory. The author abused the GATT to intercept, decrypt, and inject commands in BLE communication.

3.4.5 Method

The author started with a high overview of what BLE is, how it advertises and pairs devices, and how attackers use GATT to transfer characteristics data. The specific BLE versions in question are 4.0 and 4.2. Then he went over BLE security features: encryption, MAC randomization, and whitelisting. Then Jasek discussed possible attacks against BLE, how manufacturers have tried to mitigate these attacks, and the risk of such attacks occurring. Finally he covers a tool he developed to assist in assessing BLE devices.

3.4.6 Findings

Many of the in place security features included in BLE are either not used or not implemented correctly. Instead, manufacturers use the GATT to transfer data and start secure sessions, often incorrectly. BLE advertisements are extremely susceptible to DoS and spoofing. Manufacturers use a method called "shuffling", but it is kept secret and likely not implemented correctly. Handshakes using the GATT are often not encrypted and passive interception is very profitable for attackers. Active interception is also useful due to MAC spoofing and GATT cloning.

3.4.7 Future Directions

The author does not give any indication of where he believes future research should go. However, Jasek used BLE 4.0 and BLE 4.2 in this paper. Researchers should look into how security practices have changed with the adoption of BLE 5.

3.5 Bluetooth Low Energy Mesh Networks: A Survey

3.5.1 Group Member

Jacob Ruud

3.5.2 Citation

Mahdi D. Seyed and Carles Gomez. Bluetooth low energy mesh networks: A survey. *Sensors*, 17(7):1467, 2017. URL `https://ezproxy.rit.edu/login?url=https://search-proquest-com.ezproxy.rit.edu/docview/2108690652?accountid=108`.

3.5.3 Main Idea

The authors analyze the composition, architecture, and implementation of Bluetooth Low Energy mesh networks. Their main goal with this paper is to assess the strengths and weaknesses of mesh networks as they compare to star networks that are beginning to phase out as the industry standard.

3.5.4 Theory

In the open issues section of the paper, the authors use game theory to describe different scenarios that an attacker may be able to compromise a BLE mesh network.

3.5.5 Method

The majority of the work done for this paper was survery of proposed technologies, therefore the methods that the authors used for their conclusions involved reading publishings from other academics, corporations, and organizations and analyzing the architecture the each proposed. They used Bluetooth standards 4.0,4.1,4.2, and 5.0 in their comparison.

3.5.6 Findings

The main security takaway from this paper is that bluetooth low enerygy was originally designed for a star topology, and therefore there exist a number of flaws in the implementation of mesh networks that still have yet to be sorted out. For example, currently data channels are protected by per-hop security; therfore, end-to-end encryption and authentication are not currently supported in BLE mesh networks. Also, routing and data packets that are transmitted through advertising channels are not secured unless the application layer provides a security solution.

3.5.7 Future Directions

The authors suggested that future community work should focus on solving problems in security, multicast, and interoperability. They noted that these areas would best help deliver secure and high quality BLE mesh networks.

4 Summary 4

4.1 On Privacy and Security Challenges in Smart Connected Homes

4.1.1 Group Member

Daniel Capps

4.1.2 Citation

Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. On privacy and security challenges in smart connected homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)*, pages 172–175. IEEE, 2016. URL `https://muep.mau.se/bitstream/handle/2043/21507/2857a172.pdf?sequence=4&isAllowed=y`

4.1.3 Main Idea

The authors give an overview of the privacy and security challenges directed towards the smart home domain. The authors discuss different constraints, soulution, challenges, and research issues where further investigation is required.

4.1.4 Theory

Game Theory. The authors identify different attack vectors for smart homes and give some solutions to these attacks.

4.1.5 Method

The authors identified different categories of security risks and then listed what a solution would have to look like in order to mitigate the security risks.

4.1.6 Findings

The authors identified different security risks involved in smart homes. For the devices in smart homes they found problems with resource constraints, lack of user interface, and a need for tamper resistant devices and data. For the communication used in smart homes they found problems with heterogeneous protocols and devices going in and out of the network. The authors also found an issue with devices in smart homes not supporting dynamic patches for various reasons.

4.1.7 Future Directions

The authors offer multiple future research directions. They recommend further investigation into, identity management, risk assessment methods, information flow control, and security management methods relating to smart home environments.

4.2 An Active Man-in-the-Middle Attack on Bluetooth Devices

4.2.1 Group Member

Connor Leavesley

4.2.2 Citation

Tal Melamend. An active man-in-the-middle attack on bluetooth smart devices, 2018

4.2.3 Main Idea

The author looks to outline the main issues with BLE security. He focus on a possible architecture for a man-in-the-middle attack and a case study on a MITM'd device and an associated application.

4.2.4 Theory

The author is utilizing Game Theory. He is attacking a Bluetooth connection via a MITM.

4.2.5 Method

The author uses a Dax-Hub SW-28 Smart Bracelet and its associated app PowerSensor and the subject of the MITM attack. He used Kali Linux as the attacker and installed GATTacker and BtleJuice. He connected a CSR 4.0 dongle to a VM to transmit data between the app, the bracelet, and the middleman. He then uses GATTacker to intercept the BLE advertisements and copy the GATT profile of the bracelet. The author uses the GATT to simulate the device. Tal was then able to send fake to the device.

4.2.6 Findings

The author found that it was far to easy to intercept device communications and take control. Due to the inherent insecurities of the BLE protocol, he was able to change data that the device displayed, as well as take control of mobile camera via the app.

4.2.7 Future Directions

The author does not give any ideas as to future directions. The security issues with BLE are widely know, and Tal hopes to explain the security issues here and how to exploit them in a unique manner.

4.3 Bluetooth: With Low Energy comes Low Security

4.3.1 Group Member

Joshua Niemann

4.3.2 Citation

Mike Ryan. Bluetooth: With low energy comes low security. In *Presented as part of the 7th USENIX Workshop on Offensive Technologies*, Washington, D.C., 2013. USENIX. URL `https://www.usenix.org/conference/woot13/workshop-program/presentation/Ryan`

4.3.3 Main Idea

The author of this paper breaks almost all the security measures relating to Bluetooth Low Energy after key generation, and builds an open-source tool that allows for the exposure of the Long-Term Key from a BLE packet if provided the pairing sequence. The author also breaks the channel hopping algorithm, allowing for passive attackers to follow Bluetooth packets on air.

4.3.4 Theory

The author directly attacks the Bluetooth Low Energy protocol and exposes weaknesses in the key generation algorithm, the channel hopping algorithm, and other flaws in the Bluetooth Low Energy protocol. Directly attacking the protocol allows this article to resemble Game Theory.

4.3.5 Method

The authors work backward from the Bluetooth protocol, breaking the security measures of Low Energy. An Ubertooth One is used as the intercept device. Using this ubertooth, the authors figured out how to calculate the Hop Interval, the Hop Increment, the Access Address, and CRC init. Finally, the author works on breaking the key exchange algorithm.

4.3.6 Findings

The author found that an attacker could both follow a Bluetooth packet through the channel hopping algorithm, which would allow any passive attacker to follow a Bluetooth Stream with readily-available hardware like an Ubertooth. The author also found that the key exchange algorithm is extremely broken and can be reversed in under 1 second on a modern computer.

4.3.7 Future Directions

The author outlined several next steps. The first of which details a hypothetical attack that would allow an attacker to force key negotiation, which would use the Bluetooth Low Energy key exchange protocol, of which was already broken in this paper. From there, an attacker could effectively decode any live Bluetooth Low Energy communication, even if not present during the initial pairing process.

4.4 Analysis of Bluetooth Threats and v4.0 Security Features

4.4.1 Group Member

Jacob Ruud

4.4.2 Citation

S Sandaya and K A Sumithra Devi. Analysis of bluetooth threats and v4.0 security features, Apr 2012. URL `https://ieeexplore-ieee-org.ezproxy.rit.edu/stamp/stamp.jsp?tp=&arnumber=6179149`

4.4.3 Main Idea

The authors aim to assess the security features added to bluetooth in the 4.0 security update. They specifically focus on the addition of new security association models as well as secure simple paring both in normal and low energy mode.

4.4.4 Theory

This paper covers multiple scenarios that can be attributed to the standard alice, bob, and oscar method of describing game theory. In which oscar attemps to steal sensitive information from the communication between alice and bob treating the leak of any such data as a win.

4.4.5 Method

The authors break down the protocol based on a framework called "A Bluetooth Threat Taxonomy" previously developed by a man by the name of John Paul Dunning. They use this framework to provide a comprehensive risk asssessment of the bluetooth 4.0 protocol and determine what likely attack vectors are. The Attack Classifications Include: Surveillance, Range Extension, Obfuscation, Fuzzer, Sniffing, Denial of Service, Malware, Unauthorized Direct Data Access, and Man In the Middle.

Upon furhter reading, the authors dive deeper into the secure simple pairing function to assess its four association models: Numeric Comparison, Just Works, Out of Band, and Passkey Entry. Each one of these models is used independantly of each other depending of the IO capabilities of the two connecting devices.

4.4.6 Findings

The findings of this paper demonstrate the advantages of Bluetooth Low Energy over standard Bluetooth communication. The main reason behind this destinction lies in the fact that BLE does not use DHKE in it's exchange of authentication data. This means that the protocol is less likely to be compromised due to the fact that potential threat actors are able to compute the shared DH Key and therefore have less trouble bypassing the other security mechanisms in place. Therefore, Bluetooth LE is not affected by PFS, KCI, or MitM attacks.

4.4.7 Future Directions

The authors vaugely recommend at the end of their paper that "version 4.0 undergo a continual security analysis process by people involved." They suggest the possibility of integrated security to help "protect data privacy and to prevent misuse of data."

4.5 Review of the Open Supervised Device Protocol (OSDP) for DoD Applicability

4.5.1 Group Member

Quintin Walters

4.5.2 Citation

SEIWG. Review of the open supervised device protocol (osdp) for dod applicability. Report, Security Equipment Integration Working Group, 2015. URL `https://www.acq.osd.mil/ncbdp/nm/pseag/news-references/references/SEIWG_OSDPReview_PublicRelease_20140801_v1.0.pdf`

4.5.3 Main Idea

The authors review the Open Supervised Device Protocol, how it wworks, what it supports, the messages sent, and the legal implications of using the protocol in DoD facilities. They go in depth on the specific functioning of the protocol, the messages it sends, and the wiring necessary for it. The authors also compare it to the Wiegand protocol, covering the differences between them and the possible issues with upgrading from Wiegand to OSDP.

4.5.4 Theory

The authors implement Systems theory in this article. They observe how OSDP interfaces with other systems and how it has been implemented without attempting to attack it in any way.

4.5.5 Method

They authors surveyed multiple suppliers of OSDP compatible devices and they reviewed numerous papers on OSDP. There was no hands on research done.

4.5.6 Findings

They find that OSDP is "not yet widely adopted" and it is not explicitly called for in various legal compliances. They also found that vendors have managed to keep Wiegand relevant but it is not able to support high levels of assurance. The authors claim that vendors use "FICAM as a selling point more than OSDP" but if OSDP is associated with FICAM it will be implemented more often.

4.5.7 Future Directions

The authors indirectly recommend to "more clrealy associate" OSDP with FICAM guidance to increase the usage of it.

5 Summary 5

5.1 Security analysis of Internet-of-Things: A case study of august smart lock

5.1.1 Group Member

Daniel Capps

5.1.2 Citation

Mengmei Ye, Nan Jiang, Hao Yang, and Qiben Yan. Security analysis of internet-of-things: A case study of august smart lock. In *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 499–504. IEEE, 2017. URL `http://cse.unl.edu/~qyan/paper/MobiSec17_AugustLock.pdf`

5.1.3 Main Idea

The authors investigate the security of August smart locks by discussing different threat models for attacking August smart locks. The authors then show different attacks on August smart locks including handshake key leakage, owner account leakage, personal information leakage, and denial of service (DoS) attacks. The authors alongside each attack show a method for dealing with said attacks.

5.1.4 Theory

Game Theory. The authors determine different types of attacks and mitigation techniques for smart locks against different types of attacks.

5.1.5 Method

The authors use different tests for each attack vector using a specific environment. The four attack vectors described by the authors are handshake key leakage, owner account leakage, personal information leakage and DoS attacks. Handshake key leakage is an attack that makes use of the fact that the owner's handshake key is in plain text on their phone. Allowing them to make covert changes to the owner's lock. The owner account attack allows an adversary to mimic the original owner's account and send commands to the lock as if they were them. They simply have to replace their system file from the app with the owners and they're in. Personal information leakage is just the data on the phone in plaintext. DoS attack is when there are multiple users connecting to a single lock, it will suspend the app and no user is able to lock/unlock at the same time.

5.1.6 Findings

The authors proposed mitigation methods for the four different attacks. The first method is requiring authentication with lock controlling requests. Denying the attacker the ability

to even with the owner's handshake key to make covert changes to their lock. The second method is to have an authentication mechanism to protect the system files from improper use. The authors recommend using FlaskDroid which is mandatory access control for Android. The third method is to just encrypt the data on the phone. The fourth method is to have a simple priority-based request control mechanism allowing the most authorized party to gain priority instead of having no one be able to control the lock.

5.1.7 Future Directions

Does FlaskDroid have secure file access control? Are there any authentication mechanisms for smart locks to detect fake apps? How would someone develop a holistic security framework to secure IoT devices?

5.2 BLE Injection-Free Attack: A Novel Attack On Bluetooth Low Energy Devices

5.2.1 Group Member

Connor Leavesley

5.2.2 Citation

Aellison C. T. Santos, Jose L. Soares Filho, Avilla I. S. Silva, Vivek Nigam, and Iguatemi E. Fonseca. Ble injection-free attack: A novel attack on bluetooth low energy devices, 2019. URL `https://nigam.info/docs/jaihc19.pdf`

5.2.3 Main Idea

The authors propose a new method of attacking the cryptography of BLE devices, called an injection-free attack. The authors propose this attack for when forced key renegotiation is not possible.

5.2.4 Theory

The theory being used is Game Theory. The authors are attacking BLE devices in a zero sum game.

5.2.5 Method

The authors use a BLE device with enough interfaces to fill the bonding list of a target device. An attacker will keep pairing new devices to the target until the bonding list fills up. Once this occurs, the next device to join will cause the target device to forget a key and negotiate a new one with the new device. Now the target device will need to renegotiate keys with legitimate devices. The attacker could carry out this attack without the packet injection needed in other attacks.

5.2.6 Findings

The authors found that it is remarkably easy to attack BLE devices even without abuse the weak cryptography due to the limited resources of the devices. This method could be used by attackers to maliciously pair with devices and remove legitimate devices from the bonding list of devices.

5.2.7 Future Directions

The authors believe that future research should go into automating injection free attacks and the development of defenses against such attacks.

5.3 You Can Clone But You Can't Hide: A Survey of Clone Prevention and Detection for RFID

5.3.1 Group Member

Joshua Niemann

5.3.2 Citation

K. Bu, M. Weng, Y. Zheng, B. Xiao, and X. Liu. You can clone but you cannot hide: A survey of clone prevention and detection for rfid. *IEEE Communications Surveys Tutorials*, 19(3):1682–1700, thirdquarter 2017. ISSN 2373-745X. doi: 10.1109/COMST.2017.2688411

5.3.3 Main Idea

The authors evaluate RFID cards and the ease of cloning them using various cloning countermeasures.

5.3.4 Theory

The authors demonstrate Game Theory by directly comparing different card-cloning prevention techniques and their overall effectiveness.

5.3.5 Method

The authors evaluate the practicality of each detection technique or anti-cloning to determine the best option for an organization looking to secure their enviornment.

5.3.6 Findings

The authors found that card cloning is hard to particularly stop. Card cloning prevention requires a secret to be kept, and as long as the secret has to be transmitted to the reader at some point, the secret can be intercepted. Encryption isn't often too much help either, due to the low-powered nature of the RFID cards in question. Detection on the other hand is often a much better option. With detection, you can probalistically determine if a user is

likely a clone using enviornmental attributes as well. This could entail detection based on a location that is improbable for a legitimate tag to be, or subsequent scans that are too far apart from each other.

5.3.7 Future Directions

The authors specify no formal future directions for this research, but do mention that further research on how to detect cloning attacks is not only necesary, but required for the security of every RFID system. The paper also mentions that more can be done on the hardware security front, such as better readers, better hash algorithms to avoid collision, strengthening the reliability of wireless connections, and better encryption techniques.

5.4 Output Characteristics and Circuit Modeling of Wiegand Sensor

5.4.1 Group Member

Jacob Ruud

5.4.2 Citation

Xiaoya Sun, Tsutomu Yamada, and Yasushi Takemura. Output characteristics and circuit modeling of wiegand sensor. *Sensors*, 19(13), 01 2019. URL `https://ezproxy.rit.edu/login?url=https://search-proquest-com.ezproxy.rit.edu/docview/2301762026?accountid=108`. Copyright - © 2019. This work is licensed under https://creativecommons.org/licenses/by/ (the "License"). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License; Last updated - 2019-10-08; SubjectsTermNotLitGenreText - United States–US

5.4.3 Main Idea

In this paper the authors take a deep dive into the circuit design and output characteristics of a sensor using weigand technology as well as propose a new design for the sensor to make it more efficient.

5.4.4 Theory

Game Theory is the underlying theory behind this paper as the authors propose a situation where a wiegand sensor can use its own pulse voltage as a power source as a win

5.4.5 Method

The authors first measured the pulse voltage from a test sensor they had in their lab, they then created an equivalent electrical circuit to generate the same numbers generated from the weigand, they then used this circuit to calculate the amount of voltage needed to run the device consistantly and determine whether or not their idea was sound. They also used matlab/simulink simulation to help with this process.

5.4.6 Findings

The authors found that the pulse voltage created by the internals of the wiegand sensor were uniform enough to be used for energy harvesting, and that the simulation numbers agreed with the real world behavior reflected by the test circuit they created.

5.4.7 Future Directions

The authors propose further testing of their design at abnormal temperatures as they state that the device will behave differently depending on the outside air temperature where the circuit is being operated.

5.5 Security Analysis of Vendor Customized Code in Firmware of Embedded Devices

5.5.1 Group Member

Quintin Walters

5.5.2 Citation

Muqing Liu, Yuanyuan Zhang, Juanru Li, Junliang Shu, and Dawu Gu. Security analysis of vendor customized codein firmware of embedded device, Jun 2017. URL `https://loccs.sjtu.edu.cn/~romangol/publications/securecomm16.pdf`

5.5.3 Main Idea

The authors propose that the vendor customized code within device firmware is the most likely attack vector. They cover the tools to analyze this section, methodology to test it, and then analyze five embedded devices.

5.5.4 Theory

The authors implement Game Theory in this article. They examine multiple devices for security threats and treat it as a zero sum game.

5.5.5 Method

The authors assess five devices: the TP-Link WR740nv5, TOTOLINK A850R, HUAQIN HGU421, Thunder Money Maker, and Yi Smart Webcam. They check hte device's standard functionality and then test the sections for vulnerabilities.

5.5.6 Findings

The authors discover that the TP-Link WR740nv5 and the Thunder Money Maker do not perform code integrity checks. The TOTOLINK A850R has a vulnerability in its authentication method that can cause a web server crash if an attacker sends a carefully crafted

request. Finally, the Yi Smart Webcam is vulnerable to Man-In-The-Middle attacks and the camera will respond to anyone on TCP port 38888 with the session key. These vulnerabilities were all found in the vendor specific code for the devices, proving the author's point about the possible weakness there.

5.5.7 Future Directions

The authors recommend further development in current firmware analysis tools. Further research can be done to better them and the implementation of standards for vendor code segments in embedded devices.

6 Summary 6

6.1 An efficient access control scheme for smart lock based on asynchronous communication

6.1.1 Group Member

Daniel Capps

6.1.2 Citation

6.1.3 Main Idea

The authors propose an asynchronous and consistent lock access management scheme to avoid unauthorized access through the lock. The authors also present a lightweight and efficient tree-based access control solution to such smart lock network's problems, which enable cascading deletion.

6.1.4 Theory

Game Theory. The authors propose mitigation techniques for smart locks to defend against different exploits, primarily evasion attacks.

6.1.5 Method

The authors proposed secure command transmission and a tree based access control system and then evaluated their proposed systems. The secure command transmission system is a device centered system that has two phases, the user-lock phase and the user-cloud phase. In the user-lock phase, users give an unlock request or forward the commands from the cloud to the smart lock. In the user-cloud phase, users are able to send and receive access control commands from the cloud. During this process there is a preprocessor in the smart lock that checks the security of incoming requests and determines how to handle them. The tree based access control system (TACS) is stored directly on the smart lock and every command from the owner is performed on this tree. The smart lock maintains this tree by executing commands sent by the owner. When a user's request comes to TACS, it checks whether the user is authorized to make that request or not.

6.1.6 Findings

The authors found that against evasion attacks their scheme forces each user to connect to the cloud to get a valid period, which only then can the user unlock the door. However adversaries can still unlock the door within the valid period (authors set it to 24 hours) just after being revoked. The authors weren't able to have all information updated immediately after an owner's command is sent due to their asynchronous communication scheme. All operations on the tree took less than 100 milliseconds in the authors experiments and in most cases the tree took up less than 1 MB and could store up to 12 nodes.

6.1.7 Future Directions

Can the scheme used here for smart locks be expanded into other fields? Is there a way to remove the valid window so that adversaries can't use the lock immediately upon being revoked?

6.2 Bluetooth: With Low Energy comes Low Security

6.2.1 Group Member

Connor Leavesley

6.2.2 Citation

6.2.3 Main Idea

The simplification of Bluetooth Low Energy to reduce power use caused a number of security issues. The author gives an overview of Bluetooth Low Energy, BLE packet injection, and encryption weaknesses.

6.2.4 Theory

This paper is utilizing Game Theory. The author attacks the BLE protocol in a zero sum game.

6.2.5 Method

The author implements several types of Bluetooth attacks utilizing an Ubertooth: eavesdropping, packet injection, and bypassing encryption. He then explores the flaws and devises a number of mitigations to fix the issues present.

6.2.6 Findings

The author found that attacking BLE is trivial after a few, small technical hurdles. To eavesdrop on a BLE device, an attacker needs to know the hop interval, hop increment, access address, and CRC init. Ryan used this information to calculate which of the 37 channels the connection would switch to next. There are three types of methods to set up a Temporary Key (TK) for BLE, Just Works, with a key of all zeros, a six digit pin, or OOB, which is an agreed out-of-band 128 bit key. The author found that this key could be brute forced in less than a second if the device used a six digit pin. He can use the TK to derive the Short Term Key, and that to derive the Long Term Key. OOB is far harder for an attacker to crack, but exchanging a key out-of-band is difficult and not practical in practice.

6.2.7 Future Directions

The author believes that future researchers should investigate main-in-the-middle attacks against Bluetooth devices to increase the effectiveness of the proposed attacks.

6.3 Lock Picking in the Era of Internet of Things

6.3.1 Group Member

Joshua Niemann

6.3.2 Citation

E. Knight, S. Lord, and B. Arief. Lock picking in the era of internet of things. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 835–842, 2019

6.3.3 Main Idea

The authors perform a security analysis of a common Bluetooth Smart Lock created by a major brand. A MasterLock was chosen because of the strong brand recognition in the lock segment, with a smaller emphasis on IOT devices.

6.3.4 Theory

Game Theory. The authors perform an attack on a common lock in order to determine inherent weaknesses in the product.

6.3.5 Method

The authors conducted an analysis on the backend server API calls. They do this by reverse engineering the mobile application for the product. From there, valid requests were sent to determine how the API server would handle various different scenarios.

6.3.6 Findings

The authors found that guest and master codes are statically generated, meaning that they could not be revoked. The authors also found that many APIs could be misused to generate unliimited future access codes from the perspectie of a limited guest account.

6.3.7 Future Directions

The authors discuss the possibility of investigating the bluetooth connection between the lock and the phone. Although a limited amount of bluetooth research was done in the authors' testing, a lot more work can be done in investigating the bluetooth link, particularly on guest accounts.

6.4 Investigations of Power Analysis Attacks on Smartcards

6.4.1 Group Member

Jacob Ruud

6.4.2 Citation

Thomas S. Messerges, Ezzy A Dabbish, and Robert H Sloan. pdf, May 1999

6.4.3 Main Idea

The main idea of this paper is to analyze power anylysis techniques that had been used in the past to attack the DES encryption protocol. The authors then propose a method to model the signal vs noise ratio.

6.4.4 Theory

The main theory on display during this analysis is game theory, the authors treat the ability to measue power levels from the reader as a win in this scenario.

6.4.5 Method

The authors were able to measure the power dissipation of the smartcard by reading from the ground pin with the assisstance of a small resistor in series between the VSS pin on the card and the true ground.

6.4.6 Findings

The authors confimed "that power analysis attacks can be quite powerful and need to be addressed." They also were able to successfully propose a way to model the noise characteristics of the power signal coming from the smartcard in hopes of inspiring future work to secure smartcard software against power analysis attacks.

6.4.7 Future Directions

The authors suggest that "Future research in this area will investigate power analysis attacks on hardware encryption devices and publickey cryptosystems." At the time this paper was written, AES had not yet been published so there definately room for more work on this topic.

6.5 Poster: Power Replay Attack in Electronic Door Locks

6.5.1 Group Member

Quintin Walters

6.5.2 Citation

Seongyeol Oh, Joon-sung Yang, , Andrea Bianchi, and Hyoungschick Kim. Poster: Power replay attack in electronic door locks, 2014. URL `https://www.ieee-security.org/TC/SP2014/posters/OHSEO.pdf`

6.5.3 Main Idea

The authors theorize that electronic door locks are susceptible to a power replay attack in which an insider modifies the lock with a bypass circuit. This circuit can be triggered to provide power to the locking mechanism and unlock the door remotely.

6.5.4 Theory

The theory shown is game theory, if the lock is susceptible to this attack then it is bypassable and considered insecure.

6.5.5 Method

The authors attached a Bluetooth capable circuit and LiPo battery to the internal circuitry of the lock. This is wired in parallel with the original locking circuit so that the lock will still perform normally while the implant is in place.

6.5.6 Findings

The authors found that locks from the manufacturers Gateman, Samsung, Mille, and Hyegang are susceptible to this attack. A malicious insider could place these implants without being detected and use it to gain access at a later date.

6.5.7 Future Directions

The authors recommend adding tamper detection circuitry to the locks in order to detect if they have been opened along with additional hardware to detect changes in the internal capacitance. These modifications would make it harder to place an implant like this and allow for an easier detection of an existing implant.

7 Summary 7

7.1 Title

7.1.1 Group Member

Daniel Capps

7.1.2 Citation

7.1.3 Main Idea

Main Idea

7.1.4 Theory

Theory

7.1.5 Method

Method

7.1.6 Findings

Findings

7.1.7 Future Directions

Future Directions

7.2 Extracting the Security Features Implemented in a Bluetooth LE Connection

7.2.1 Group Member

Connor Leavesley

7.2.2 Citation

Angel Robles-Cordero, William Zayas, and Yesem Peker. Extracting the security features implemented in a bluetooth le connection, 2018. URL `https://ieeexplore-ieee-org.ezproxy.rit.edu/document/8622000`

7.2.3 Main Idea

Many of the IoT devices adopting Bluetooth do not impliment the security features that Bluetooth Special Interest Group developed. To promote visability of this issue, the authors have developed an application to extract the security features of a Bluetooth device to test the security of devices.

7.2.4 Theory

The authors are utilizing Systems Theory. They are observing how a device interacts with other Bluetooth devices trying to connect to it.

7.2.5 Method

The authors developed an Android application for two smartphones, the Zenfone Max 3 and the OnePlus 6. They are using Lenovo HW02 fitness tracker as the second bluetooth device. The app extracts logs from the btsnoop log created by Android devices. The app can discover security information about the connection from the logs.

7.2.6 Findings

When pairing the tracker to the phones the fitness tracker sent the Long Term Key (LTK) to the tracker with no encryption, even though both are using Bluetooth 4.2. When using the app, this was not the case. Unfortunately the authors did not go into greater detail about what security features were found, only focusing on the inital transfer of the LTK.

7.2.7 Future Directions

The authors believe that future research should be done in further improving the security of BLE, as it is here to stay.

7.3 Title

7.3.1 Group Member

Joshua Niemann

7.3.2 Citation

7.3.3 Main Idea

Main Idea

7.3.4 Theory

Theory

7.3.5 Method

Method

7.3.6 Findings

Findings

7.3.7 Future Directions

Future Directions

7.4 C

onfidence in Smart Token Proximity: Relay Attacks Revisited

7.4.1 Group Member

Jacob Ruud

7.4.2 Citation

Gerhard P Hancke, KE Mayes, and Konstantinos Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, 28(7):615–627, 2009

7.4.3 Main Idea

The authors revisit the fesibility of implementing both passive and active relay attacks against smart tokens. They also discuss the security implications should the attackers succeed. Finally, the authors discuss possible actions that device owners could take to mitigate the risk of these attacks.

7.4.4 Theory

The authors use game theory to explain the red vs blue scenario, treating a win for red as a breach of information and a win for blue as witholding access control.

7.4.5 Method

The authors utilize a proxy-token and proxy-reader to create a virtual clone of the authenticated users access card and relay it to the reader. This can be done by creating your own hardware or using existing tools. The authors chose to implement their own proxy reader and proxy token for this experiment.

7.4.6 Findings

the authors were able to successfully perfom a relay attack against an ISO 14443A contactless system using guidelines in public literature and easily obtainable hardware. They also found that timing constraints have little to no effect against relay attacks, and although 2FA is effective if nullifies some of the advantages of smart token systems. The authors suggest using distance bounding or monitoring using a trusted interface as more effective methods against this attack, although they warn that these methods are generally more expensive or complex.

7.4.7 Future Directions

The authors leave open the option for further research on methods against relay attacks since they believe that the methods they proposed could be improved upon.

7.5 Portable RFID Bumping Device

7.5.1 Group Member

Quintin Walters

7.5.2 Citation

Romke van Dijk, Loek Sangers, and Ari Davis. Portable rfid bumping device, Feb 2016. URL `https://delaat.net/rp/2015-2016/p04/report.pdf`

7.5.3 Main Idea

The authors proposed that RFID cards may be vulnerable to a high speed cloning attack performed by bumping into the target. They posit that this attach can be used to gain clones of security cards without the target's knowledge or raising suspicion.

7.5.4 Theory

Game Theory. By showing the ease of cloning the cards the authors show that they are broken and need increased security in order to stay useful.

7.5.5 Method

The authors used a Proxmark 3, a LG Nexus 5 with Nethunter, a Hirose usb cable, MIFARE Classic 1K, and MIFARE Classic EV1 1K. The authors wrote a default key to the cards and then a large number of random keys. They then generated a large number of random keys to try and gathered a large number of nonces to perform their attack.

7.5.6 Findings

The authors found that the HF Hirose Antenna increased the range to 6-8cm. They also successfully implemented BTWA to read multiple cards. The attacks against the cards were successefully performed against both the Classic and the Classic EV1.

7.5.7 Future Directions

The authors posit that more research can be done into the maximum number of cards that can be read at one time. They also believes that the attack framework can be extended to support more attacks, optimization can be performed on the keyspace calculation software, attempts can be made to try the attack in an unstable environment, and finally optimazation of the Proxmark firmware.

8 Bibliography

Tim Andersson. Bluetooth low energy and smartphones for proximity-based automatic door locks, 2014. URL http://www.diva-portal.org/smash/get/diva2:723899/FULLTEXT01.pdf.

Mark Baseggio and Eric Evenchick. Breaking Access Controls with BLEKey, 2015. URL https://www.blackhat.com/docs/us-15/materials/us-15-Evenchick-Breaking-Access-Controls-With-BLEKey-wp.pdf.

K. Bu, M. Weng, Y. Zheng, B. Xiao, and X. Liu. You can clone but you cannot hide: A survey of clone prevention and detection for rfid. *IEEE Communications Surveys Tutorials*, 19 (3):1682–1700, thirdquarter 2017. ISSN 2373-745X. doi: 10.1109/COMST.2017.2688411.

Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. On privacy and security challenges in smart connected homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)*, pages 172–175. IEEE, 2016. URL https://muep.mau.se/bitstream/handle/2043/21507/2857a172.pdf?sequence=4&isAllowed=y.

Brandon Chung. Wiegand Protocol Access: A Decade of Decryption, 2017. URL http://www.cs.tufts.edu/comp/116/archive/fall2017/bchung.pdf.

R. S. Divya and M. Mathew. Survey on various door lock access control mechanisms. In *2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT)*, pages 1–3, April 2017. doi: 10.1109/ICCPCT.2017.8074187.

Daniel Filizzola, Sean Fraser, and Nikita Samsonau. Security Analysis of Bluetooth Technology, 2018. URL https://courses.csail.mit.edu/6.857/2018/project/Filizzola-Fraser-Samsonau-Bluetooth.pdf.

Zhaoyang Han, Liang Liu, and Zhe Liu. An efficient access control scheme for smart lock based on asynchronous communication. In *Proceedings of the ACM Turing Celebration Conference-China*, pages 1–5, 2019. URL https://dl.acm.org/doi/pdf/10.1145/3321408.3321567?casa_token=XLwSkaZuu3oAAAAA%3AOYckBvFs3ZoQa0y3SfxB1HF3ooW0GrGILpeUBDc8N1CKRui-bRr8X0gyaUMuvHHMWiPedvi4I5w.

Gerhard P Hancke, KE Mayes, and Konstantinos Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, 28(7):615–627, 2009.

Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security*, pages 461–472, 2016. URL https://people.csail.mit.edu/dtl/pdf/ho-smartlocks.pdf.

Slawomir Jasek. Gattacking bluetooth smart devices. In *Blackhat 2016*, 2016. URL https://paper.seebug.org/papers/Security%20Conf/Blackhat/2016/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool-wp.pdf.

E. Knight, S. Lord, and B. Arief. Lock picking in the era of internet of things. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 835–842, 2019.

Muqing Liu, Yuanyuan Zhang, Juanru Li, Junliang Shu, and Dawu Gu. Security analysis of vendor customized codein firmware of embedded device, Jun 2017. URL https://loccs.sjtu.edu.cn/~romangol/publications/securecomm16.pdf.

Angela M Lonzetta, Peter Cope, Joseph Campbell, Bassam J Mohd, and Thaier Hayajneh. Security vulnerabilities in bluetooth technology as used in iot. *Journal of Sensor and Actuator Networks*, 7(3):28, 2018. URL https://www.mdpi.com/2224-2708/7/3/28.

Tal Melamend. An active man-in-the-middle attack on bluetooth smart devices, 2018.

Thomas S. Messerges, Ezzy A Dabbish, and Robert H Sloan. pdf, May 1999.

Seongyeol Oh, Joon-sung Yang, , Andrea Bianchi, and Hyoungschick Kim. Poster: Power replay attack in electronic door locks, 2014. URL https://www.ieee-security.org/TC/SP2014/posters/OHSEO.pdf.

Harry O'sullivan. Security vulnerabilities of bluetooth low energy technology (ble). URL http://www.cs.tufts.edu/comp/116/archive/fall2015/hosullivan.pdf.

Christopher Robberts and Joachim Toft. Finding Vulnerabilities in IoT Devices: Ethical Hacking of Electronic Locks, 2019. URL https://pdfs.semanticscholar.org/3eb1/c453464f50c30b2dfb2aff705d45bfe7a6d1.pdf.

A. M. Robles-Cordero, W. J. Zayas, and Y. K. Peker. Extracting the Security Features Implemented in a Bluetooth LE Connection. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 2559–2563, 2018. doi: 10.1109/BigData.2018.8622000.

Angel Robles-Cordero, William Zayas, and Yesem Peker. Extracting the security features implemented in a bluetooth le connection, 2018. URL https://ieeexplore-ieee-org.ezproxy.rit.edu/document/8622000.

Anthony J Rose. *SECURITY EVALUATION AND EXPLOITATION OF BLUETOOTH LOW ENERGY DEVICES*. PhD thesis, 2017. URL https://apps.dtic.mil/dtic/tr/fulltext/u2/1054747.pdf.

Mike Ryan. Bluetooth: With low energy comes low security. In *Presented as part of the 7th USENIX Workshop on Offensive Technologies*, Washington, D.C., 2013. USENIX. URL https://www.usenix.org/conference/woot13/workshop-program/presentation/Ryan.

S Sandaya and K A Sumithra Devi. Analysis of bluetooth threats and v4.0 security features, Apr 2012. URL https://ieeexplore-ieee-org.ezproxy.rit.edu/stamp/stamp.jsp?tp=&arnumber=6179149.

Aellison C. T. Santos, Jose L. Soares Filho, Avilla I. S. Silva, Vivek Nigam, and Iguatemi E. Fonseca. Ble injection-free attack: A novel attack on bluetooth low energy devices, 2019. URL https://nigam.info/docs/jaihc19.pdf.

SEIWG. Review of the open supervised device protocol (osdp) for dod applicability. Report, Security Equipment Integration Working Group, 2015. URL https://www.acq.osd.mil/ncbdp/nm/pseag/news-references/references/SEIWG_OSDPReview_PublicRelease_20140801_v1.0.pdf.

Seth Sevier and Ali Tekeoglu. Analyzing the Security of Bluetooth Low Energy, 2019. URL https://www.researchgate.net/profile/Ali_Tekeoglu2/publication/333228988_Analyzing_the_Security_of_Bluetooth_Low_Energy/links/5de01b6a4585159aa4518887/Analyzing-the-Security-of-Bluetooth-Low-Energy.pdf.

Mahdi D. Seyed and Carles Gomez. Bluetooth low energy mesh networks: A survey. *Sensors*, 17(7):1467, 2017. URL https://ezproxy.rit.edu/login?url=https://search-proquest-com.ezproxy.rit.edu/docview/2108690652?accountid=108. Copyright - © 2017. This work is licensed under https://creativecommons.org/licenses/by/4.0/ (the "License"). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License; Last updated - 2018-10-09.

Xiaoya Sun, Tsutomu Yamada, and Yasushi Takemura. Output characteristics and circuit modeling of wiegand sensor. *Sensors*, 19(13), 01 2019. URL https://ezproxy.rit.edu/login?url=https://search-proquest-com.ezproxy.rit.edu/docview/2301762026?accountid=108. Copyright - © 2019. This work is licensed under https://creativecommons.org/licenses/by/4.0/ (the "License"). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License; Last updated - 2019-10-08; SubjectsTermNotLitGenreText - United States–US.

Romke van Dijk, Loek Sangers, and Ari Davis. Portable rfid bumping device, Feb 2016. URL https://delaat.net/rp/2015-2016/p04/report.pdf.

Thomas Willingham, Cody Henderson, Blair Kiel, Md Shariful Haque, and Travis Atkison. Testing vulnerabilities in bluetooth low energy. In *Proceedings of the ACMSE 2018 Conference*, ACMSE '18, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450356961. doi: 10.1145/3190645.3190693. URL https://doi.org/10.1145/3190645.3190693.

Mengmei Ye, Nan Jiang, Hao Yang, and Qiben Yan. Security analysis of internet-of-things: A case study of august smart lock. In *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 499–504. IEEE, 2017. URL http://cse.unl.edu/~qyan/paper/MobiSec17_AugustLock.pdf.