Devil in a Box: Installing Backdoors in Electronic Door Locks

Seongyeol Oh, Joon-Sung Yang, Andrea Bianchi and Hyoungshick Kim
College of Information and Communication Engineering
Sungkyunkwan University, Republic of Korea

Email: {seongyeol, js.yang, abianchi, hyoung}@skku.edu

***Abstract*—Electronic door locks must be carefully designed to allow valid users to open (or close) a door and prevent unauthorized people from opening (or closing) the door. However, lock manufacturers have often ignored the fact that door locks can be modified by attackers in the *real world*. In this paper, we demonstrate that the most popular electronic door locks can easily be compromised by inserting a malicious hardware backdoor to perform unauthorized operations on the door locks. Attackers can replay a valid DC voltage pulse to open (or close) the door in an unauthorized manner or capture the user's personal identification number (PIN) used for the door lock.**

I. Introduction

Electronic door locks have recently become popular since they have various benefits compared with traditional mechanical locks. For example, in the case of keyless locks which are the most popular types of electronic door locks, a physical key is not needed anymore. Furthermore, state-of-the-art electronic door locks are also invulnerable to the existing physical attacks based on mechanical techniques (see Section VII).

However, despite such benefits, we question whether electronic door locks are really considered secure. Although manufacturers have claimed that their electronic door locks are securely designed against a wide range of attacks, several security flaws have been recently discovered (*e.g.*, [1] and [2]). To make matters worse, the current focus was only directed to one particular type of adversary attacks by a stranger who tries to open a door from outside. However, in many real life scenarios, another type of attackers can also be found. For example, a thief could sojourn in accommodations such as hotels, resorts, hostels and inns protected by an electronic door lock, and therefore obtain physical access for a (limited) period of time to the electronic door lock. While accessing the inside of the door lock may not be possible from *outside* the door, it is a trivial task from *inside* the room. The thief could therefore plan to modify some parts of the lock during his staying in the hotel, and use such modifications to access the room after his staying, perhaps to steal the belongings of future guests who will sojourn later in the same room. We found that the most popular and commercially endorsed electronic door locks cannot cope with this type of threat. Currently an *insider attacker* – an attacker who has access to the back side of an electronic door lock, which is usually located inside of the room – can covertly insert a malicious hardware component into the electronic door lock to control the lock itself or monitor the transferred informations, without user's possible notice that the device was tampered. Among the possible types of *inside attacks*, in this paper, we introduce two critical attacks: (1) `power replay attack` and (2) `keypad logging attack`.

The most trivial one is what we name as `power replay attack`, for which a malicious attacker can simply apply an externally controlled voltage to activate the relays that mechanically unlock (or lock) the door. We argue that this type of attack is a real threat since it does not require complex reverse-engineering to bypass the central processing unit responsible of holding and decoding a legitimate user's personal identification number (PIN) which is a secret knowledge required to control the door lock. The `power replay attack` only requires a simple hardware modification such that from outside the door the attacker can activate a low-voltage DC signal that can trigger the lock to be opened (or closed).

The `keypad logging attack` requires slightly more electronic sophistication, but is still very simple, and replies on sensing directly from the back of the keypad when a user tries to enter his PIN information. Probably, this attack tend to be much more serious because the victim's PIN information is permanently stolen.

To reduce the potential risks of those attacks, we discuss and recommend several countermeasures at board level, such as an alarm for detecting power line removal, cryptographic protocols and anomaly detection.

The following section explains a common architecture of electronic door locks and communication channels that attackers might be interested in. Section III shows how an attacker makes a power replay attack possible. Section IV presents another possible attack by which an attacker can acquire the user's PIN information, and the implementation details of these attacks are shown in Section V. Section VI suggests several countermeasures to mitigate such attacks. Related work is discussed in Section VII. Our conclusions are in Section VIII.

II. Electronic Door Lock Architecture

We experimentally investigated the feasibility of attacks with the four most popular electronic door locks made by `Gateman`, `Samsung`, `Mille`, and `Hyegang`, which account for over 65% of the total Korea market share in 2013[1]. These electronic door locks follow a common architecture.

[1] http://www.dvnnews.com/news/articleView.html?idxno=10140 (in Korean)

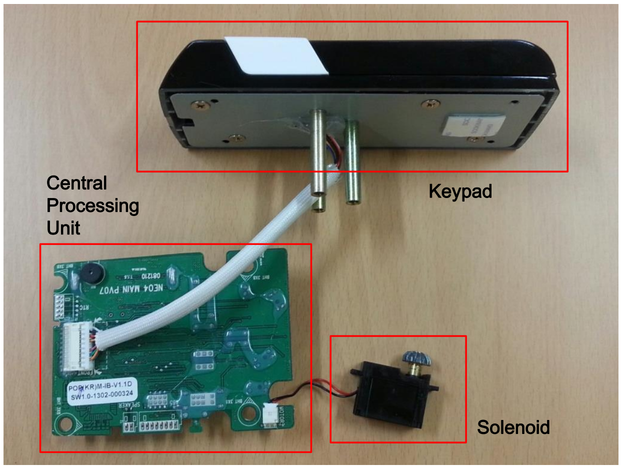


Fig. 1. An example of electronic door locks (made by `Gateman`)

An electronic door lock consists of the three hardware components: *a keypad* for the user input (external side), *a central processing unit* which detects the input and denies or grants authentication, and *an actuator (a solenoid)* which is used to open or close the lock. Figure 1 shows an example of such door locks. In general, the keypad part is located on the outer side of the door while the remaining parts are located on the interior side of the door.

All electronic door locks (`Gateman`, `Samsung`, `Mille`, and `Hyegang`) that we observed use the same mechanism to open the lock. When a user provides a valid credential such as a physical/tangible object or secret knowledge (e.g., PIN), the credential information is transformed to a coded signal at the keypad part and then the coded signal is delivered to a central processing unit that controls a solenoid to actuate the lock by supplying a positive (or negative) DC voltage. There are two communication channels that attackers might be interested in: (1) the **power line** between the central processing unit and solenoid for the delivery of DC voltages and (2) the **data channel** between the keypad and central processing unit for coded signal transfers.

Although these communication channels are not physically exposed to the outside of an electronic door lock device, we found that the communication channels do not remain protected in the inside of the lock device. In practice, the back cover of all electronic door locks that we tested can easily be removed in a few minutes – anyone with a standard Phillips screwdriver can open the back of a lock. Thus an insider attacker with access to the inside of a lock can intercept, manipulate, fabricate, or interrupt the transmitted data and/or power over these channels.

III. Power Replay Attack

First, we have focused on replay attacks for the power line, a simple but powerful attack to which most electronic door locks are susceptible. In practice, an attacker can provide the necessary voltage to the actuating solenoid contained in the back of the device to mechanically detract the lock with a small extra power source. This is very important since an empty space in the door locks is not enough to insert a high-capacity battery as the power supply for replay attacks.

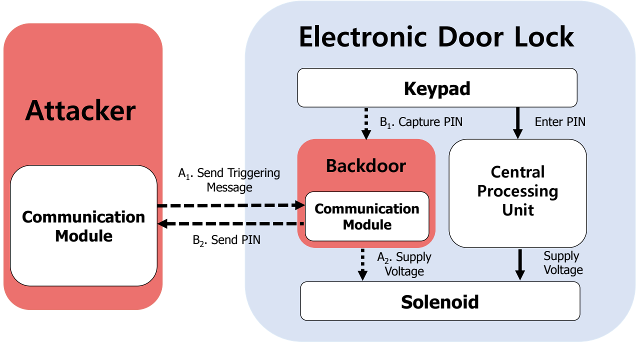


Fig. 2. The overview of attacks on electronic door locks: Dotted lines represent a malicious operation by attacker while solid lines represent a normal operation of door lock. "A_1 and A_2" and "B_1 and B_2" represent the steps for *power replay attack* and *PIN logging attack*, respectively.

A. Attack Scenario

In Figure 2, A_1 and A_2 represent the sequential steps for `power replay attack`. The core idea is to insert a malicious hardware component into the door lock (*a backdoor*) which can remotely supply a voltage to the lock actuator and therefore control the lock itself. There are potentially many different ways to implement power replay attacks. For example, we can use a communication protocol such as Bluetooth or WiFi for the interaction between the *controller* and the *backdoor*. The backdoor circuit is installed as a spurious circuit connected in parallel to the original circuit, hence not replacing, but coexisting with the original. For such reason, from the user perspective, no hardware changes can be noticed during the regular usage of the device. However, if an attacker sends a triggering message through a communication module, then the backdoor supplies an adequate voltage to the solenoid resulting in a door open or close from the outside.

B. Electric Power Measurement

To analyze the electric power needed for the `power replay attack`, we measured the output voltage and current levels at the solenoid in each door lock with an oscilloscope when the door lock is actuated.

According to the user manuals for all door locks tested (`Gateman`, `Samsung`, `Mille`, and `Hyegang`), the voltage level is at least 6.5V to control their solenoids (+6.5V is supplied to open the lock, -6.5V to close it). However, we found that a much smaller voltage level is enough to actuate the door locks. we empirically tested different input voltage configurations ranging from 0 to 6.5V in 0.1V steps as shown in Figure 3. The experimental results show that at the worst case, 0.4W ($1.6V \times 0.25A$) is required to effectively operate the lock. This implies that an attacker can implement the `power replay attack` with using a small external power source (e.g., button cell, as those found in watches) that can easily fit inside the door lock shell.

IV. Keypad Logging Attack

Tampering the back of the keypad and decoding the user PIN – a technique commonly known as the key logging attack – is an equally simple task. We found that coded

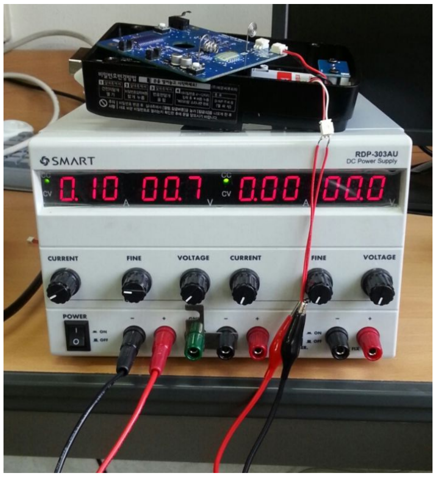


Fig. 3. The minimum voltage needed for a power replay attack (on `Hyegang`)

signal transferred through the data channel between the keypad and the central processing unit can be easily captured and transferred to the attacker. In Figure 2, B_1 and B_2 represent the sequential steps for `keypad logging attack`. When a button is pressed on the keypad, the button information is delivered as an electrical signal from the keypad to the central processing unit, but this information can be easily captured and interpreted by the backdoor, without relying on sophisticated signal processing techniques.

All electronic door locks that we observed use a grid-type structure to implement the keypad. An example is shown in Figure 4. This type of keypad is widely deployed since it can be implemented economically with only $m + n$ electric wires in order to represent $m \times n$ buttons. In such a $(m \times n)$ grid structure, each row or column is independently associated with a unique wire and a pull-up register. Therefore, when a button is pressed, a micro controller can measure each wire's voltage level to identify the pressed button information – if a button is pressed, the voltage level of the associated wire indicates `HIGH`; and `LOW` otherwise.

In summary, an attacker can implement a backdoor which identifies which wires are in the `LOW` state and delivers the information about the pressed buttons to the attacker.

V. Implementation

To show the feasibility of the `power replay attack` described in Section III and IV, we implemented several prototypes. In this section, we describe the details of our implementations.

A. Implementation of Power Replay Attack

For `power replay attack`, we implemented two prototypes: one based on magnet and the other based on the Bluetooth communication. The most difficult challenge in the design of the attack components is how to remotely trigger the installed backdoor from outside of the door lock.

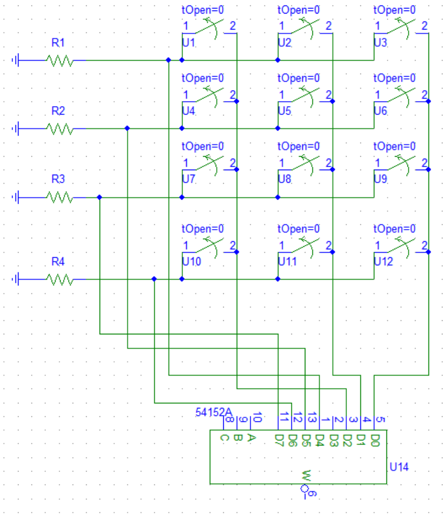


Fig. 4. An example of matrix keypad structure

The first prototype is to use a custom magnetic reed switch that turns on or off when a magnet is nearby. The reed switch is initially opened and is then closed when the switch is exposed to a magnetic field by an attacker with a strong magnet. When the switch is closed, current is drained from a power source to activate the solenoid that locks or unlocks the door. We note that this prototype has some advantages: (1) a reed switch can simply be implemented with a small magnet and stripped wires and (2) it requires a small space only. However, this approach has critical limitations in some attack environments. Inherently, a very strong magnet is required if the target door lock is located on a particularly thick door. To make matters worse, this approach is not reliable depending on the material of a door. For example, if the door is made of metal, the reed switch is not available anymore for backdoor implementation.

In the second prototype[2], we decided to use Bluetooth for the communication between the attacker and the backdoor since Bluetooth is a stable, low power and well-defined wireless technology. The backdoor (see Figure 5) consists of `Nulsomino-HANA`, the tiny micro controller which is compatible with `Arduino Leonardo`, a Bluetooth-embedded module and two lithium-ion polymer batteries and is then inserted to make a circuit connected in parallel to the solenoid. During normal operation, the installed backdoor does not affect the original circuit in the door lock. Only when an attacker sends a trigger message through a Bluetooth channel, the backdoor part is operated to make the door open or close. As the attacker's remote controller for the backdoor, we used an application named '`BTInterface Free Trial BETA`' on the Android platform.

The Bluetooth module is connected to the micro controller with a serial port, so we can transmit a signal from the Android phone to the micro controller via serial communication. The micro controller runs a simple program to receive the data from the Bluetooth module. When receiving a control message (we here set '`o`' and '`c`' for opening and closing, respectively, the door) from the attacker's application, the micro controller

[2] Our demonstration is available in YouTube (http://www.youtube.com/watch?v=Id7HclNYc0s).

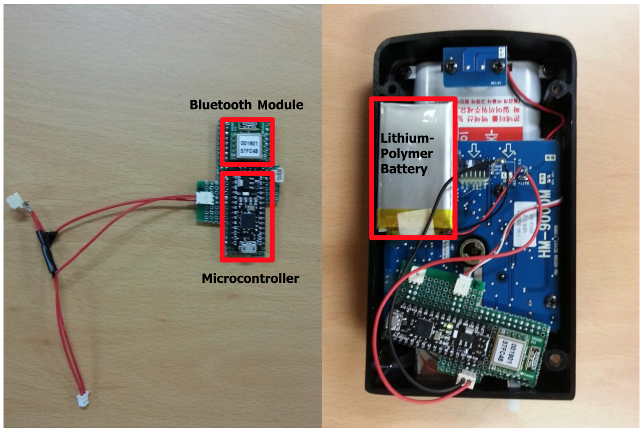


Fig. 5. The prototype implementation for the `power replay attack` based on Bluetooth (on `Hyegang`)

provides a proper voltage to the solenoid.

That is, the micro controller sets `HIGH` (≈ 5V) on a digital port connected to the solenoid when '`o`' is received while it sets `LOW` (≈ 0V) on the same port when '`c`' is received. In addition, we used a Y-shaped cable so that the solenoid and the backdoor are connected to the main board in parallel. This is because the main board rings alarm when the solenoid and the main board are disconnected. Another important consideration, in practice, is that which battery type should be used for running the backdoor because of the limited space within the door lock box. A thin lithium polymer battery that supports 3.7V, 1000mA is suitable for opening and closing a door lock. `Nulsomino-HANA` requires 7∼12V power source, so we connected two batteries in series.

B. Implementation of Keypad Logging Attack

For `keypad logging attack`, we also implemented a prototype. We used an Arduino and a Bluetooth module for this prototype. We connected the keypad part to the Arduino, and ran a program to read the signals generated by the keypad.

If a keypad with 4×3 buttons is used, 7 wires are enough to process the keypad buttons in theory. However, we found that there are some extra wires which have no relation to actual keypad buttons (e.g., power source for the backlight of the keypad). In this paper, we call them "dummy wires". At first glance, it seems a challenging task to distinguish the valid wires related to the keypad buttons from these dummy wires since the specification for the keypad is not available in public. However, we claimed that this is not a challenging task – an attacker can promptly analyze the electrical signals to identify which wires are associated with each button on the keypad. This can be achieved in a brute force manner.

We can use an ohm meter to check whether each wire is associated with either a row or column of the keypad. While the $(i,\ j)$ button of the keypad is pressed, the ohm meter indicates *a closed circuit* only if the inspected wires physically connected with i^{th} row and j^{th} column, respectively. With this test procedure, we constructed a simple algorithm for identifying all valid and dummy wires, which has $\mathrm{O}(d^2)$ operations in the worst case where d is the number of dummy wires.

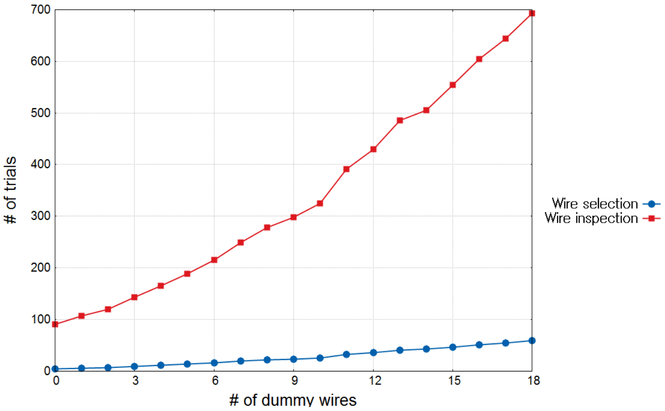


Fig. 6. The average numbers of *wire selection* and *wire inspection* operations

However, in practice, we can achieve better performance. We used simulations to measure how many trials are needed to identify all valid wires when valid and dummy wires are randomly shuffled. The results are shown in Figure 6. Here, the number of *wire selection* represents the number of trials to select a new candidate pair of wires for the test; the number of *wire inspection* represents the number of trials to press a keypad button for each pair of wires. This figure shows how these numbers are changed with the number of dummy wires.

From this figure, we can see that the number of *wire selection* is scalable with respect to the number of dummy wires although the number of *wire inspection* is greatly increased. Hopefully, these results seem promising since the time for a *wire inspection* operation might be much shorter than the time needed for a *wire selection* operation according to our observations from the prototype implementations.

For example, even when 13 dummy wires are used (e.g., for the `Samsung` electronic door lock), if an attacker takes 2 seconds for a *wire selection* operation and 0.5 seconds for a *wire inspection* operation, respectively, the attacker can identify all valid wires within 5 minutes on average.

VI. COUNTERMEASURES

As shown in Section V, the communication channels inside an electronic door lock are not protected well against *inside* attackers. In this section, we suggest two countermeasures to effectively mitigate such attacks for future electronic door lock designs.

A. Detecting Power Line Removal

To insert a backdoor into an electronic door lock, it is required to detach the power line connection from the main board to the solenoid. Unfortunately, in the current design, there is no effective mechanism to detect such removal of the power line. Some electronic door locks have an audible alarm when all components in the electronic door lock are not properly connected to each other. However, the current alarms might remain ineffective since an attacker can easily bypass this warning system by removing the battery from the circuit. To make matters worse, the alarm can be silenced when the power line is promptly recovered again. Therefore, we need to deploy a new circuit design to effectively detect the power line

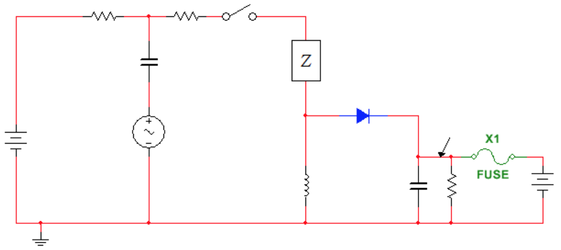
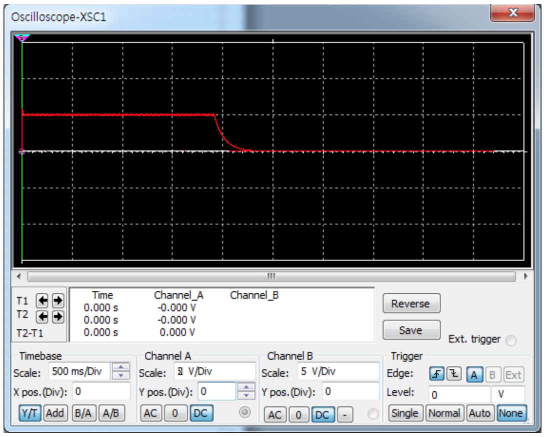


Fig. 7. Open circuit detector to detect power line removal



Time	Channel_A	Channel_B
0.000 s	-0.000 V	
0.000 s	-0.000 V	
0.000 s	0.000 V	

Timebase
Scale: 500 ms/Div
X pos.(Div): 0

Channel A
Scale: 2 V/Div
Y pos.(Div): 0

Channel B
Scale: 5 V/Div
Y pos.(Div): 0

Trigger
Edge: A
Level: 0 V

Fig. 8. Lowering voltage level simulation measurement by capacitor discharging

disconnection which is typically required prior to the insertion of a backdoor component.

An open circuit detector might be one of the most promising solutions since an electronic door lock device forms a closed circuit when all components including its battery are properly connected. The proposed open circuit detector is shown in Figure 7.

Unlike conventional electronic door locks, we use an AC voltage source (e.g., a crystal oscillator) in addition to the main DC source. While the DC voltage is still consumed at the impedance (i.e., a solenoid), the newly added AC voltage provides energy to the inductor and the diode rectifier which is used to transform AC supply to DC supply. Therefore, the capacitor connected to the rectifier stores the energy.

When the power line is properly connected, there is no potential difference between the capacitor and the voltage. Therefore, there is no current flowing through the fuse. However, if an attacker disconnects the power line, no AC voltage is supplied and the capacitor discharges the energy as shown in Figure 8. This figure shows a voltage level on the node marked with an arrow in Figure 7. Hence, this makes a potential difference and the current starts to flow though the fuse. The fuse becomes disconnected by the excessive current. The fuse can be used to make a sound alarm to warn the power line disconnection from the digital door lock. It should be noted that the fuse would be physically disconnected even with any temporal access for the power line detachment; an attacker might finally fail to stop the alarm sound.

Providing power to the crystal oscillator is another important issue in implementing countermeasure of power replay attacks. If the crystal oscillator is operated by a removable power source, an attacker can simply disable the crystal oscillator by removing the power source. To avoid this possible threat, the battery needs to be physically protected by using tamper resistant techniques.

B. *Cryptographic Protocol Design*

Protection against eavesdropping and replay attacks has already been studied well in the area of security protocol design [3]. Well-designed cryptographic techniques might play an important role in protecting communication links inside an electronic door lock from eavesdropping and replay attacks. For example, the input from keypad is authenticated if the central processing unit can successfully decode the transmitted input with a pre-shared key. To implement cryptographic operations on the circuit level, we need to consider introducing physical layer encryption [4] and authentication [5] protocols — spread spectrum modulation techniques, such as frequency hopping and direct sequence, might be used to generate scrambled signals at the physical layer under the control of a secret key that the keypad and central processing unit share in advance.

To deploy cryptographic protocols for door locks, there are three challenging issues: (1) At the physical layer, prior coordination or secret sharing between the keypad and central processing unit is required. We expect that this might be achieved under manufacturing process; (2) cryptographic protocols must securely be implemented against classical side channel attacks, such as timing or power analysis; and (3) central processing unit and solenoid must be integrated onto a single circuit board to prevent power replay attacks at the lower layer addressed in this paper. Without strong protection for the voltage supply to the solenoid, cryptographic protocols only offer slight improvement against keypad logging attacks.

C. *Detecting Abnormal Behavior*

The installation of a backdoor component may introduce new physical characteristics (e.g., extra capacitance on the circuit). In principle, these characteristics can be used to detect the existence of the backdoor. For example, when the overall capacitance on the circuit increases due to the added backdoor, we can measure an additional time delay in operating the solenoid.

Manufacturers can construct a set of fingerprints for electric characteristics of normal door lock circuits such as power consumption, temperature, and processing time. We can design a verifying process with these fingerprints to check whether the circuit of a door lock has been modified. This is often called as a side-channel analysis. An alarm should regularly monitor these physical characteristics and warn users if some suspicious changes are detected.

VII. Related Work

Despite the importance of door lock security, there have been only a few studies of the actual security analysis of door locks.

Blaze [6] particularly studied the security of master-key locking systems and discovered their vulnerabilities. A typical master-keyed lock system checks each pin information independently, not their combination. This architectural design flaw causes the vulnerability of master-keyed lock systems – a working master key can be generated within a small number of trials if a single master-keyed lock and any valid key (not the master key) are given. The general security issues of mechanical locks are also briefly summarized in Chapter 11 in [3].

As for electronic door locks, Brocious [1] demonstrated that a popular type of hotel room locks can be vulnerable through reverse-engineering of the used lock protocol. The DC barrel connector can be used for transmitting data or command. With this channel, an attacker can read the secret data at a specific memory address, which is used for opening command.

Some guidelines introduced challenging issues and best security practices for designing secure door locks. The Centre for the Protection of National Infrastructure (CPNI) particularly provided security practices to security door sets and their associated locking hardware [7]. Their guideline pointed out important features which should be carefully considered when designing door locks. For example, we should consider various threats such as accidental damage, fire, opportunistic crime and organized crime. In this context, the attacks presented in this paper can be categorized into the organized crime. Also, the `BS-EN-14846:2005` standard from Door & Hardware Federation (DHF) summarized nine major issues for designing stable and secure door locks [8]. To protect door locks against possible electrical manipulations, this standard presented several security requirements in four grades — *Grade 0* represents the lowest resistance against electrical attacks while *Grade 3* represents the highest resistance level. Table I summarizes the security requirements and grades related to the attacks addressed in this paper. According to their criteria, door locks with the highest resistance level (*Grade 3*) should be deployed to prevent installing malware at board level where cutting of cables and/or wire manipulation are required. Although those guidelines and standards specified the detailed security requirements for door locks, they did not mention how to implement secure door locks to satisfy the requirements.

TABLE I. GRADES FOR FEATURES TO PROTECT DOOR LOCKS AGAINST ELECTRICAL MANIPULATION (THIS TABLE WAS ADOPTED FROM [8])

Requirement	*Grade 0*	*Grade 1*	*Grade 2*	*Grade 3*
`Voltage drop protection`	–	–	Yes	Yes
`Protection against cutting of cables`	–	–	Yes	Yes
`Protection against wire manipulation`	–	–	–	Yes
`Resistance to electromagnetic manipulation`	–	–	Yes	Yes

Our work is more focused on the design flaw at the physical layer in electronic door locks that are used in practice. We showed that a hardware backdoor can be simply installed by an attacker who has access to their back sides. This paper is extended from the earlier work [9].

VIII. Conclusion

Current electronic door locks are susceptible to hardware backdoor tampering by insiders with temporal access to the unit of the lock which is placed on the inner side of a door. We implemented a prototype to show the feasibility of inside attacks – the prototype can be covertly inserted to the electronic door lock without any change in its appearance.

To reduce the risk of such a hardware backdoor, we need to securely protect communication channels inside the box. We particularly suggest the following three ways: (1) an alarm for detecting power line removal should be implemented at the board level; (2) cryptographic protocols can securely be deployed between the keypad and central processing unit; and (3) physical characteristics of a door lock should be monitored to detect their changes by backdoors on circuit.

Future work is envisioned to implement suggested countermeasures and evaluate their performance. We will consider how to integrate those techniques with existing door locks without huge implementation costs. To show the effectiveness of the proposed attacks, we also plan to analyze how many accommodations in the real-world are currently using a vulnerable door lock type against those attacks.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (No. 2014R1A1A1003707), the ICT R&D program (2014-044-072-003 , 'Development of Cyber Quarantine System using SDN Techniques') of MSIP/IITP and the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2015-H8501-15-1008) supervised by the IITP (Institute for Information & communications Technology Promotion).

References

[1] C. Brocious, "My arduino can beat up your hotel room lock," in *Black Hat USA 2012*, 2012.

[2] A. Greenberg, "Hotel lock hack still being used in burglaries, months after lock firm's fix," *Forbes*. Available: http://www.forbes.com/sites/andygreenberg/2013/05/15/hotel-lock-hack-still-being-used-in-burglaries-months-after-lock-firms-fix/, [Last accessed: 15 August 2013], 2013.

[3] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Wiley Publishing, 2008.

[4] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[5] P. Yu, J. Baras, and B. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, 2008.

[6] M. Blaze, "Cyptology and physical security : Rights amplification in master-keyed mechanical locks." IEEE Security and Privacy, 4 2003.

[7] "A guide to security doorsets and associated locking hardware," The Centre for the Protection of National Infrastructure, 2013.

[8] "Electromechanically operated locks & striking plates to bs en 14846: 2008," Door & Hardware Federation, 2011.

[9] S. Oh, J. Yang, A. Bianchi, and H. Kim, "Power replay attack in electronic door locks," in *the 35th IEEE Symposium on Security and Privacy (Poster)*, 2014.