Poster: Power Replay Attack in Electronic Door Locks

Seongyeol Oh, Joon-sung Yang, Andrea Bianchi, Hyoungshick Kim
College of Information and Communication Engineering
Sungkyunkwan University
Suwon, Republic of Korea
Email: {seongyeol, js.yang, abianchi, hyoung}@skku.edu

I. Introduction

Electronic door locks have recently become popular since they have many 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. They might also be invulnerable to the existing physical attacks against mechanical door locks[1]. Despite these known benefits of electronic door locks, we question whether electronic door locks are really secure enough against any possible intrusion and alterations. Manufacturers often claim that their electronic door locks are secure and against a wide range of attacks despite the fact that several flaws have been recently discovered (e.g, [2] and [3]), but the current focus was only directed to one particular type of adversary attacks by a stranger who tries to open doors from outside — ignoring an insider attacker with temporal access to the inside of a lock. However, the second type of adversary models can also be found in many real life scenarios. For example, a thief who sojourns in a hotel room protected by an electronic door, obtains complete physical access for a prolonged period of time to the electronic door lock. Hence, the thief would have plenty of time to modify some parts of the lock in the room or implement a hidden backdoor switch that could be used to steal the belongings of future guests who will stay later in the same hotel room.

We found that the most popular and commercially endorsed electronic door locks cannot cope with this type of threats. An insider attacker can covertly insert malicious hardware components into an electronic door lock to replay a valid DC voltage pulse to illegally open the door. We name this attack the "Power Replay" attack since the inserted component replays a power supplement irrespective of the central processing unit in the target door lock. Our experiments with the four electronic door locks showed the feasibility of power replay attacks: all door locks that we investigated were vulnerable to power replay attacks.

II. Power Replay Attack

We experimentally investigated the possibility of power replay 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.

These electronic door locks follow a common architecture. An electronic door lock consists of three functional units: a *keypad* for the user input, a *central processing unit* which detects the input and denies or grants authentication, an *actuator (a solenoid)* which is used to open or close the lock, and *batteries* for power supply. Figure 1 shows an example of such door locks.

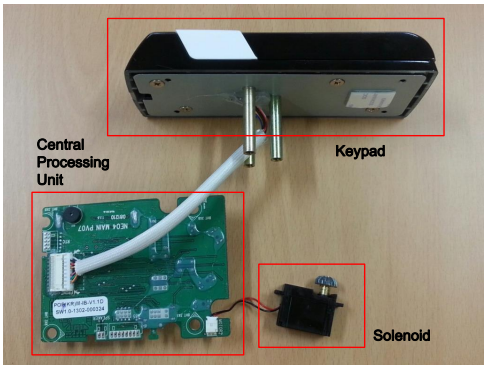

Fig. 1. An example of electronic door lock (made by `Gateman`)

All electronic door locks that we observed use the same procedure to open the lock. When a user provides valid credential (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. Here there are two communication channels that attackers might be interested in: (1) the **data channel** between keypad and central processing unit for coded signal transfers and (2) the **power line** between central processing unit and solenoid for the delivery of DC voltages.

A. Attack Scenario

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 who owns a typical screwdriver can remove the back lid cover of the door lock protecting the internal components. Thus an insider

attacker who has accessed to the inside of a lock can intercept, might manipulate, fabricate, or interrupt the transmitted data and/or power over these channels. In this paper, we have focused on replay attacks for the power line, which is a simple but powerful attack to which most electronic door locks are susceptible. In practice, it is enough to provide the necessary voltage by the solenoid in an electronic door lock to open the door.

Figure 2 shows the overview of a power replay attack. The core idea is to insert some malicious hardware components inside the door lock (*a backdoor*) which can remotely supply 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 parallel circuit to the original circuit, which does not substitute but choosiest with the original. From the user perspective, no changes of the hardware 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.

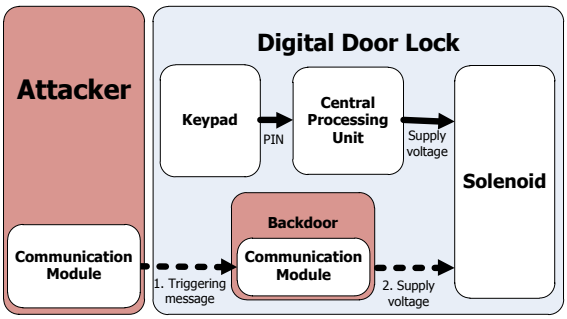

Fig. 2. The overview of power replay attacks: Dotted lines represent a malicious operation by attacker while solid lines represent a normal operation of door lock.

B. Electric Power Measurement

To analyse the electric power needed for the power replay attack, we measured the output voltages and currents at the solenoid in each door lock with an oscilloscope when the door lock actuates. In the experiments, we found that the voltage level provided to the solenoid was on average 6.5V (+6.5V is supplied to open the lock, -6.5V to close it). To simplify the hardware, we empirically tested for several door lock brands (`Hyegang`, `Gateman`, `Mille` and `Samsung`) different input voltage configurations ranging from 0 to 6.5V in 0.1V steps. We found that in the worst case an attacker is required to supply 0.4W ($1.6V \times 0.25$A) to effectively operate the lock. These experiments show that an attacker can base the attack using a small external power source (e.g., button cell, as those found in watches) that can easily fit inside the door lock shell.

III. Implementation

As bluetooth is stable and low powered wireless technology, we implemented a bluetooth based backdoor. The backdoor (see Figure 3) consists of `Nulsomino-HANA`, the tiny micro-controller which is compatible with `Arduino Leonardo`, bluetooth embedded module and two Lithium-Polymer batteries. For pairing with bluetooth module and sending a triggering message through the terminal, we used the free bluetooth interface application, `BTInterface Free Trial BETA`. The micro-controller sets HIGH the digital I/O pin connected to a solenoid when receives a doorlock open triggering message. `Nulsomino-HANA` can provide 0.2W ($5V \times 0.04$A) which is sufficient for most of our target door locks. Our demonstration is available in YouTube[1].

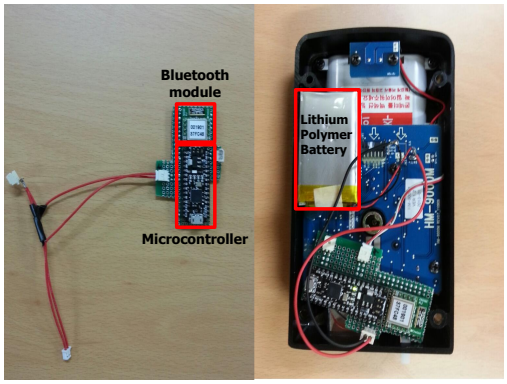

Fig. 3. Our prototype implementation for a power replay attack based on bluetooth (on `Hyegang`)

IV. Conclusion and Future Work

We found that the current electronic door locks are susceptible to a hardware backdoor by insiders with temporal access to the inside of a lock. We implemented a prototype to show the feasibility of such attacks - the prototype can be covertly inserted to the electronic door lock without any modification in the appearance or in the standard functionalities.

To prevent a power replay attack, we suggest future avenues of research: (1) providing an alarm to warn users when the door lock was tampered; and (2) detecting additional hardware installation by sensing variations in the capacitances of inner circuit. We plan to implement these countermeasures as a future work.

References

[1] Matt Blaze. Cryptology and Physical Security : Rights Amplification in Master-Keyed Mechanical Locks. In *IEEE Security and Privacy*, April 2003

[2] Cody Brocious. My arduino can beat up your hotel room lock. In *Black Hat USA 2012*, July 2012

[3] Andy Greenberg. Hotel Lock Hack Still Being Used In Burglaries, Months After Lock Firm's Fix. In *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], May 2013

[1] http://www.youtube.com/watch?v=Id7HclNYc0s