Towards Wireless Spiking of Smart Locks

Abdullah Z Mohammed*¶, Alok Singh*, Gökçen Y Dayanıklı†, Ryan Gerdes*, Mani Mina ‡ and Ming Li §

*Department of Eletrical and Computer Engineering, Virginia Tech
†Qualcomm, San Diego, CA
‡Department of Eletrical and Computer Engineering, Iowa State University
§Department of Eletrical and Computer Engineering, University of Arizona

***Abstract*—The rapid growth of the Internet-of-Things (IoT) has made Smart Homes not only possible but popular in our society. While devices such as wireless security cameras, smart locks, etc. can be more convenient than their traditional counterparts, and may even lead to an increased sense of security, they may actually cause an increase in the attack surface of a home. For example, successful cyber attacks against these smart devices has been extensively documented in the literature. In contrast to existing work we discuss the vulnerabilities of these devices from a cyber-physical perspective; specifically, the threat posed by intentional electromagnetic interference (IEMI). In this paper, we present a methodology to carry out 'wireless spiking' attacks on smart lock devices that would allow an unauthenticated adversary to open a lock, without direct physical tampering, through the manipulation of its electrical control circuitry using IEMI. We demonstrate the proposed methodology—reverse engineering, identification of attack points, development of an attack vector, and design and transmission of attack signals—on a commercially popular smart lock. In doing so we lay the groundwork for wireless spiking attacks on smart locks, in general.**

***Keywords*—intentional electromagnetic interference (IEMI), IoT security, cyber physical systems security, smart lock**

I. Introduction

A smart home consists of inter-connected electronic devices that interact with the physical world, using sensors and actuators, to provide improved security for, and better (e.g., easier or more efficient) control of, our a home. The devices, such as wireless security cameras, smart doorbells, and smart locks are generally thought to provide stronger protection against home threats (e.g., theft or break-ins) than their conventional counterparts; however, like most devices, and especially wireless ones, they are vulnerable to cyber attacks. For example, research has shown that the smart homes are vulnerable to Denial of Service (DoS) [3] and traffic analysis [4], which may lead to loss of functionality (e.g., a door can't be opened) or privacy (e.g., lack of activity may indicate the home is unoccupied). On the other hand, the impact of cyber-physical attacks on smart homes has not been extensively studied.

A smart lock is possibly the most logical starting point in designing a secure smart home. A market report [5] predicts the number of smart lock devices sold annually will rise to more than 25 million by the year 2023 and the smart lock market be worth $2.4 B. The many functionalities of a standard smart lock include allowing for the locking/unlocking of the door via a passcode, fingerprint scan, or even remotely using, e.g., a smartphone.

¶Corresponding Author Email: abdullahzubair@vt.edu

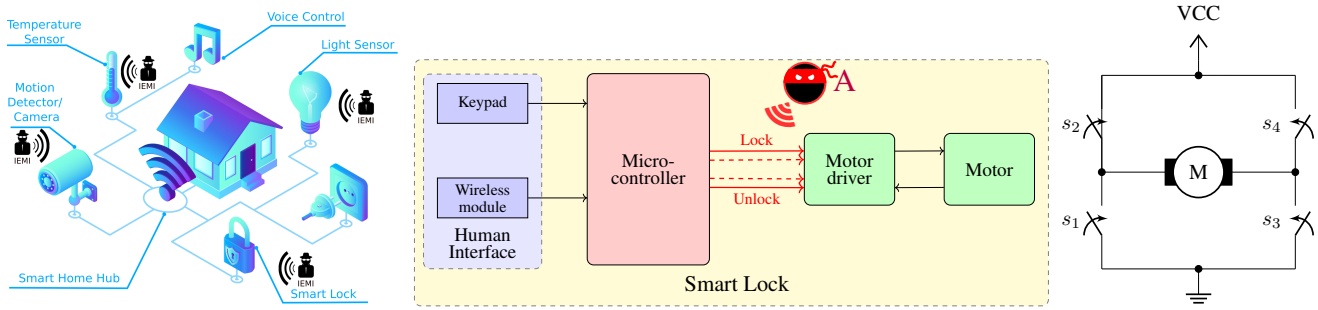
In an intentional electromagnetic interference (IEMI) attack, an adversary uses electromagnetic waves as the primary means by which to manipulate a device in such a way as to produce an intended secondary effect. IEMI-based attacks have been demonstrated that alter the voltage at a sensor's output and change the apparent timing of actuator control signals [6]. A typical smart home will have temperature sensors, motion detectors, cameras, light sensors and smart locks, all of which an IEMI-capable attacker can target using low-cost and widely available signal sources, amplifiers and antennas (Figure 1a).

In the context of a smart lock, the aim of an IEMI attack is to lock/unlock the associated door, without direct physical tampering (i.e., no disassembly or removal of the lock), by manipulating the voltage signals of the lock's motor control circuitry. Within the locksmith community, the technique to force the unlocking of an electronic lock is known as voltage spiking. Specifically, the motor in a lock is opened by connecting the motor terminals, via wires, to a power source that is sufficient to drive the motor. This often necessitates that the lock be either partially disassembled or drilled into. In this paper, we propose a completely non-invasive wireless form of spiking that leverages IEMI. *Wireless* spiking, when fully realized, can bypass standard authentication and encryption methods used to control smart lock and would allow for unauthorized entry into a homes without direct tampering to the door or lock, even when electrical shielding is used.

In this work we propose, and illustrate the use of, an attack methodology necessary to compromise smart locks, in general, through wireless spiking. It consists of understanding the workings of the electrical circuit architecture of the device through reverse engineering and identification of attack points in the circuit that are vulnerable to IEMI. Based on the characteristics of the attack points and the particular motor control circuitry, a theory of attack can be developed. The exact characteristics of the signal used to manipulate the circuitry must then be determined; e.g., its frequency and duration. The final aspect of the methodology is establishing the minimum power required to manipulate the lock, at a given distance, and establishing a way to localize the IEMI, if the theory of attack requires it. We demonstrate the proposed methodology on the commercially available and popular Smart Lock X (anonymized). We believe that the methodology is broadly applicable to all smart lock devices.

A. Related Work

IEMI has recently been established as a significant threat to sensors and actuators. It has been demonstrated that IEMI can be



(a) (b) (c)

Figure 1: (a) Illustration of devices that an IEMI-capable adversary can target to attack a smart home (Image source: iuriimotov © 123RF.com [1]). (b) The hardware architecture of a smart lock in the presence of an adversary, A, trying to lock and unlock the smart lock through IEMI. (c) The circuit architecture of a generic H-bridge. The switches s_2 and s_3, when closed, move the motor in one direction and s_4 and s_1 move it in the opposite direction [2].

used to manipulate sensor outputs [7], [8], control actuators [6], [8], and even alter digital communications between embedded systems and these components [6].

While there has been some work that examines the security of smart locks from a cyber perspective, e.g. [9]–[11], cyber-physical attacks against these locks remain largely unexplored [12], [13]. In [14] a side-channel attack (differential power analysis) was used to extract the secret key used by the lock for adding authorized transponders and users, thus allowing the attacker full control of the lock. A fault analysis was performed against an FPGA-based lock controller analogue in [15], where it was found that if such faults could be injected into the lock then its integrity could be compromised. The technique most closely related to ours, viz. *spiking*, has been utilized in the locksmith community for years to open electronic locks [16]. In spiking an electronic lock is controlled by attaching an external power source (e.g., a battery) directly to the motor [17], causing it to move and open the lock. This technique, while effective [18], [19], is invasive in that it requires some disassembly of, and/or drilling into, the lock.

II. Background and Threat Model

In this section, the background required to understand the methodology of attack is provided along with the adversary's goals and capabilities.

A. Architecture of a Smart Lock

A generic smart lock architecture includes a microcontroller, a human interface module and a motor controlled by a motor driver (Figure 1b). The interface module is typically a keypad where a pass code can be entered to lock/unlock the door. Wireless-enabled smart locks can also be unlocked remotely, e.g., through a (hopefully authenticated) link with a smart phone or fob. The microcontroller receives input from the interface module, evaluates its acceptability (e.g., the provided pass code does or does not match the stored code), and decides whether to actuate the motor, usually via a motor driver controlled by a general purpose input output (GPIO) peripheral.

Most GPIO pins operate at 3.3 V or 5 V and can source only a small amount of current (mA), whereas higher voltage/currents are required to run the lock's motor. Thus a motor controller is used to supply the power required to control the direction/speed of the motor. A commonly used motor controller is the H-bridge, so-called because it consists of electrical switches laid out in the shape of the letter 'H' (Figure 1c). When one pair of switches, i.e., s_1, s_4, are closed and the other, i.e., s_2, s_3, are open the current from the voltage supply, V_{cc}, flows from s_4, through the motor, to s_1 and then to ground, causing the motor to run in one direction. The opposite configuration of the switches runs the motor in the reverse direction [2]. The switches are usually transistors, either Bipolar Junction Transisitos (BJTs) or Field Effect Transistors (FETs) and, again, controlled by the GPIO pins of a microcontroller.

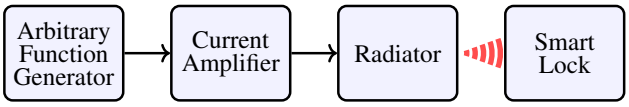


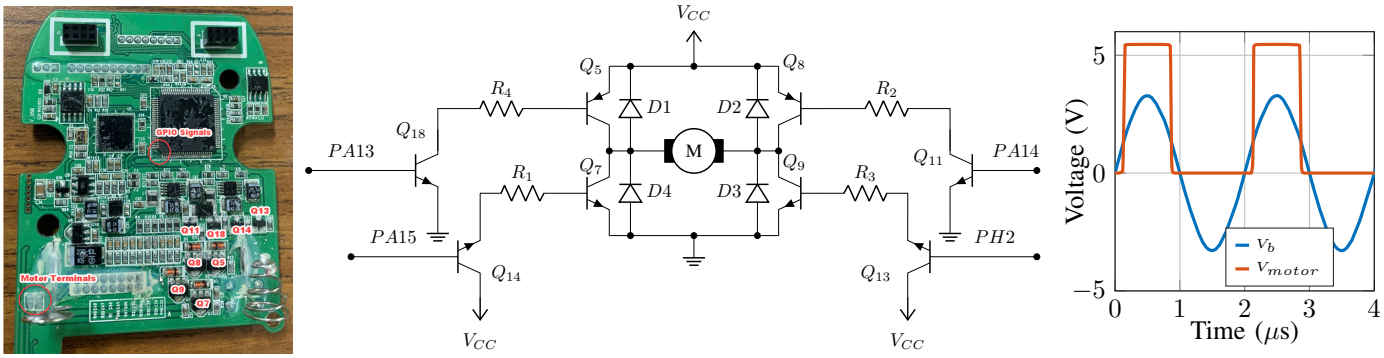
Figure 2: Adversarial Setup: The adversary generates the attack signal using an arbitrary function generator, amplifies the current and feed it to a radiator to produce a high intensity magnetic field directed towards the smart lock.

B. Threat Model

The adversary aims to lock/unlock the smart lock by altering, through IEMI, the low-level voltage signals from the microcontroller (Figure 1b). They lack a wired connection to the smart lock, and do not tamper with the casing of the lock or door, but they are in close proximity to it (centimeters away). Because the adversary needs to generate IEMI capable of penetrating the metal enclosure of the lock (and possibly the metal door it is situated in), we incorporate the threat model of [6], whereby the magnetic near field, as it is difficult to shield against, is assumed for IEMI. The adversary's hardware setup consists of a current amplifier to produce the high current necessary to generate a magnetic field sufficient to induce the necessary voltage changes in the lock, and a radiator to direct the field towards the smart lock (Figure 2).

III. Foundations of Wireless Spiking

In this section we detail a methodology necessary to execute wireless spiking on smart locks and, through experimentation, demonstrate it on a commercial smart lock. In outline, by reverse engineering, we extract the circuitry of the device



(a) (b) (c)

Figure 3: (a) Top view of the Smart Lock X PCB along with motor drive components highlighted. (b) Equivalent Circuit Model of the motor drive circuit for the Smart Lock X is given. Resistors R_1-R_4 are used to limit the current. Transistors (Q_{18}, Q_{14}, Q_{11},Q_{13}) controlled by the GPIO pins amplifies the input current. "M" denotes the dc-motor for the lock, and D_1-D_4 are used as flyback diodes [20]. (c) The base (V_b) voltage of transistor Q_{14} and voltage across the motor (V_{motor}) when a sinusoidal input is applied to `PA15`. The motor stays at rest during the negative cycle of sine wave.

to understand its operation. This is essential in identifying vulnerable attack points for IEMI and developing a method by which IEMI may manipulate the circuitry in the required fashion. Then we move forward in designing the attack signal (e.g., its frequency and the duration). Through simulation we estimate the power that a radiator would require to generate sufficient IEMI to induce the required voltage on the attack points. Lastly, we discuss methods to localize the field to specific attack points.

A. Reverse Engineering

The Smart Lock X was completely disassembled to expose the PCB, control circuitry, and locking mechanism (Figure 3a). The motor was disconnected from the PCB to expose motor terminals and, using a continuity test, connections from the motor to the components Q_5, Q_7, Q_8, Q_9 were established. Given their markings, shape, and layout it was clear at this point that the components were transistors and that an H-bridge circuit was used to drive the motor of the lock. It was definitely established that the transistors were NPN/PNP BJTs by using a multi-meter: the probable base of the transistor was attached to the positive terminal of the multi-meter and the negative terminal of the multi-meter was attached to the probable emitter. For an NPN transistor, the meter would indicate a voltage drop between $0.4\,\mathrm{V}$ to $0.9\,\mathrm{V}$, whereas an impedance measurement would indicate a PNP if an "Over Limit" reading resulted [21]. Using a continuity test, additional transistors Q_{11}, Q_{13}, Q_{14} and Q_{18} were identified as part of the motor driver as they were connected to the base of the transistors that control power to the motor. The voltage supplied to the motor was measured at $6\,\mathrm{V}$.

Visual inspection of the PCB (e.g., following traces from the H-bridge) suggested that a microcontroller was used to control the motor driver; IC markings revealed it to be from the *STM32L15xVC* family [22]. Continuity tests were performed between the transistors and pins of the microcontroller to establish the existence of a connection to it and the H-bridge; perusal of the datasheet indicated that these pins (`PA13`,`PA14`,`PA15`,`PH2`) could serve as GPIO. Measurements confirmed they were configured for $3.3\,\mathrm{V}$ operation.

PA14	PA15	PA13	PH2	Motor
Low	Low	Low	Low	No operation
High	High	Low	Low	Unlock
Low	Low	High	High	Lock

Table I: H-bridge Truth table: how signals from the microcontroller influence the lock.

By measuring the suspected GPIO pins during locking and unlocking, we determined that $3.3\,\mathrm{V}$ from the microcontroller was used to turn on the transistors Q_{18}, Q_{14}, Q_{11}, and Q_{13}. These transistors are used to amplify the output current of the GPIO pins, as a micro controller does not generally provide sufficient current to turn on the (current controlled) H-bridge transistors (Q_5, Q_7, Q_8, Q_9). Specifically, the amplified GPIO output current generates sufficient base drive current, which when applied to the base terminal of the H-bridge transistors causes them to operate in the saturation region (i.e., turn `ON`). The GPIO pins themselves are not used to drive the motor as it requires orders of magnitude more current than the pins can provide. Based on the above procedure an equivalent circuit model (ECM) was built of the circuit (Figure 3b) and its functionality validated in an LTSpice circuit simulation. Table I summarizes the voltage-pin combinations necessary to control the lock (low being $0\,\mathrm{V}$ and high $3.3\,\mathrm{V}$) and which an attacker must induce in order to change the lock's state.

B. Attack Points and Theory of Attack

Having gained an understanding of the smart lock's electrical operation, we move on to the identification of an attack point(s) to target with IEMI. Direct control (powering) of the motor as an avenue to unlock/lock the device was viewed as impractical. First, the power needed to actuate a motor is orders of magnitude greater than needed to modify common digital signals (e.g., $3.3\,\mathrm{V}$) and, indeed, is larger than has been used/demonstrated in attacks found in the open literature. Second, the threat model we incorporate from [6] uses time-varying currents, specifically sinusoidal ones, that create magnetic fields that are zero mean (i.e., no DC component)[1].

[1]A DC magnetic field cannot induce a voltage on circuitry as its derivative is zero and by Faraday's law the resulting voltage would thus be zero.

Thus, even should sufficient power be provided at the motor terminals, the coupled voltage would be a sinusoid with zero-mean: this would merely cause the motor to rotate in one direction during it's positive half cycle and in the opposite direction during the negative half cycle, resulting in zero actual movement on the part of the lock.

The rationale to use a narrow-band sine wave as the attack signal—as opposed to other zero-mean, time varying, wide-band signals such as square or saw tooth waves—is that they are far simpler to generate and transmit at high power levels. The hardware (signal sources, amplifiers and antennas) for narrow-band signals are commonly available, cheaper, and more effective (powerful) than their wide-band equivalents.

The GPIO pins responsible for controlling the movement of the motor through low-voltage signalling are thus the preferred attack point. In [6] it was demonstrated that GPIO signals could be manipulated, but in a random and uncontrolled fashion, while in [8] switches were reliably closed. We leverage and expand on both of these mechanisms of attack to introduce a plausible mechanism for an attacker to cause the switches to open/close.

To unlock the smart lock wirelessly, the adversary needs to induce voltage on the unlock GPIO pins (`PA14, PA15`) (Table I). When induced sinusoidal voltage crosses the threshold voltage ($V_{be} \approx 0.7\,\text{V}$) of the transistors, Q_{14} and Q_{11}, their region of operation moves from cut-off to active. This causes the H-bridge transistors Q_7 and Q_8 to switch `ON` and rotate the motor in the direction of unlock. When the induced voltage is less than the threshold voltage, the attack signal has no effect on the motor and it stays at rest (Figure 3c).

Similarly, if the adversary intends to lock the device, the lock pins (`PA13, PH2`) should be attacked. It should be noted, however, that the induced voltages on the unlock and lock pins should never cross the threshold simultaneously. This would switch `ON` all the four H-bridge transistors at the same time and create a short circuit between V_{cc} and ground, thus damaging the circuitry of the lock (Figure 3b). This necessitates that the generated EM field be localized precisely so that the voltage is induced only on the target GPIO pins. The strategies to achieve localization is discussed in Section III-E.

We validated the above theory of attack through further LTSpice simulations. Specifically, a sine wave of 3.3 V was applied to `PA14` and `PA15` from 0 µs to 10 µs to emulate the induced voltages on the pins during an unlock attack (Figure 4, top). The voltage across the motor terminals can be seen to increase during the positive half-cycle of the sine waveform (Figure 4, bottom). Over the duration of the attack, an average of 2.35 V was measured across the motor, which would cause it to move in forward (unlock) direction. Similarly, to lock, starting from 10 µs a sine wave of 3.3 V was applied to `PA13` and `PH2` (Figure 4, middle). The voltage across the motor terminals shows an average voltage of −2.35 V, which would cause it to move in reverse (lock) direction (Figure 4, bottom).

The time spent to reverse engineer the Smart Lock X and identify attack points was roughly eight hours. With the same amount of effort, we reverse engineered another smart lock, Smart Lock Y, from a different manufacturer. We discovered that it also employs H-bridge as the motor-driver and although FETs were used as switches instead of BJTs, the working of circuitry was similar. Therefore, for Smart Lock Y as well,

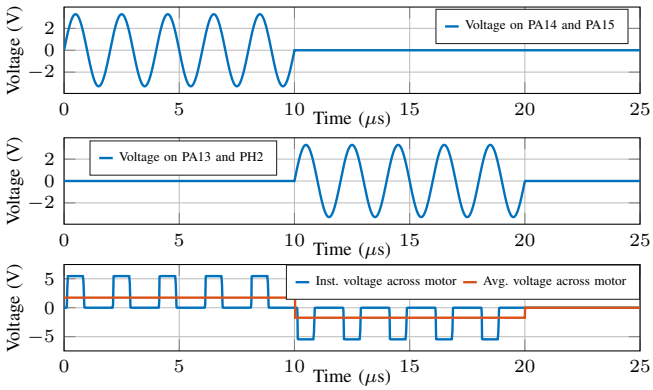


Figure 4: LTSpice simulation of the equivalent circuit model under attack. An AC sine wave applied to the GPIO pins moves the motor forward/backwards.

the preferred attack points are the control signals between the GPIO pins of the microcontroller and the H-bridge. This can be generalized for any smart lock device because we believe that most, if not all, of the devices use H-bridge based architecture.

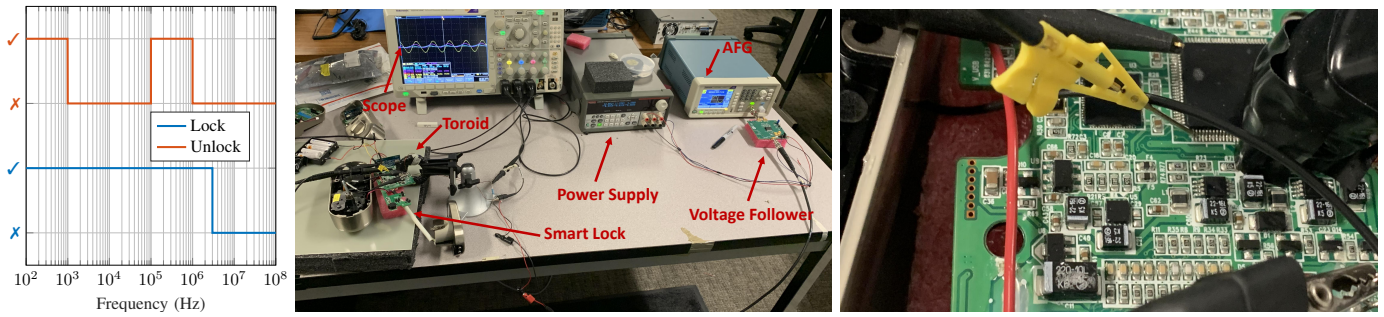
C. Attack Signal Characteristics

Having established an attack vector to control the lock, we then focused on selecting a signal(s) that would allow manipulation with the lowest attacker cost (e.g., minimizing the power needed to open/close the lock at a given distance). From a power and transmission perspective, the two most important components of the attack signal to consider are its frequency and duration: while lower frequency/duration signals are cheaper to amplify, their transmission is generally less efficient. However, as we discuss below, lower frequency signals will generally not couple as efficiently to victim circuitry, so the trade-off is seldom straightforward.

With this in mind, we performed a series of experiments, both wired and wireless, on the Smart Lock X to determine which signal types would open the lock most advantageously for the attacker. The first set of experiments yielded the frequencies of signals that would open the lock, while the second sought to understand at which frequency the attacker would couple power to most efficiently (i.e., the ratio of input power of the attacker setup to power observed on the lock circuitry), and the final experiments determined how long an attacker would need to transmit a given signal to affect the lock.

1) Lock/Unlock Frequencies: As discussed in Section III-A, the motor driver of Smart Lock X is designed to be driven by a 0 V and 3.3 V rectangular pulse, whereas an attacker induces a rectified sinusoid on the driving line. We thus needed to understand the range of frequencies for which the motor driver responds to/moves the motor in the desired direction.

Measurement Method: The smart lock is powered on. An arbitrary function generator (AFG) connected to a voltage follower is used to generate sinusoidal signals over the range of 100 Hz to 10 MHz with an amplitude of 3.3 V. The output of the voltage follower is directly attached to the GPIO pins of the microcontroller that sends the lock signal to the motor driver (pins `PA13` and `PH2`) using a microSMD connector. It should be noted here that the GPIO pins' default state are



(a) (b) (c)

Figure 5: (a) The frequencies of the sinusoidal signals at which the Smart Lock unlocks and locks when probed physically. (b) The experimental setup for the wireless frequency response measurement. (c) The micro SMD probe connected to the GPIO pin `PA15` of the microcontroller

`LOW` and, in order to maintain that state, the GPIO pins of the microcontroller will sink current when an external signal is applied to it. Therefore, a voltage follower, which is in parallel to the GPIO pin, is employed to source current more than the latter can sink, so that the voltage from the AFG is observed on the GPIO pins. The frequencies at which the motor rotates in the direction of the lock are are noted. Similarly, by attaching the voltage follower's output to pins `PA14` and `PA15` and performing a frequency sweep, the frequencies at which the motor moves in the direction of unlock are noted.

Discussion: To design an attack signal the adversary should select a frequency for which both locking/unlocking occur so that they can use the same attack setup to launch a bidirectional attack. Therefore, the desired range of frequencies for wireless spiking the GPIO pins are from 100 Hz to 1000 Hz and 100 kHz to 1 MHz (Figure 5a).

2) IEMI Compatible Frequencies: Because of the geometry of the PCB traces connecting the microcontroller and motor driver, an attacker will more efficiently induce a waveform on a lock's circuitry at some frequencies rather than others [23]. For Smart Lock X the frequency range of 100 Hz to 1000 Hz can be eliminated because the ratio between transmitted versus induced signal is so low due to: 1) the wavelength of these signals is considerably larger than the dimensions of the PCB traces, and 2) as discussed in [6], Faraday's law of induction states that induced voltages are directly proportional to frequency, thus higher frequencies induce greater voltages. We thus performed experiments to determine at which frequencies the lock's circuitry best responded to IEMI.

Measurement Method: In the experimental setup a toroid with an air gap was used as the radiator, with an AFG connected to a voltage follower circuit acting as a source (Figure 5b). Due to the frequency-dependent impedance of the toroid, a voltage follower was used in an attempt to provide a uniform current, or at least one strong enough, to create a magnetic field that would reliably induce voltages on the lock's circuitry. The toroid was placed around the PCB near the GPIO pins and the voltage induced on the pin `PA14` measured using an SMD microprobe and oscilloscope (Figure 5c).

Additionally, as the toroid produced stray magnetic fields (i.e., fields not confined to the air gap) that could couple to the probe and corrupt the measurements, we introduced a control in the form of an unconnected probe at the same location. An increase in the voltage measured by the connected probe, without a commensurate increase in the disconnected probe, would thus indicate an increased coupling between the wireless signal and the board, as opposed to merely an increase in the coupling of the stray magnetic field to the probes themselves.

A frequency sweep from 100 kHz to 1 MHz was performed and the *coupling ratio* recorded to evaluate the efficacy of attack signals of varying frequency. For our purposes, the coupling ratio is the ratio between the voltage induced on the GPIO pin `PA14` and the voltage across a sense resistor placed in series with the the radiator; the latter of which is proportional to input power. This ratio indicates, assuming equal input power, the frequency that will have the greatest affect on the lock's control circuitry (i.e., induce the greatest voltage. Measurements were taken versus frequency when the lock was powered `ON` and `OFF` to understand whether the lock was more susceptible to attack when in a (probable) sleep or active mode.

Discussion: As expected the disconnected probe shows that induced voltage increases linearly with increase in frequency (it is proportional to the derivative of the current through the radiator due to Faraday's law [6]) (Figure 6, red). The coupling ratio of the GPIO pin is, however, non-linear which indicates that some frequencies are more advantageous to an attacker than others (Figure 6, blue). It was also observed that when the smart lock is powered `ON` the frequency response for $\geq$ 100 kHz is flatter than when it is `OFF`. The source of this discrepancy requires further investigation. An attacker should select the

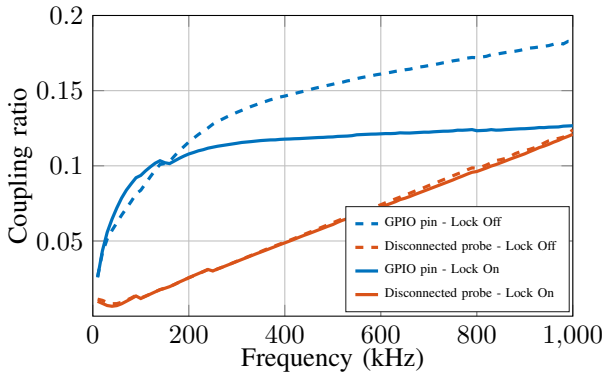


Figure 6: The coupling ratio vs. frequency plots for the lock powered `ON` and `OFF`.

attack signal's frequency as close to $1\,\mathrm{MHz}$ as possible so as to induce the requisite voltage at the lowest cost.

3) Attack Signal Duration: A well-resourced attacker could generate high currents continuously for as long as it takes for the motor to complete the lock/unlock cycle. This, however, may not be cost-effective as the continuous power delivery of amplifiers/sources is considerably lower than their sporadic, peak power delivery (primarily due to heat considerations). We propose to analyze a time-versus-cost trade-off in the form of lower duration attack signals that take longer for the lock to open/close yet consume lower average (RMS) power.

Measurement Method: The experimental setup is as described in Section III-C1. A $1\,\mathrm{MHz}$ sine wave with an amplitude of $3.3\,\mathrm{V}$ was applied to the GPIO pins `PA13` and `PH2` via a wire (this representing the most efficient attack signal). However, in this case the AFG was configured to output the sine wave for a specified duration with large gaps between re-transmission. The initial duration of the signal was set to $1\,\mathrm{s}$ and gradually decreased until the motor ceased to rotate (visual inspection).

Discussion: It was observed that the motor moved slightly in one direction so long as the signal duration was greater than $25\,\mathrm{ms}$ (25,000 cycles of a $1\,\mathrm{MHz}$ sine wave). Interestingly, our experiments revealed that the duration between pulses is a non-factor in a successful attack; i.e., so long as the initial pulse overcomes the inertia of the motor it will always continue to move forward in lock/unlock cycle. This implies that an attacker can wait a significant amount of time between transmitting attack signals (e.g., for the equipment to cool down) without worrying about lock reverting to its previous state. In summary, an attacker only needs to transmit a fixed-frequency sinusoid for at least $25\,\mathrm{ms}$ to successfully lock/unlock the door.

D. Power

Having established how a lock can be wirelessly manipulated and determined the signal parameters that would produce a cost-effective attack setup, the most substantial impediment (in our view) to the realization of wireless spiking is the requirement to generate a sufficiently high field to induce the necessary voltages at the vulnerable points of the lock.

In Section III-C1 we determined that an attacker needs to induce a sinusoid of $3.3\,\mathrm{V}$ amplitude to lock/unlock the Smart Lock X . To estimate the current required to induce such a voltage on the lock's traces from a distance of $5\,\mathrm{cm}$, we measured the voltage induced using a toroid by a $500\,\mathrm{kHz}$ signal on said traces. We then measured the field produced by toroid in the absence of lock, at the same frequency and power. Assuming an increase in field strength would produce a roughly 2:1 increase in the voltage on the traces it was determined that a magnetic flux density of $24.7\,\mathrm{mT}$ would be necessary to induce a $3.3\,\mathrm{V}$ signal on GPIO pin of the smart lock.

The exact amount of current required to create such a field will depend on the type of radiator used by the attacker. We assumed that they would employ a thirty-turn coil, as such structures are commonly used to generate high-intensity magnetic fields. Using a 3d electromagnetic simulator, Ansys HFSS, we calculated that an attacker would need to drive the coil with $150\,\mathrm{A}$ source to generate the requisite field. So far as we are aware such sources are not commercially available but could be built.

E. Localization

Depending on the point of attack and topology of the smart lock, it may be necessary for the attacker to ensure that the IEMI affects some elements of the circuit without affecting others (or at least affecting them to a lesser extent). For example, as indicated by the ECM (Figure 3b) if two transistors on the same side of H-bridge (e.g., Q_5 and Q_7) are switched `ON` at the same time, the current will flow from V_{cc} to ground without powering the motor. For the Smart Lock X , all of the control pins (`PA13`, `PH2 PA14`, `PA14`) and associated traces are in close proximity of each other on the PCB. Therefore it is possible (probable) that IEMI generated by the attacker, especially at frequencies with wavelengths larger than the dimensions of the traces, would couple to multiple traces and cause non-targeted switches to simultaneously open/close (depending on state of GPIO lines). Thus it is likely that in order to effect the attack the IEMI must be localized to, or have only an appreciable effect on, only the identified attack points.

We suggest the following strategy to achieve this: It is known that traces on PCB exhibit multiple, distinct resonances at which they respond to EMI more strongly than other traces [23]. By way of a detailed analysis and meticulous selection of non-overlapping attack frequencies (i.e., selecting a frequency that is closer to the resonant peak of one trace and away from the peak of the adjacent trace), we believe it's possible for an attacker to target individual switches even when they are physically and electrically close to others that would affect the outcome of the attack. To add further credence to this supposition, we note that the susceptibility of a trace to EMI is a function of not only a trace's geometry but also its location and orientation to the radiated field [24]. Hence, it is possible that, with the proper orientation of a highly focused magnetic field radiator(s), an attacker will be able to induce sufficient voltages to affect attack points while producing insignificant voltages on non-attack points.

IV. Future work and Conclusion

We laid the groundwork to carry out wireless spiking attacks on smart lock devices. If successful, such an attack would allow an attacker to bypass all of the lock's traditional security mechanisms, such as authentication and encryption, and unlock/lock it by inducing voltages on the device circuitry through IEMI. The proposed attack methodology, demonstrated on the Smart Lock X , included reverse engineering the device circuitry to identify attack points for IEMI. Through experimentation we determined the attack signal's parameters, such as its optimal frequency by measuring the circuit's frequency response to IEMI. The estimation of the power required by the radiator for a successful attack was provided and methods to localize the IEMI field were discussed.

Our future work includes designing a high current amplification circuit that can generate sufficiently power IEMI to induce the 3.3 V on the GPIO pins to successfully open the lock. We will also be designing radiators that can, with proper orientation, generate highly focused IEMI to affect only the desired pins of the microcontroller.

Acknowledgements: This work is supported in part by the National Science Foundation (NSF Grant CNS-1801611) and Army Research Office (ARO Grant W911NF-21-1-0320).

REFERENCES

[1] "Smart home system," 2022. [Online]. Available: https://www.123rf.com/profile_iuriimotov

[2] C. McManis, "H-bridge theory & practice-chuck's robotics notebook," *H-Bridge Theory & Practice-Chuck's Robotics Notebook*, 2013.

[3] U. Saxena, J. Sodhi, and Y. Singh, "An analysis of ddos attacks in a smart home networks," in *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 2020, pp. 272–276.

[4] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home iot privacy," *Proceedings of the ACM on Human-Computer Interaction*, vol. 2, no. CSCW, pp. 1–20, 2018.

[5] J. Narcotta, 2018. [Online]. Available: https://www.strategyanalytics.com/access-services/devices/connected-home/smart-home/reports/report-detail/smart-home-access-control-systems-predictions-players-and-products

[6] J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems," in *Asia Conference on Computer and Communications Security*, 2018, pp. 499–510.

[7] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 145–159.

[8] G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang, and R. Zane, "Electromagnetic sensor and actuator attacks on power converters for electric vehicles," in *IEEE Security and Privacy Workshops*. IEEE, 2020, pp. 98–103.

[9] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. 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*, 2016, pp. 461–472.

[10] M. Ye, N. Jiang, H. Yang, and Q. Yan, "Security analysis of internet-of-things: A case study of august smart lock," in *2017 IEEE conference on computer communications workshops (INFOCOM WKSHPS)*. IEEE, 2017, pp. 499–504.

[11] B. D. Davis, J. C. Mason, and M. Anwar, "Vulnerability studies and security postures of iot devices: A smart home case study," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 102–10 110, 2020.

[12] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[13] R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J. R. Fontaine, A. Filippoupolitis, and E. Roesch, "A taxonomy of cyber-physical threats and impact in the smart home," *Computers & Security*, vol. 78, pp. 398–428, 2018.

[14] M. Weiner, M. Massar, E. Tews, D. Giese, and W. Wieser, "Security analysis of a widely deployed locking system," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 929–940.

[15] J. Lojda, R. Panek, J. Podivinsky, O. Cekan, M. Krcma, and Z. Kotasek, "Hardening of smart electronic lock software against random and deliberate faults," in *2020 23rd Euromicro Conference on Digital System Design (DSD)*. IEEE, 2020, pp. 680–683.

[16] L. Mayhew, *Electronic Safe Locks & How To Defeat Them (Enspyklopedia)*. Unknown: ACLESL.

[17] T. Technologies, "Ionic spike kit," *Tools and Equipment for Security Technicians*. [Online]. Available: https://www.taylortechtools.com/product-page/ionic-spike-kit/

[18] D. Lodge, "Different 'smart' lock, similar security issues," Feb 2019. [Online]. Available: https://www.pentestpartners.com/security-blog/different-smart-lock-similar-security-issues/

[19] A. Lomas, "Smart male chastity lock cock-up," Oct 2020. [Online]. Available: https://www.pentestpartners.com/security-blog/smart-male-chastity-lock-cock-up/

[20] D. Cook, *Adding Gearhead Motors*. Apress, 2015, p. 255–263.

[21] T. Kuphaldt, "Lessons in electric circuits, volume iii–semiconductors," 2009.

[22] *STM32L15xVC Datasheet*, ST Microelectronics, Sep 2021, rev. 8.

[23] J.-K. Du, Y. Kim, J.-G. Yook, J. Lee, and J. S. Choi, "Coupling effects of incident electromagnetic waves to multilayered pcbs in metallic enclosures," in *International Workshop on Antenna Technology (iWAT)*. IEEE, 2015, pp. 359–361.

[24] M. Mehri, N. Masoumi, and J. Rashed-Mohassel, "Trace orientation function for statistical prediction of pcb radiated susceptibility and emission," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 5, pp. 1168–1178, 2015.