Summary of Defensive Charging: Mitigating Power Side-Channel Attacks on Charging Smartphones

Austin Conn
M11809075

ABSTRACT

To help combat cyber criminals from targeting public charging hubs, the authors of Defensive Charging: Mitigating Power Side-Channel Attacks on Charging Smartphones sought to prove the viability of using a malicious charging hub to infer data from a victim's device. To prove their theory, the authors first developed a malicious charging hub that could analyze the power consumption of a connected device. Once proving the viability of the attack, the authors sought to mitigate the attack through both a hardware device and a software mechanism to obfuscate the data that could be inferred. With a viable attack vector and two successful mitigation methods, the door is opened for further research to pick up where they left off.

CCS CONCEPTS

• **Hardware** → **Power estimation and optimization**; • **Security and privacy** → **Side-channel analysis and countermeasures**; *Software security engineering*; *Pseudonymity, anonymity and untraceability*;

ACM Reference Format:
Austin Conn. 2018. Summary of Defensive Charging: Mitigating Power Side-Channel Attacks on Charging Smartphones. In *Proceedings of ACM XXXXX, XX, XX, XX, XX 2018 (ACM XXXXX'18),* 4 pages.
https://doi.org/10.475/123_4

1 INTRODUCTION

Smartphones have forever changed the way people interact with one another, whether it be through social media, phone calls or text messaging. Today, so much of our life lives in the digital domain and our smartphones have become a portal through which we interact with our digital selves. Given our reliance on our portable devices, the need to keep them powered throughout the day has led many to realize the battery life of their phone is no longer sufficient to last them through the day on a single charge. That is where the proliferation of public charging hubs have taken over.

Many public places such as airports, train terminals, and restaurants now offer free-to-use, publicly accessible charging hubs so people can charge their devices while on the go. Due to their ubiquity, the authors of Defensive Charging: Mitigating Power Side-Channel Attacks on Charging Smartphones realized the enticing target these hubs can become for cyber criminals. The authors set out to determine if a viable attack vector exists utilizing these public charging hubs.

Assuming the attack vector is viable, the authors also wanted to determine if a user can protect their vital information through either a hardware based mitigation device or a software mechanism, both meant to obfuscate any data an attacker could infer based on the power consumption of the device as it is charging.

Where the authors' research concludes, I propose several avenues for further research, citing some of the areas missed by their research.

2 RELATED WORKS

In addition to the authors' works in Defensive Charging: Mitigating Power Side-Channel Attacks on Charging Smartphones[2], two additional related works are cited by the authors: "Power to peep-all: Inference Attacks by Malicious Batteries on Mobile Devices" by Lifshits *et al.* [1] and "A Study on Power Side Channels on Mobile Devices" by Yan *et al*[3].

The authors do note that the two mentioned research studies differ from their research in that their research focuses solely on the charging smartphone rather than the battery within the smartphone. The authors recognize that with Lifshits research, the compromised battery would have more precise readings on power consumption as opposed to readings from the charging device.

3 A VIABLE ATTACK VECTOR?

The authors set out to determine whether an attacker, given ample time to inspect and replicate the charging hub, create a device that could analyze the power consumption of the connected smartphone to infer: websites visited by the device, keystrokes or pin codes entered into the device, and whether the device was receiving a phone call. There is precedent for this type of an attack already common in our daily lives; the use of credit card skimmers in everyday items such as gas pumps, point-of-sale terminals, and ATM machines have proven to be a successful means of exploiting a user's data as the attack is imperceptible at the time of exploitation. It is when the bank statement comes that the victim realizes their information has been compromised.

The authors found that the attack was technically possible by building a device that measured the current of the smartphone as it was charging. By applying machine learning to this dataset, an attacker could reasonably infer which websites the device visited, what keystrokes were made on the device, and whether the phone received a phone call while it was charging. Their research concludes that utilizing this device and machine learning, an attacker could greatly improve the success rate beyond randomly guessing.

ACM XXXXX'18, XX 2018, XX, XX, XX

ACM ISBN 123-4567-24-567/08/06…$15.00
https://doi.org/10.475/123_4

4 MITIGATION TECHNIQUES

4.1 Hardware Based

The authors next sought to develop a hardware solution be developed to mitigate the inference of information by the attacker's device. Their mitigation device, nicknamed "The Scrambler" consisted of a micro controller with built in RAM, several MOSFETs, and several load resistors. Each of the load resistors was connected via a MOSFET in such a way that when the MOSFET was activated, the resistor was placed into the charging circuit, thus increasing the current drawn from the charger. Each MOSFET was controlled by the micro controller which was flashed with code that loaded a random value from RAM to generate a random 10-bit bit string. Each bit of the bit string corresponded to each MOSFET where a 0 indicated the MOSFET was OFF, and a 1 indicating the MOSFET was ON. The micro controller would generate a new bit string at a rate of 1kHz leading to a randomized number of resistors being placed into the charging circuit. This allowed the scrambler to fluctuate the current draw from the charger between 0ma and 1488mA. [2]

4.2 Software Based

For their software mitigation mechanism, the authors tried several different experiments to determine an adequate method for increasing power consumption of the smartphone through software and concluded that CPU utilization alone was not sufficient in causing the power consumption spikes desired for a successful mitigation mechanism. To obtain the desired effects, the authors ultimately decided to use Image Manipulation Operations as this required both CPU and RAM utilization as well as allowed for fine tuning of several variables to tailor the power consumption of the device quite accurately.

Their mechanism employed an algorithm that could generate an image of any arbitrary dimension. The algorithm would then perform random rotations on the image and then write the image to memory. After writing the image to memory, the algorithm would not only release but also clean up the memory used by the image in preparation for the next iteration. The authors found this algorithm introduced several variables, including the image dimensions, the computations on the image, and the number of read from and write to memory operations, leading to the authors being able to finely tune their mechanism to have the desired effect on the charging current of the smartphone.

5 TESTING METHODOLOGY

The devices used by the authors for their experiment were a Samsung Galaxy S5 and a Samsung Galaxy S6. Both devices were running a stock Android 6.0.1 image with the default configuration and applications installed. Both devices had an active WiFi-internet connection. The authors installed two applications on each device, the StayAlive application meant to prevent the device from dimming the screen and going into any sleep modes. The second application was a custom Android application that collected metrics from the Android OS for correlation between actions on the victim device and the readings from the malicious charging hub.

The authors employed machine learning in their data analysis for both the unmitigated and mitigated testing. In the first scenario, with no mitigation, the device was connected directly to the malicious charging hub. In the second scenario, the hardware based mitigation, the device was connected to the malicious charging hub via the hardware mitigation device. And for the software based mitigation, the device was connected directly to the malicious charging hub but also had the author's software based mitigation mechanism installed.

The authors developed three test cases to test in the unmitigated and mitigated portions of their research. The first was the website inference test. The authors compiled a list of the top 50 websites as ranked by Alexa in 2017 and utilized a native Android application to launch each website in the Chrome browser, allow the site to load for 15 seconds, close the site, and begin loading the next site.

For the keystroke inference test, the authors used an application similar to the built in Android PIN lock screen. Users held the device in their left hand in portrait orientation while using their right index finger to press each key in any random order. In total, the authors collected data on 2,400 key presses.

For the call detection test, the authors recorded and analyzed the power consumption of the device while at idle as well as while the device was ringing. The testing consisted of twenty phone calls using each of the two distinctly different ringtones.

6 SUCCESSFUL MITIGATION

The authors determined that the mitigation techniques, both hardware based and software based, were successful in reducing an attacker's success rate. The threshold used by the authors to determine the successful mitigation of the attack was based on the success rate of an attacker randomly guessing.

6.1 Hardware Based

During the website inference test, the authors found that using only two bits on The Scrambler, the attacker's success rate was reduced by a factor of roughly four. When utilizing eight bits on The Scrambler, the attacker's success rate crossed below that of random guessing.

During the keystroke inference test, the authors found that utilizing eight bits on The Scrambler was sufficient in reducing the attacker's success rate to below that of random guessing.

During the phone call inference test, the authors found that utilization of even a single bit on The Scrambler was effective at reducing the attacker's success rate to below random guessing.

6.2 Software Based

For all three tests, the authors noted the largest image size tested was 2000x2000 pixels.

During the website inference test, the authors found that any arbitrary image size was effective at reducing an attacker's success rate to close to the success rate of randomly guessing.

During the keystroke inference test, the authors found that the large image size tested of 2000x2000 pixels was sufficient in reducing the attacker's success rate to below randomly guessing.

During the phone call inference test, the authors found that any use of the software mitigation mechanism was sufficient in reducing the attacker's success rate blow random guesses.

7 FURTHER TESTING

The authors also conducted the following test: if an attacker was aware of the mitigation techniques employed, would the mitigation techniques still be sufficient in thwarting the attack? The authors found that while the attacker's success rate did increase given the additional knowledge, the mitigation techniques they employed were still effective and noted the attacker's success rate did not notably approach the results from the unmitigated attacks.

8 MITIGATION DRAWBACKS

The authors found that, while both mitigation techniques were successful in reducing the attacker's success rate below the rate of randomly guessing, they did find that the mitigation techniques negatively impacted the charging speed and power consumption of the device. As the power consumption was increased during their mitigation, the authors also noted the environmental impacts of the mitigation in terms of CO2 emissions.

9 LIMITATIONS OF THE RESEARCH STUDY

The authors focused on the old standard for USB charging devices. The old protocol relied on a constant 5v supply and a variable current, often up to 1500mA. Newer protocols such as Power Delivery and Fast Charging utilize variable voltages up to 20v along with variable current. While this allows a device to charge faster, this would complicate their research as the theoretical attacker's device would need to monitor not only current but also voltage. It would be interesting to see if the same type of analysis could be applied to infer information about the connected device. I would suspect this might make it more difficult as there would be a second independent variable that would need to be accounted for. An analysis could be made converting voltage and current to wattage, but I would suspect this would lead to a loss of precision that this type of analysis would benefit from.

The authors also do not mention other methods of charging, such as wireless charging. At first, I would assume this type of analysis could aid an attacker in attacking a victim device, but with my limited knowledge of the technology enabling wireless charging, I imaging additional variables would be introduced such as the inductance in the wireless charging coils, proximity between transmitter and receiver, etc.

Another limitation of the research study surrounds the implementation of power saving modes in modern smartphones. Power saving modes were implemented to attempt to squeeze more battery life out of the device by design. Given the Mitigation Drawbacks, it would be unlikely that a manufacturer would incorporate a software mechanism to mitigate this type of attack since it leads to greater power consumption and a longer charging time. Further, the research study neglects to mention the likelihood of a manufacturer implementing the hardware based mitigation technique. The compact design of smartphones means physical space is at a premium and adding the additional circuitry would further complicate the design and manufacturing process of smartphones. Further, with additional circuitry would imply a greater cost of materials to produce the phone. Given that manufacturers are trying to maximize profit margins, it is unlikely a hardware implementation would be added as this would further reduce their profit margin on a device that is already very costly to produce.

10 FUTURE RESEARCH OPPORTUNITIES

Given the Limitations of the Research Study, the future opportunities for further research immediately point to the investigation of other charging protocols such as Power Delivery and Fast Charging, as well as alternative modes of charging such as wireless charging.

Another avenue that warrants further research is whether additional information could be obtained using this attack vector. Could an attacker use this method to derive specific information? Bank account details and log in credentials for sensitive websites would be immediate candidates for research. Additional research could be focused at obtaining contact lists, calendar and schedule information, and biometric data could also be of interest to an attacker.

11 CONCLUSION

Using existing attack vectors present in the wild, the authors theorized a new attack vector that could prove to be a viable threat in the future. Given the absence of digital communication with a victim device, the authors theorized an attacker could use the power consumption figures while a device charges to infer key information about a connected victim device. After proving this to be a successful attack vector, the authors sought to mitigate such an attack and devised two approaches to mitigate an attacker's attempt to infer this information.

By developing a hardware based solution and a software mechanism with the aim of mitigating the attack, the authors proved that if an attacker, equipped with a device that could function and appear identically to the publicly available charging hub, attempted to deploy this attack in the wild, there would be a viable method for mitigating the attack. The authors thoroughly analyzed the positive and negative effects employing such a mitigation technique would impose on the user experience, including additional cost of a hardware device and degraded performance due to running a computationally intensive process on the victim device.

The authors' research into this newly identified attack vector have exposed the need for further research into this type of attack vector. This type of attack and the corresponding mitigation efforts could extend to other protocols such as Power Delivery and Fast Charging, as well as other mediums of charging such as wireless charging. Further, this type of research could be employed against tablets and laptops which often accompany people to the locations where these charging hubs may be available to the public.

REFERENCES

[1] Pavel Lifshits, Roni Forte, Yedid Hoshen, Matt Halpern, Manuel Philipose, Mohit Tiwari, and Mark Silberstein. 2018. Power to peep-all: Inference Attacks by Malicious Batteries on Mobile Devices. *Proc. Priv. Enhancing Technol.* 2018, 4 (2018), 141–158.

[2] Richard Matovu, Abdul Serwadda, Argenis V. Bilbao, and Isaac Griswold-Steiner. 2020. Defensive Charging: Mitigating Power Side-Channel Attacks on Charging Smartphones. In *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy (CODASPY '20)*. Association for Computing Machinery, New York, NY, USA, 179–190. https://doi.org/10.1145/3374664.3375732

[3] Lin Yan, Yao Guo, Xiangqun Chen, and Hong Mei. 2015. A Study on Power Side Channels on Mobile Devices. In *Proceedings of the 7th Asia-Pacific Symposium on Internetware (Internetware '15)*. Association for Computing Machinery, New York, NY, USA, 30–38. https://doi.org/10.1145/2875913.2875934