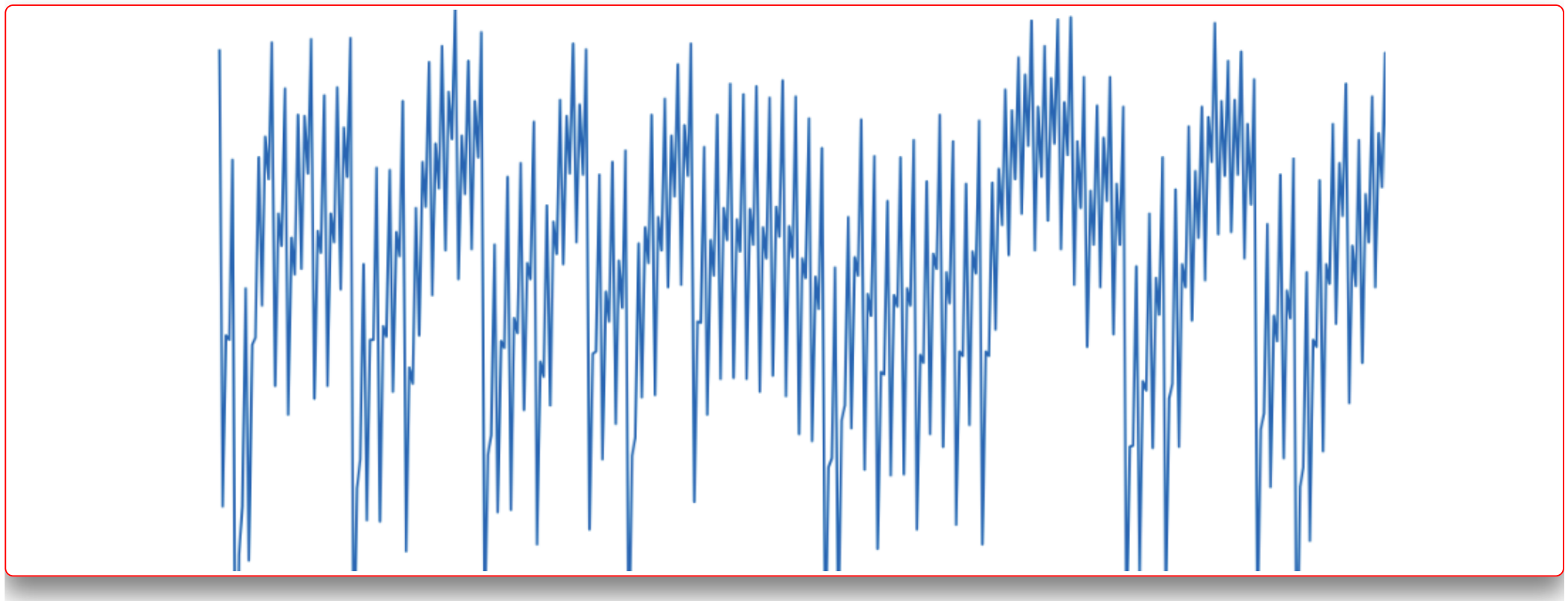
IoT Security - Part 19 (101 - Introduction to Side Channel Attacks (SCA))

asmita-jha

8-December-2020



This blog is part of the IoT Security series, where we discuss the basic concepts about the IoT/IIoT ecosystem and its security. If you have not gone through the previous blogs in the series, I will urge you to go through those first. In case you are only interested in side channel attack (SCA) introduction, feel free to continue.

IoT Security - Part 1 (101 - IoT Introduction And Architecture)

IoT Security - Part 18 (101 - Hardware Attack Surface: JTAG, SWD)

In the last few parts of this blog series, we discussed hardware attack surfaces like SPI, I2C, UART, and JTAG. With an increase in the security concerns and awareness, proper countermeasures are implemented in some devices to avoid easy access to the attacker via these attack surfaces. Unfortunately, even these countermeasures against hardware attacks cannot assure a secure system. This blog will give a basic overview of one of the most famous hardware attacks called the Side Channel Attacks (SCA).This blog is an introductory, conceptual overview of SCA. In future blogs we will discuss details of each type of attack.

Introduction

Side channel attacks (SCA) exploit the information leakages in the system. The leakages can be related to timing, power, electromagnetic signals, sound, light, etc. SCA is a non-invasive and passive attack, i.e., to perform this attack, we don’t need to remove the chips to get direct access to the device’s internal

components or actively tamper any of its operations. This attack can be performed by observing, collecting, and then analyzing the information leakages in the device during processing. These attacks can be used to retrieve any sensitive information from the device. They are most commonly used to target cryptographic devices. Though attacking such devices with a very large keyspace might not be feasible via brute-force, attackers can break these so-called secured systems via SCA. Instead of targeting the standard cryptographic algorithms, SCA targets their implementation on the physical devices to recover the secret parameters by measuring and analyzing the leaked information like power analysis, timing analysis, electromagnetic analysis, etc. Links to some useful resources on SCA can be found at the end of this blog under “References” section.

Types of side channel attacks

Power Attacks

Depending on the data or the code instruction being processed in the device, its power consumption varies. In this attack, the varying power consumption is measured and analyzed to extract the device’s sensitive information or keys. It can be used to break the implementation of cryptographic algorithms like AES-256 in comparatively less time and at less cost. Internally, the devices have integrated circuits that consist of logic gates that are internally made up of transistors. Depending on the charge applied and removed on the transistors’ gate, the current flows to or from the gate, which consumes the observable power and leaks the internal characteristics of the operating algorithm. To measure the power in the device’s circuit, a small resistor of approx 50 ohm, is inserted in series with the power or the ground input. The voltage difference (V) across the resistor is calculated, that when divided by the resistance value®, gives the current(I) as per Ohm’s law, V = IR. Depending on the clock frequency, equipment like digital oscilloscope, hantek, chipwhisperer, etc can be used to sample the voltage differences and collect the trace used for further analysis and attacks. There are a few open-source frameworks like chipwhisperer, SCARED by eShard that can be used for the analysis.

Simple power analysis (SPA)

SPA is the visual analysis of the collected power trace while an operation is being performed to identify it. It is based on the fact that the power consumption at a particular instant of time is the function of operation being carried out by the device. It is targeted to work with fewer traces. This can be used to extract the key or some sensitive information. The power analysis using SPA can give the characteristic of the kind of algorithms being operated, e.g., the square and multiply operations, the number of rounds of block ciphers, etc. This attack involves comparatively more manual analysis. If the device’s power consumption can be randomized internally by adding noise or including dummy clock cycles, then extracting the secret information via SCA gets difficult.

Differential power analysis (DPA)

DPA is more powerful than SPA as it also includes statistical analysis. It is based on the fact that the power consumption at different instant of time for the same operation depends on the data being processed. Though there are different types of DPA, the Difference of Means (DoM) is one of the simple and effective methods to perform it. In this case, it is assumed that the power consumption correlates to the specific bit of an internal register of the hardware that the attacker is not aware of. The portion of the key is guessed. Based on the guessed portion, the target bit is calculated. The trace is then divided into zero-bin and one-bin depending on whether the target bit is 0 or 1. The mean of all the traces in the zero-bin and the one-bin is calculated, the difference of which gives the DoM. Finally, the correct key guess

and the wrong key guess are identified by correlating the power consumption between the guessed and the real power trace. As this attack does not require the attacker to have the system's internal knowledge, it is a black-box attack. However, it is expensive in terms of the number of traces to be collected. It also has the problem of "ghost peaks," i.e., sometimes one can get a strong peak in the statistical graph even for the wrong guesses. More detailed info about DPA can be read from the research paper titled, "Differential Power Analysis," by Paul Kocher, Joshua Ja e, and Benjamin Jun.

Correlation Power Analysis (CPA)

Research works in SCA areas later came out with the Correlation Power Analysis (CPA) method, which was found to be more effective than the DPA. The research paper, "Power Analysis Attacks to Cryptographic Cir-cuits: a Comparative Analysis of DPA and CPA" shows the comparative analysis between CPA and DPA. It requires a lower number of power traces w.r.t DPA and also avoids the problem of ghost peaks. CPA is implemented by using the power models : Hamming Weight or Hamming Distance. Hamming weight is linearly related to power consumption. So, instead of computing average power consumption for many traces, the device's power model is produced that is correlated with the actual power consumption of the device using Pearson correlation. More detailed info about CPA can be read from the research paper titled, "Correlation Power Analysis with a Leakage Model.

Electromagnetic (EM) Attacks

These attacks exploit the electromagnetic emissions from the device during operation. Performing this attack needs an electromagnetic measurement probe. It's suitable even for higher frequency signals. As discussed before, under the power analysis attack, the devices have integrated circuits; within the integrated circuits, there are transistors; the flow of current within them creates the electromagnetic field. Thus, as the power is leaked during operation, similarly, there are electromagnetic leakages. The measurement and analysis of these signals give the attacker the possibility to extract the secret information/keys. Similar to power analysis, SPA and DPA can be performed on electromagnetic traces. EM-based SCA is preferred in most cases because it does not require any manipulation in the circuit by inserting a shunt resistor as in the power analysis. Though in terms of tools, it gets expensive. However, more research is being done to develop efficient and low cost soultions to perform EM-based SCA. The research paper titled, "SCNIFFER: Low-Cost, Automated, Efficient Electromagnetic Side-Channel Sniffing" proposes a low-cost platform for this purpose. A few more research links are provided at the end of this blog under the "Reference Section".

Timing Attacks

In certain implementations of the device operation, the execution timing is dependent on the data inputs based on the different execution paths. The attacker exploits this execution timing difference to either guess or extracts the sensitive data. The research paper on "Timing Attacks on Implementations of Diffie-Hellman,RSA,DSS,and OtherSystems" by Paul C.Kocher shows the timing attacks that have been done on the cryptographic implementations to extract the secret key.

Cache Attacks

In this attack, the attacker exploits the information leaked during the cache access because the cache hit takes comparatively less time w.r.t cache miss. Sometimes, it is used with the timing attacks to determine the cache memory access timing. Though the accessed data cannot be seen, the attackers can extract the

information by knowing the memory area being accessed. Meltdown and Spectre is one of the most severe types of cache and timing-based side channel attacks on the Intel hardware that leaked the memory contents of the process and the operating system as well.

Differential Fault Attacks

These attacks involve extracting the keys/sensitive information by generating faults in the system. They can also exploit the fact that the device could be prone to faults due to higher design complexity and incomplete verification. Faults could be created by varying the voltage, clock glitching, etc. More on fault attacks would be discussed in our next blog. In this attack, the operation is performed, one with fault and the other without fault, both are then analyzed and compared to identify the operation corresponding to the fault.

Acoustic Attacks

These attacks exploit the sound produced during the computation to extract the secret information. More on it can be read in the research paper titled, "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis"

Why side channel attacks are so alarming

There is a lot of effort and investment being made to make the critical system secure, especially hardware security. It is now more focused on implementing hardware-based encryption. Ranging from the implementation of secure hardware based cryptographic devices using Trusted Platform Modules (TPM), implementing secure boot, etc., a lot of work is being done to ensure the system security by securing the hardware along with the software. Attacks like SCA make it challenging towards the secure development of these devices. Varying products like our personal computers, smart cards, etc use these cryptographic devices, but the flaw in its implementation can open opportunities for SCA attacks.
SCA is also used to target deep neural network models. More about it can be read in the paper titled, "Open DNN Box by Power Side-Channel Attack". Though on critical devices, like smart cards, proper countermeasures might be implemented, but SCA has become more dangerous for IoT devices, as these devices have resource constraints. Protection against these SCA attacks is neglected mostly on the IoT devices. In these devices, low power processors are used for running crypto operations in order to save energy. Running unprotected crypto operations on generic processors makes it easier for the attacker to perform these attacks. As these attacks are more at the CPU level, they can put critical infrastructure and devices at significant risk that software patching cannot solve. With the increase in sophisticated tools and methods, these attacks have become more reachable. Read more about its impact on cryptographic modules by YongBin Zhou, DengGuo Feng.

Possible countermeasures for side channel attacks

Though it is practically difficult to eliminate these SCA attacks, they can be made harder to achieve. A few countermeasures could be taken to make it harder for the attacker to perform these attacks. * On the hardware side, the use of physically unclonable functions (PUFs) and proper shielding from leaking electromagnetic radiation should be preferred.
* On the implementation side, the device's operation should be independent of data, i.e., the number of clock cycles should be either uniform or randomized to avoid operation timing leakages. * Error detection should be implemented to identify if any faults occur in the circuit. * The keys should not be reused on different products. * The power consumption in the device should be independent of operating

instructions. One of the techniques used is to use the differential signals, where power spikes are not seen, or by masking or adding noise such that transition from 1 to 0 or 0 to 1 cannot be leaked. * Secure programming pattern should be adopted as mentioned in the white paper by Riscure * After the development, the device must go through tests against SCA attacks. Some resources for performing these tests include, "A testing methodology for SCA, written by Gilbert Goodwill, et al.", "Welch's T-testin Side-Channel Security Evaluations"

Various other research works are done and ongoing to implement more effective countermeasures against SCA attacks for their mitigation.

Conclusion

In this blog, we went through a basic overview of side channel attacks and its types. We hope this gives you an overall understanding of it and the related severity of such attacks. Stay tuned for our future blogs where we will be showing the implementation side of respective SCA attacks.

Continue to the next part - IoT Security - Part 20 (101 - Introduction to Fault Injection Attack (FI))

References

- https://en.wikipedia.org/wiki/Side-channel_attack
- https://www.newae.com/embedded-security-101
- http://gauss.ececs.uc.edu/Courses/c653/lectures/SideC/intro.pdf
- https://www.rambus.com/blogs/side-channel-attack-targets-deep-neural-networks-dnns/
- https://whisperlab.org/introduction-to-hacking/talks/chipwhisperer
- https://troopers.de/downloads/troopers19/TROOPERS19_NGI_RT_Hardware_Side_Channels.pdf
- https://jochen-hoenicke.de/crypto/trezor-power-analysis/
- https://www.riscure.com/uploads/2018/04/Riscure_CheapSCAte_RSA.pdf
- https://paulkocher.com/doc/DifferentialPowerAnalysis.pdf
- https://www.iacr.org/archive/ches2004/31560016/31560016.pdf
- https://www.tandfonline.com/doi/pdf/10.1080/23742917.2016.1231523?needAccess=true
- https://eprint.iacr.org/2014/204.pdf
- https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9201569
- https://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1822&context=theses
- https://www.esat.kuleuven.be/cosic/publications/thesis-182.pdf
- https://csrc.nist.gov/CSRC/media/Events/Non-Invasive-Attack-Testing-Workshop/documents/03_deBeer.pdf
- Hardware Security: Design, Threats, and Safeguards Book by Debdeep Mukhopadhyay and Rajat Subhra Chakraborty

About Payatu

Payatu is a research-powered cybersecurity service and training organization specialized in IoT, embedded, mobile, cloud, infrastructure security and advanced security training. We offer a full IoT/IIoT ecosystem security assessment, including hardware, firmware, middleware and application interfaces. If you are looking for security testing services then let's talk, share your requirements:

https://payatu.com/#getstarted. Payatu is at the front line of IoT security research, with a great team, and in house tools like expliot.io. In the last 8+ years, Payatu has performed, security assessment of 100+ IoT/IIoT product ecosystems and we understand the IoT ecosystem inside out. Get in touch with us. Click on the get started button below.