Jonathan Lu
UWP 101V
14 May 2024

Annotated Bibliography

Word Count: 1347

Topic: Side Channel Attacks (SCAs)

Research Question: How are side channel attacks done, and what can be done to mitigate/prevent them?

Hertz, Jake (2022). Understanding Side Channel Attack Basics. *All About Circuits*. Retrieved from https://www.allaboutcircuits.com/technical-articles/understanding-side-channel-attack-basics/

Hertz writes this technical article to give a brief introduction on Side Channel Attacks. Side Channel attacks at a high level are a security attack on hardware that aims to gather information through cryptographic encryption. Cryptographic encryption is an algorithm that aims to send messages while keeping track of three things: confidentiality, integrity, and authenticity. Hardware can leak information through unexpected ways, and SCAs take advantage of this. Some SCAs use power consumption, EM radiation, and execution time. In the case of a power side channel attack, the power consumption of a device is measured, then information and patterns can be interpreted. SCAs are powerful because computers must use power, emit EM waves, or take time. These traits cannot be removed, so the best a programmer can do is obscure them.

The author, Jake Hertz is a technical writer and electrical engineer with 5 years of experience. He links a few other blog posts that he uses as references. His experience, as well as the usage of other sources makes this post credible. Most of the information that he uses are things that I can make sense of, and fit within the context that I know of as well.

This article alone is just a high level description of power side channel attacks, and so this article is not that helpful. It also does not offer any details about mitigation strategies. What this article does offer is some links to research articles/other blogs that offer more in depth information. From this source, I can use the high level descriptions for my own understanding.

Ha, G., Chen, H., Jia, C., & Li, M. (2023). Threat Model and Defense Scheme for Side-Channel Attacks in Client-Side Deduplication. *Tsinghua Science and Technology*, 28(1), 1–12. **https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9837022**

This article explains an SCA threat model on something known as client side deduplication for cloud storage. As cloud computing gets larger, servers need to save

space by making sure that data from a user is only saved once. To do this, cryptographic hashes are used, but this process of sending the hash is vulnerable to SCAs. The threat model is that since anyone can send information to store on the cloud, an attacker can manipulate what they send and use the deduplication responses to determine if packets exist on the cloud. The basic idea of the defense of such an attack is to use XOR to obscure some of the deduplication responses. The article then continues to do math heavy analysis on performance and proof of why the defense scheme works.

This is an academic research article, written by researchers from Nankai University, China. The supervisor has a PhD in Computer Security, and the other writers are pursuing a PhD. Their research is heavily related to cloud computing and computer security. Their status as researchers makes this somewhat credible, but there is not much other prior experience that I found.

The schemes mentioned in this paper are very interesting and helpful, because it introduces an interesting type of side channel attack, as well as an in depth explanation for how to defend against this type of side channel attack. However, this is a software based side channel attack, and I am slightly more interested in the hardware form, and how to defend against those. What I can use from this article is that it reveals how broad of a topic SCAs can be. The description of such an attack is useful as well.

Randolph, M., & Diehl, W. (2020). Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman. *Cryptography*, 4(2), 15-. https://doi.org/10.3390/cryptography4020015

This article aims to give an analysis and review of a Power SCA. The paper covers the basics of a power side channel attack, from the reasons why it is exploitable, the math that proves how it works, and a few different types of power attacks. The purpose of cryptography is to keep things secret. Power SCAs are able to be exploited because computers use power, and the power contains information about the secrets. So an attacker can read the power consumption of a computer, and steal information. The paper describes simple power SCA and differential power SCA. The details and math are too high level and complex for this summary. The paper offers some countermeasures. Then, the paper describes correlation power attacks and mutual information analysis.

The author Mark Randolph is a PhD Electrical engineering student at Virginia Tech. Being a notable individual with some academic articles and citations, he is a trustworthy source for this topic. The details of this paper also match the much more simple blog posts that cover this topic.

The paper offers incredible detail on how a power side channel attack works. It directly helps answer the research question for this type of side channel attack, explaining the math, and statistics behind how they work. It offers a comprehensive overview of this topic, with a useful amount of lower level details. It also mentions a few ways to defend against power SCAs. In my blog, this can be used to describe power SCAs, which are the

most broadly known, and mitigation strategies. Overall, the details of this paper are very informative, and the author is credible. This makes this source one of the strongest sources that I have.

Van Cleemput, J., De Sutter, B., & De Bosschere, K. (2020). Adaptive Compiler Strategies for Mitigating Timing Side Channel Attacks. ***IEEE Transactions on Dependable and Secure Computing*****, 17(1), 35–49. https://doi.org/10.1109/TDSC.2017.2729549**

This article describes how a software compiler can mitigate timing channel attacks. Time based side channel attacks use the execution time of a program to extract information: for a cryptographic algorithm, the timing may reveal information about encrypted messages. One strategy that can be used to mitigate this is to use compilers. Some places that cause time variance in the hardware are control hazards and data hazards. If conversion can reduce the variance by making the shorter cases longer. Branch prediction can also make the timing consistent. Modern systems may have variable time for different arithmetic operations, leading to different secrets having different timings. Techniques to mitigate this are to introduce a lot more static timing operations, either replacing the variable ones entirely or overwhelming it. All this reveals that timing issues can be prevented by using techniques to fix execution time. The balance is then with doing this while not adding too much overhead. The article then introduces a lot of low level, detailed schemes to mitigate this type of attack for a few select encryption algorithms, which will not be mentioned in this summary.

The authors are members of IEEE, which is a professional association that defines a few key standardizations for computer science. All three authors are also professors at Ghent university, and conduct research there. Their experience and standings make them credible as authors. The paper's level of detail and in depth explanations also make sense and make it credible as well.

This is a different type of side channel attack compared to ones mentioned in previous articles, and thus this paper is very helpful as it allows me to place more side channel attacks into my writing. This paper also goes very in depth with mitigation strategies, which is the important part. This lets me put more types of SCAs into my blog, and some mitigation strategies.

Taheritajar, A., & Rahaeimehr, R. (2024). Acoustic Side Channel Attack on Keyboards Based on Typing Patterns. ***arXiv*****. https://doi.org/10.48550/arxiv.2403.08740**

This paper introduces an acoustic side channel attack that uses keyboard typing sounds to determine what is being typed. This strategy is solely based on using someone's typing, making this very powerful when successful. By using external recording devices unknown to a user, their keystroke sounds can be recorded. Typing patterns are nearly impossible to change, so the best way to mitigate this is to prevent any sound from leaking at all (also impossible). Machine learning and statistics can correlate sound to different keyboard presses, words, and phrases. Techniques using typing patterns are particularly strong, because they must map to English words (most of the time). In

addition, multiple techniques can be done with an audio file, which can cross validate each other. Previous methods reveal that each key press has different sounds. Adding typing style increases the effectiveness of the attack greatly. The article then introduces their research, where they develop a model that does exactly this, and predicts the words being inputted. Their success rate was about 43%; while weak, this was done in an environment where there were a lot of additional sounds to typing. Adding additional sound side channel attacks can improve this as well.

The authors of this article are PhD students at Augusta University. Their status as students and researchers makes this article relatively credible; their previous research is limited however, so they are not as well established. However, the paper is very in depth and makes their work credible.

This is yet another different type of side channel attack. This reveals the important aspect of how varying side channel attacks can be, and especially now how some attacks may be unpreventable entirely. What this article reveals is how a dedicated attacker can use all sorts of means to gather information, and how broad their strategies can be. While this article does not offer too much information on mitigation strategies, I can develop my own.