Side Channel Attacks:

Even in a Crypto-Ideal World is Data Truly Secure?

JN Matthews

13 December 2017

Abstract

Side channel attacks are ones that use analysis of observable side-effects of a system's physical behaviors to crack them, rather than by using cryptanalysis or brute force. For example, in the cloud a target's cache access patterns can be monitored, and locally an attacker could monitor power consumption or the electromagnetic leakage of the target machine. This paper will investigate how these attacks are being used, both in terms of the methods that attackers are currently using to exploit side channel analysis and the typical targets of such attacks, as well as the techniques that can be deployed as countermeasures. The paper will also seek to address the societal implications of such attacks; who has the resources to perform them, and what does that mean for information security and privacy?

1 Introduction

As long as people have had the technology to build and design safes and ciphers to secure important information and valuables, others have been looking for ways to circumvent those securities; be it by learning the construction details of a lock and listening to the audio cues of their mechanisms or investigating a person of interest and using knowledge of them to make educated assumptions about their pass-phrases. Although side channel techniques are likely as old as security itself,

analogues to modern side channel attacks date back to the 1940's. During WWII secure typewriter communications were developed by Bell Telephone for military use. "When one of these mixers was being tested in a Bell laboratory, a researcher noticed, quite by accident, that each time the machine stepped, a spike appeared on an oscilloscope in a distant part of the lab. After he examined these spikes more carefully, he found that he could read the plain text of the message being enciphered by the machine!" [1] Later in 1951 it was discovered by the CIA that plain-text could be recovered with this phenomena a quarter mile away. Related techniques were used for espionage by both sides during the cold war. It wouldn't be until 1985, when the Dutch scientist Wim van Eck published his paper demonstrating that computer monitor emissions could be picked up and displayed to a TV in a neighboring building [2], that knowledge of such eavesdropping would be available outside of military circles. [3]

2 To the Community

We like to think of computers as black boxes whose only access points are the terminal prompt, monitor, or the network ports. However, computers are made of transistors and physical wires that produce high frequency electro-magnetic fields, and consume electric power. At a low level everything our computers do are a sequence of operations run in the processor; the convolution of that sequence with the data it is operating on produces unique electro-magnetic emissions. If someone can observe these signals along with knowledge of what the computer is doing at the corresponding time, they may be able to use that information to reverse-engineer what the data being operated on was. Not only can this allow someone to recover what a monitor is displaying, but more concerningly they may be able to recover passwords and cryptographic keys as they are being used.

In our modern digital world we rely on cryptographic algorithms that (hopefully)

have been proven to be mathematically sound. But even in Impagliazzo's ideal Cryptomania world [4] where public key cryptography is mathematically secure, the security of our information is only as good as the implementations of these algorithms. If the essential key to an algorithm can be recovered from side channel analysis on a computer, the algorithm's difficulty to brute force is irrelevant to an attacker who has the capabilities or opportunities to observe a machines behavior.

The foreseeable future looks to be filled with progressively more devices connected to networks, especially as we look at automation trends like those in cars, IoT, and smart housing. So far the current corporate model prioritizes profit, time-to-market, and performance over cyber-security concern, let alone the information leakage that could be used for a side channel attack. And these corporate attitudes aren't likely to change of their own volition. Declassified in the early 2000s, there exists a NSA specification and NATO certification TEMPEST, which details the emissions shielding requirements for systems handling classified data. [1, 3] It seems reasonable that we should learn from these techniques and develop similar standardization for public use.

3 The Current State of Affairs

In general, side channel attacks is analysis of observable emissions and side-effects of a machine and knowledge of it's internal flow of control to reverse engineer the data processed. As described previously these emissions could be electro-magnetic signals or power-consumption, but they can also be acoustic or the cache access pattern on a shared system. Abstractly, countermeasures tend to fall into two camps: (a) shielding emissions such that they are only discernible within a very short range, and (b) masking emissions with additional noise such that the leaked signals are indistinguishable from white noise. However, these techniques are not always enough, and due to the broad scope of the topic we will use a few case studies

to seek to to answer the following questions about these attacks: How are they preformed? What is vulnerable? Who can preform them? and What mitigations can we invoke?

3.1 Keystroke Logging with Mobile Phone Accelerometers

A team of researchers at Georgia Institute of Technology showed in 2011 that the accelerometer in an iPhone 4 could "record and reconstruct the keypresses made on a nearby keyboard based solely on the observed vibrations."[5] They used a trained neural net to compare features to a dictionary, and found that about 80% of the time the correct word was among the reconstructor's top 5 matches. "It is apparent that an attacker could easily recover a dangerous amount of text, ... simply by knowing some context for the target's writing."[5] The resources required to be able to launch such an attack are minimal. However, the fact that the attackers phone had to be within about a foot of the target implies that this would be a targeted attack, and is not likely to scale well. Despite this a possible mitigation would be to not type sensitive information in public spaces.

3.2 Cache Monitoring on Cloud Computing

Cloud computing has become extremely common, since it allows businesses to make shared use of expensive data center physical resources and allows for scaling flexibility. Thees "cloud computers" are generaly modeled as many virtual machines on a shared physical system. The authors, Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage, have demonstrated that with relatively limited money they were able to map out large sections of Amazon's Elastic Compute Cloud (EC2) physical compute infrastructure and could use this knowledge to "place their malicious VM on the same physical machine as that of a target customer."[6] They then showed that once they had this VM in place they could preform cache-monitoring attacks, such as cross-VM keystroke monitoring. These preliminary findings point to

the feasibility of side-channel attacks in cloud-computing environments." Certainly this sort of attack does not cost more than buying cloud compute time. In addition, it difficult for the cloud hosting service (in this case EC2) to determine if a VMs behavior is malicious, which limits the mitigation techniques that can be applied. What they can do, on the other hand, it to make it more difficult to reliably place a malicious VM adjacent to the target.

3.3 Cryptographic Insecurities

One of the most dangerous implications of side channel analysis is it's use against cryptography. Unfortunately mathematics doesn't consider the time or power it takes for a CPU to perform an addition vs. a multiplication. In the last couple decades we've seen a slew of exploits for cryptographic algorithms: AES [7], DES [8], RSA [9, 10], Elliptic Curve Cryptography [11, 12], etc. It been clearly shown that many implementations of these algorithms are vulnerable to side channel attacks, and in our push to encourage the use of cryptography everywhere we should also strive to use implementations that don't have these flaws and publicly document those with vulnerabilities.

4 Conclusion

Certainly side channel attacks all have some element of locality, be it physical, like with the acoustic keystroke logger, or virtual, ie. adjacent VMs, which means that such attacks tends to be more targeted than the mass distribution of malware. This makes it less likely for one individual to be a victim of a random attacker.

On the other hand we should consider the capabilities of such attacks in the hands of organizations with more resources. The NSA's declassification of their defensive project TEMPEST and information on related potential attacks, both that information which is public and that which can be gleaned from the context of what has

been redacted, suggests that they have the capabilities to take advantage of these attacks — possibly by using large orbiting antennae.

In our current world where trivial security risks, like SQL and command injections, are still common place, we're probably not going to convince both software and hardware designers to prioritize the lack of information leakage over marketing concerns. And perhaps we should not worry about it at the expense of working to fix the simple problems.

However, despite this, it is important to not delude ourselves into the illusion good cryptography algorithms are enough. Implementation matters and our machines are not Turing Machines where every step is externally indistinguishable. Our security is only as strong as its weakest link. Perhaps side channel attacks are not our biggest threats now, but we cannot ignore their future risk. We are moving into a world where cheap hardware, firmware, and software, will become even more ubiquitous. Given the likelihood of even more smart homes and the further digitization of cars, it is not difficult to imagine that the side channel attacks being found today will become the techniques of car theft and breaking and entering of tomorrow. We have trouble enough with attribution in "ordinary" cyber-security, and given the passive nature of side channel attacks, which are often impossible to detect having happened and don't tend leave traces, this will only become exaggerated.

References

[1] Jeffrey Friedman. Tempest: A signal problem. *NSA Cryptologic Spectrum*, 35:76, 1972.

[2] Wim Van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4):269–286, 1985.

[3] Ryan Singel. Declassified nsa document reveals the secret history of tempest. *Wired Magazine*, 29, 2008.

[4] Russell Impagliazzo. A personal view of average-case complexity. In *Structure in Complexity Theory Conference, 1995., Proceedings of Tenth Annual IEEE*, pages 134–147. IEEE, 1995.

[5] Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (sp) iphone: Decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 551–562. ACM, 2011.

[6] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *Proceedings of the 16th ACM conference on Computer and communications security*, pages 199–212. ACM, 2009.

[7] Daniel J Bernstein. Cache-timing attacks on aes, 2005.

[8] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in cryptology—CRYPTO'99*, pages 789–789. Springer, 1999.

[9] Werner Schindler. A timing attack against rsa with the chinese remainder theorem. In *CHES*, volume 1965, pages 109–124. Springer, 2000.

[10] Roman Novak. Spa-based adaptive chosen-ciphertext attack on rsa implementation. In *Public Key Cryptography*, pages 252–262. Springer, 2002.

[11] Elisabeth Oswald. Enhancing simple power-analysis attacks on elliptic curve cryptosystems. In *CHES*, volume 2002, pages 82–97. Springer, 2002.

[12] Louis Goubin. A refined power-analysis attack on elliptic curve cryptosystems. In *Public Key Cryptography*, volume 2567, pages 199–210. Springer, 2003.

[13] Shuo Chen, Rui Wang, XiaoFeng Wang, and Kehuan Zhang. Side-channel leaks in web applications: A reality today, a challenge tomorrow. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 191–206. IEEE, 2010.

[14] Ilya Kizhvatov. *Physical Security of Cryptographic Algorithm Implementations*. PhD thesis, University of Luxembourg, Luxembourg, Luxembourg, 2011.

[15] Plore. Def con 24 - plore - side channel attacks on high security electronic safe locks. `https://www.youtube.com/watch?v=lXFpCV646E0`, 2016.