InfoSecIITR: CSAW ESC'23 Quals Submission

Gyanendra Kumar Banjare, Manas Ghandat, Abhishek Kumar Singh, Priyansh Rathi and Rahul Thakur
Indian Institute of Technology, Roorkee
Roorkee, India

Email: gyanendrabanjare8@gmail.com, manasghandat7099@gmail.com, abhishekkrsingh05kr@gmail.com, techiepriyansh@gmail.com, rahul.thakur@cs.iitr.ac.in

***Abstract*—In Cyber Physical Systems due to the integration of many aspects like communication, computation, etc., and their manifest in terms of physical aspect, they remain vulnerable to various information leaks which can be used as a vector to perform side-channel attacks on the device. This report aims to provide a comprehensive summary and analysis of the various side-channel attacks in cyber physical systems and their defenses.**

I. Introduction

Cyber Physical Systems (CPS) are physical devices (or groups of devices) that integrate computation, cyber systems, and interactions with physical entities via sensors and actuators operating in a feedback loop. Examples of CPS are autonomous driving vehicles, implantable medical devices, and building control systems.

The advancement of technology in these systems introduces new security vulnerabilities that are being exploited by adversaries as seen in [12] due to desynchronized clocks, Dragonfly attacks against power grids [8] and even medical implants are susceptible to severe risks [7]. In this report, we will focus on a specific category of attacks known as side-channel attacks.

II. Side Channel Attacks

A side-channel attack is any attack based on the physical implementation of a system which is performed via channels that are produced as a result of the fundamental way in which the system is implemented. This can be achieved by measuring or analyzing various physical parameters like timing information, power consumption, electromagnetic leaks and sound.

Side-channel attacks are difficult to detect as neither they do not leave any trace on the system while it's running nor do they alter it. In the case of cyber physical systems, it is even tougher to detect the attacks due to the various aspects involved like communication, physical implementation, etc. Side channel attacks are differentiated based on the vulnerable observable parameter:

1. **Power Analysis Attacks:** In the case of power-based attacks we monitor the power consumption of the device. The minute variation in power can reveal information about the device like code flow path.
2. **Timing Attacks:** Timing attacks exploit variations in the time it takes for a system to perform specific operations. By measuring these time differences, attackers can infer information about the system's behavior and leak data as well.
3. **Electromagnetic Attacks:** Electromagnetic attacks capture the various electromagnetic radiation or radio waves, given off by a target device to reconstruct the internal signals of that device.
4. **Acoustic Attacks:** Acoustic side-channel attacks use sound and vibrations to reveal critical information about the output of the device like the design that is being printed by a 3D printer.

This report will majorly focus on the following side-channel attacks: 1) Acoustic attacks, 2) Power analysis attacks and 3) Timing attacks.

III. Attacks

In order to execute side-channel attacks, we assume that we have access to the vulnerable device on which we want to perform the attack or we can remotely measure the concerned physical parameters like sound, electromagnetic radiations and timing measurements of the device. Also, we assume that we are able to minimize the associated noise generated while capturing data either by:

1. **Gathering data with low noise:** For example, acoustic attacks are based on the noise that is emitted by the device. Hence the attacker tries to ensure that the environment of the device is quiet i.e. there is very little background noise.
2. **Using error correction techniques:** We can use error correction techniques to compensate for the generated noise to provide better results. For example, in timing attacks, we can make a good guess of the k^{th} bit of the secret key statistically if we know the first $k-1$ bits using *T-test* based on the concept of confidence intervals [2].

Also, in order to successfully execute the attack there must be another similar machine on which various machine learning models can be trained and analysis can be carried out.

A. *Acoustic Attacks*

Acoustic cryptanalysis is a type of side-channel attack that exploits sounds emitted by computers, computer keyboards, internal computer components or other devices. The domain of acoustic attacks is mainly constrained to stealing critical information that might not be available to the user.

To get started with the attack we first need to identify a reliable source of sound from which we can extract the required information about the state of the machine. In the case of cyber physical systems, there are various sources of sound like motors. Also, in this case, a problem that arises is we need to filter out different sounds which might be environmental or other sounds emitted by the device. We can use machine learning algorithms to filter out the sounds.

In the case of a 3D printer[3] we can use the two hybrid stepper motors which are the primary sources of sound. Using the current that is input to the system and the moment of inertia of the system we can write its equation of motion. We can write the equation of analogous emission as follows:

$$O = f_d(G) + N$$

Where $f_d(G)$ represents a deterministic leakage function dependent on the G-code (language that humans use to tell a machine how to do something) that an attacker may model. N represents a random variable denoting noise independent from f_d. From the G-code, it is possible to reconstruct the original input with an accuracy of 92.54%.

Also in the report [4] they have discussed extending the above attack to the case of fully-automated DNA synthesizers. Using the techniques aforementioned they were able to replicate the DNA strand with 88.07% accuracy.

B. *Power Consumption Attacks*

A power analysis attack is a form of side-channel attack that includes analyzing the power consumption of a cryptographic hardware device. These attacks rely on the basic physical properties of semiconductor devices that is the change in voltage leads to a change in current. Data-related details can be derived by assessing the current.

As we increasingly rely on hardware acceleration to improve the performance and energy efficiency of computing systems, Field Programmable Gate Arrays (FPGAs) have recently been widely adopted in large-scale data centers. This report shows that these integrated FPGAs introduce a new security vulnerability that can be exploited to perform power side-channel attacks in software, without requiring physical access or proximity to the target system. There are two major types of Power Analysis 1) Simple Power Analysis [10] and 2) Differential Power Analysis [6].

Simple Power Analysis (SPA) involves interpreting power traces or visual examination of graphs of the current used by

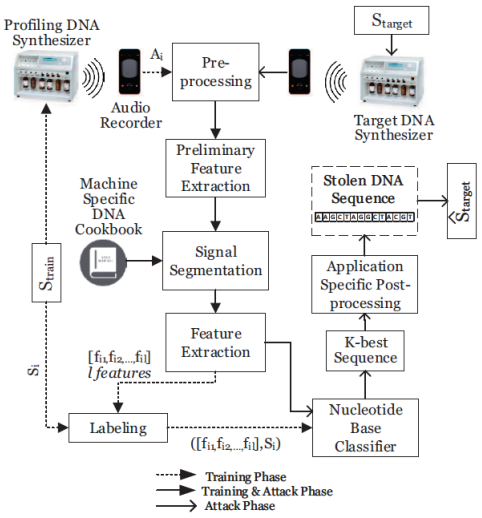

Fig. 1: Side Channel Attack in DNA Synthesizer machine in order to capture the DNA strand [4]

the device over time. Variation in power consumption occurs as the microprocessor executes different instructions. Similarly, squaring and multiplication operations in RSA implementations can often be distinguished, enabling an adversary to compute the secret key[11]. Even if the magnitude of the variations in power consumption is small, standard digital oscilloscopes can easily show the data-induced variations.

In the square-and-multiply circuit, if the current bit of the exponent is 1, then both multipliers will be performing sequences of additions, resulting in high switching activity in the flip flops and look up tables that store and compute the multiplied intermediate results. However, if the exponent bit is 0, then only the squaring multiplier's logic will switch, while the other multiplier's logic will be idle. Thus, we expect that the power consumption will be different between an iteration with an exponent bit of 1 and an iteration with an exponent bit of 0. As a result, the RSA crypto module is vulnerable to a Simple Power Analysis (SPA) attack.

C. *Timing Attacks*

Timing Attacks exploit the inherent computational as well as communication time associated with the different physical components of a cyber physical system operating in non-constant time. Timing attacks can be used to extract sensitive information like private keys by analysis of precisely measured computation times as described in [5]. CPS uses control commands based on inputs from sensors measuring physical parameters and transmits them to the actuators that alter the system state accordingly. It is also possible to disrupt the functioning of CPS via delaying the control commands [9] known as a time delay attack.

Bruteforcing the secret key is possible if the implementation of the algorithm compares two values sequentially, byte-by-byte (or bit-by-bit), and stops as soon as it encounters an unequal byte (or bit). If the first $n-1$ bytes are equal then the time measured will be greater when the n^{th} byte is equal as compared to when it is unequal. Thus given $n-1$ equal bytes we can brute force the n^{th} byte. The 1^{st} byte is brute forced, then the 2^{nd} byte and so on until the complete key is found.

Cryptographic algorithms like RSA, Diffie-Hellman, etc. uses modular exponentiation algorithm which computes

$$R \Leftarrow y^x \pmod{n}$$

where n is the public key, y is a known value (either plain-text or public key) and x is the secret key which is w bits long.

Algorithm 1 Modular Exponentiation

Input: y, $x = (b_{w-1}, b_{w-2}...b_1, b_0)_2$, n
Output: $y^x \pmod{n}$

$R \leftarrow 1$
for i = 0 upto $w-1$ **do**
  $R \leftarrow R^2 \pmod{n}$
  if b_i = 1 **then**
    $R \leftarrow R \cdot y \pmod{n}$
  end if
end for
return R

The operation $R \leftarrow R \cdot y \pmod{n}$ is only computed when the bit is equal to 1, which introduces additional computational time and can be used to determine the n^{th} bit of x when $n-1$ bits are known by analyzing the time difference between successive iterations. The x can be found starting with the 1^{st} bit and then sequentially finding the next bit till the entire x is known.

IV. Defenses

A. Acoustic Attacks

The major downside of acoustic attacks is the proximity they require with the vulnerable device. The suitable range of these attacks is about 10 cm from the device and the accuracy drops significantly as the distance increases. In the case of side-channel attacks on printers[1] it was discovered that on increasing the distance to 2 meters the accuracy decreases from 62% to 4%. In case there is any barrier between the recording device and the target device, then the accuracy can drop down to 0%.

Acoustic shielding is another way in which we can decrease the accuracy. Adding a layer of acoustic foam or other sound muffling device decreases the operable range in which we can perform the attack.

B. Power Analysis Attacks

Cryptosystem engineers must ensure that devices' power variations do not reveal information usable by adversaries. Simple power analysis can easily distinguish the outcome of conditional branches and other expensive operations such as modular exponentiation. One of the approaches would be to tweak the algorithm a bit so that modular exponentiation is safer as stated in *Algorithm 2*.

Algorithm 2 SPA safe modular exponentiation

Input: m, $d = (d_0, d_1..., d_{n-1})$ odd, N , k
Output: ($m^{d-1} \pmod{k \cdot N}$, $m^d \pmod{k \cdot N}$)

$a_0 \leftarrow m$
$a_1 \leftarrow a_0^2 \pmod{k \cdot N}$
for $i = n-1$ to 1 **do**
  $a_{\bar{d_i}} \leftarrow a_{\bar{d_i}} \cdot a_{d_i} \pmod{k \cdot N}$
  $a_{d_i} \leftarrow a_{d_i}^2 \pmod{k \cdot N}$
end for
$a_{d_1} \leftarrow a_{d_1} \cdot a_{d_0} \pmod{k \cdot N}$
$a_{d_0} \leftarrow a_{d_0}^2 \pmod{k \cdot N}$
if (Loop Counter i not disturbed) & (Exponent d not disturbed) **then**
  return (a_0,a_1)
else
  return "A fault attack has been detected."
end if

C. Timing Attacks

In industrial CPS like power grids, if the clock among nodes is desynchronized, we can use a clock synchronization approach as described in [12] based on voltage signal's cycle length fluctuations to encode fine-grained global time information. We can also use deep learning models using stacked bidirectional long short-term memory (LSTM) [9] to predict possible delays and handle them accordingly.

When comparing two values, use a hashing algorithm like SHA-256 to hash the input and compare its hash with the original value's hash instead of byte-by-byte comparison.

For modular exponentiation and similar algorithms, choose a random integer z that is invertible $\pmod{q}$ where q is multiple in order of y and then do the following as stated in *Algorithm 3*.

Algorithm 3

Input: y, $x = (b_{w-1}, b_{w-2}...b_1, b_0)_2$, n , q , z
Output: $y^x \pmod{n}$

$x' \leftarrow x \cdot z \pmod{q}$
$y \leftarrow y^{x'} \pmod{n}$
$R \leftarrow y^{z^{-1} \pmod{q}} \pmod{n}$
return R

In step 1, we multiply x with z, and in step 3, we nullify step 1 by using $z^{-1} \pmod{q}$ and the result of modular exponentiation in step 2 is unaffected. After the timing attack, the attacker would find x' and since x' is obtained through multiplying z and x, there is no way to recover x as z is randomly chosen and is unknown to the attacker.

V. Conclusion

In general, CPS can leak information owing to their hardware implementation even if they are cryptographically secure. Therefore, additional hardware and software safeguards must be implemented to protect against potential information leaks.

The report concisely discussed the various side-channel attacks on Cyber Physical Systems and defenses against them. It outlined the methodologies of SCAs focusing on Acoustic Attacks, Power Analysis Attacks and Timing Attacks.

References

[1] Michael Backes et al. "Acoustic {Side-Channel} attacks on printers". In: *19th USENIX Security Symposium (USENIX Security 10)*. 2010. URL: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Backes.pdf.

[2] Cai-Sen CHEN, Tao Wang, and Jun-Jian Tian. *An Improved Timing Attack with Error Detection on RSA-CRT*. Cryptology ePrint Archive, Paper 2010/054. https://eprint.iacr.org/2010/054. 2010. URL: https://eprint.iacr.org/2010/054.

[3] Sujit Rokka Chhetri, Arquimedes Canedo, and Mohammad Abdullah Al Faruque. "Confidentiality Breach Through Acoustic Side-Channel in Cyber-Physical Additive Manufacturing Systems". In: *ACM Trans. Cyber-Phys. Syst.* 2.1 (2017). DOI: 10.1145/3078622. URL: https://doi.org/10.1145/3078622.

[4] Sina Faezi et al. "Acoustic Side Channel Attack Against DNA Synthesis Machines: Poster Abstract". In: *2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS)*. 2020, pp. 186–187. DOI: 10.1109/ICCPS48487.2020.00026. URL: https://ieeexplore.ieee.org/document/9095984.

[5] Paul C. Kocher. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems". In: *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*. Vol. 1109. Lecture Notes in Computer Science. Springer, 1996, pp. 104–113. DOI: 10.1007/3-540-68697-5_9. URL: https://www.iacr.org/cryptodb/data/paper.php?pubkey=1469.

[6] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. "Differential Power Analysis". In: *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*. Vol. 1666. Lecture Notes in Computer Science. Springer, 1999, pp. 388–397. DOI: 10.1007/3-540-48405-1_25. URL: https://www.iacr.org/cryptodb/data/paper.php?pubkey=1471.

[7] Ana Longras, Henrique Oliveira, and Sara Paiva. "Security Vulnerabilities on Implantable Medical Devices". In: *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. 2020, pp. 1–4. DOI: 10.23919/CISTI49556.2020.9141043. URL: https://ieeexplore.ieee.org/document/9141043.

[8] Xin Lou et al. "Assessing and Mitigating Impact of Time Delay Attack: Case Studies for Power Grid Controls". In: *IEEE Journal on Selected Areas in Communications* 38.1 (2020), pp. 141–155. DOI: 10.1109/JSAC.2019.2951982. URL: https://ieeexplore.ieee.org/document/8892729.

[9] Xin Lou et al. "Learning-Based Time Delay Attack Characterization for Cyber-Physical Systems". In: *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. 2019, pp. 1–6. DOI: 10.1109/SmartGridComm.2019.8909732. URL: https://ieeexplore.ieee.org/document/8909732.

[10] Stefan Mangard. "A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion". In: *Information Security and Cryptology — ICISC 2002*. Ed. by Pil Joong Lee and Chae Hoon Lim. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 343–358. ISBN: 978-3-540-36552-5. URL: https://link.springer.com/chapter/10.1007/3-540-36552-4_24.

[11] Roman Novak. "SPA-based adaptive chosen-ciphertext attack on RSA implementation". In: *International Workshop on Public Key Cryptography*. 2002, pp. 252–262. URL: https://e6.ijs.si/~novak/papers/PKC2002.pdf.

[12] Sreejaya Viswanathan, Rui Tan, and David K. Y. Yau. "Exploiting Power Grid for Accurate and Secure Clock Synchronization in Industrial IoT". In: *2016 IEEE Real-Time Systems Symposium (RTSS)*. 2016, pp. 146–156. DOI: 10.1109/RTSS.2016.023. URL: https://ieeexplore.ieee.org/document/7809851.