CSAW ESC 2023 Qualification Report

Team: IIT-Madras

Arun Krishna AMS
Dept. of Electrical Engineering
IIT-Madras
Chennai, India
ee19b001@smail.iitm.ac.in

Antonson J
Dept. of Electrical Engineering
IIT-Madras
Chennai, India
ee19b025@smail.iitm.ac.in

Surya Prasad S
Dept. of Electrical Engineering
IIT-Madras
Chennai, India
ee19b025@smail.iitm.ac.in

Niranjan A Kartha
Dept. of Electrical Engineering
IIT-Madras
Chennai, India
ee19b025@smail.iitm.ac.in

Chester Rebeiro
Dept. of Computer Science & Engineering
IIT-Madras
Chennai, India
chester@cse.iitm.ac.in

***Abstract*—In the context of cyber-physical systems (CPS), the evolving landscape of security threats has prompted extensive research and countermeasure development. This paper investigates three prominent side-channel attack vectors targeting CPS: timing attacks, fault injection attacks, and power side channel attacks. A side-channel attack exploits additional information that can be acquired due to the implementation of a computer protocol or algorithm, rather than relying on inherent flaws in the protocol or algorithm's design.**

Each of these threats exploit distinct vulnerabilities within CPS, presenting unique challenges for mitigation. This paper explores the intricacies of these attacks, their potential consequences, and highlights current countermeasures.

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

In an increasingly interconnected world, cyber-physical systems (CPS) serve as the linchpin of critical infrastructure, orchestrating the seamless fusion of digital control and physical processes. These systems underpin vital sectors such as energy, healthcare, transportation, and manufacturing. Yet, this increased interconnectivity and reliance on CPS also expose them to an array of sophisticated side channel attacks.

These attacks exploit unintended information leakage channels—such as timing, power consumption, and fault responses—to compromise the confidentiality, integrity, and availability of these systems. We delve into the mechanisms, risks, and countermeasures associated with these threats, highlighting the pressing need for robust security in safeguarding the integrity and reliability of CPS.

II. Timing Attacks

Timing attacks are a family of attacks that exploit the information leakage through the time it takes for a system to respond to a given input. For example, the duration it takes for an algorithm to encrypt a specific message can inadvertently disclose information about the cryptographic key in use. If an attacker possesses a means to accurately measure these time intervals, they may exploit this information to gain unauthorized access to sensitive data

As an illustrative example, consider the following C code snippet that verifies a password:

```
// password and password_len are defined elsewhere
bool verify_password(const char* str, int len) {
    if (len != password_len)
        return false;
    for (int i = 0; i < len; i++)
        if (str[i] != password[i])
            return false;
    return true;
}
```

In the above function, the time it takes to return a result varies depending on the similarity of the input to the actual password. More character matches between the input and the password results in longer execution times. If this function is used without addressing this timing aspect, an attacker could potentially reconstruct the password through an iterative process, exploiting these timing differences.

For another example, consider the following "trivial" implementation of the fast modular exponential algorithm, commonly employed in cryptographic schemes like RSA:

```
def expmod(a, b, m): # computes a^b mod m
  out = 1
  while b > 0:
        if b & 1 == 1:
            out = (out * a) % m
        a = (a * a) % m
        b >>= 1
  return out
```

In RSA, private keys are used as exponents in such operations, with 'b' representing confidential information. Notably, the execution time of this algorithm is influenced

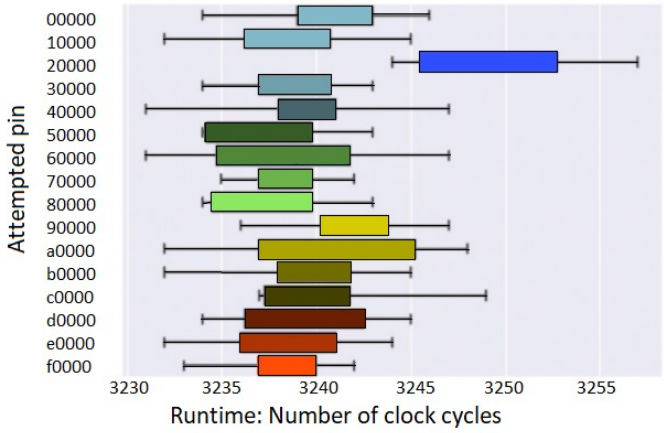

Fig. 1. an illustration of how inputs that are more similar to the password may result in a longer execution time if a poorly implemented verification function is used

by the number of '1's in the binary representation of 'b'. Consequently, an attacker can exploit timing variations to infer information about 'b' and potentially deduce the entire key [1]. Indeed, even sophisticated implementations of RSA have been demonstrated to be susceptible to remote timing attacks [2].

To mitigate timing attacks, one approach is to introduce random delays into functions. A more robust strategy involves ensuring that all possible branches of a function consume a consistent amount of time to compute. This practice is known as constant-time programming and should be employed whenever a function handles sensitive information.

III. Power Side Channel Attacks

Power side channel attacks pose a significant threat to the security of embedded systems, cryptographic devices, and hardware implementations. These attacks exploit variations in a device's power consumption to glean information about its inner workings, potentially revealing critical secrets such as cryptographic keys.

A. Simple Power Analysis (SPA)

Simple Power Analysis (SPA) represents a basic form of power side channel attack involving the observation of power traces. SPA aims to map specific operation types to power consumption patterns to extract information.

Consider the fast modular exponential algorithm used in RSA:

```
def expmod(a, b, m): # computes a^b mod m
out = 1
while b > 0:
        if b & 1 == 1:
            out = (out * a) % m
        a = (a * a) % m
        b >>= 1
return out
```

The device's power consumption during the multiplication operation may exhibit a distinct trace on an oscilloscope compared to other operations, enabling the inference of whether the i'th bit in the secret key corresponds to 0 or 1.

B. Differential Power Analysis (DPA)

While relatively simple systems perform a single operation at a time, more complex systems are usually performing several operations at once. Trying to infer statistical patterns of a single operation is extremely difficult. To improve the chances of success, Differential Power Analysis (DPA) analyzes and correlates the power traces obtained from multiple runs of the same operation with different inputs, to statistically infer the secret key.

DPA typically involves the following steps:

- **Power trace capturing:** An attacker captures a set of power traces (power consumption measurements) while the target device processes different inputs.
- **Hypothesis:** The attacker hypothesizes potential values of the secret key.
- **Analysis on non-linear operations:** The attacker calculates intermediate values within the cryptographic algorithm based on the hypothesized key. DPA targets non-linear operations, such as S-box operations
- **Correlation:** The attacker statistically correlates the power traces with the hypothesized intermediate values to determine the likelihood of a correct key guess. The correct key guess's intermediate values are expected to exhibit the highest correlation with power, while those from incorrect guesses show lower correlation.
- **Key Recovery:** By accumulating evidence and repeating the process for various key guesses, the attacker eventually recovers the secret key.

Equivalent to power traces, leaked electromagnetic radiation emanating from chipsets can also be used to infer cryptographic secrets.

C. Countermeasures

*1) **Threshold**:* Threshold countermeasures against side channel attacks aim to sever the connection between input data, secret keys, and any intermediate results that might leak information

Threshold implementation divides the input variables into multiple shares with each share containing partial information, but none of them reveal the entire secret. Every function/computation is independent of at least one share of each of the input variables. (Non Completeness).

Random masking values are applied to input shares to prevent consistent patterns that can be exploited. (Randomness). Finally, techniques are used to combine output shares to yield the desired output (Correctness).

This process results in output shares that are uncorrelated with the input variables, preventing the leakage of information

about the input [3].

*2) **Desynchronization of traces**:* Random delays or operations added in the execution will introduce desynchronization when collecting traces, thereby increasing the complexity of mounting a side channel attack.

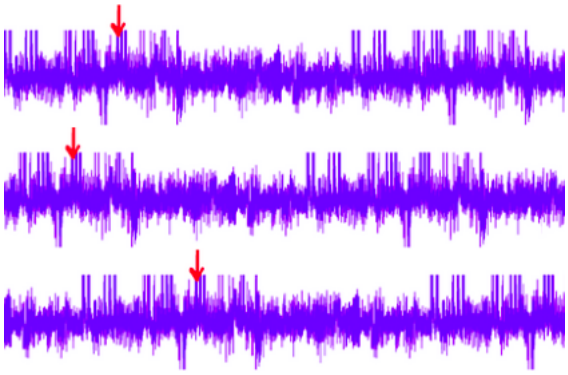

Fig. 2. Random delay addition to desynchronize traces

Microprocessors designed specifically with increased resistance to power side channel attacks can also be used in cyber-physical systems [4]. These countermeasures collectively bolster the security of systems against power side channel attacks.

IV. Fault Injection Attacks

Fault Injection attacks aim to compromise the integrity and security of a target system by intentionally inducing errors or faults in its operation by stimulating the device beyond its operating conditions.

Typically, fault injection attacks involve introducing controlled disturbances or perturbations into the target system, in the form of voltage glitching, clock glitching, laser fault injection and electromagnetic fault injection. The objective is to induce unexpected behavior and utilize sophisticated mathematical analysis to bypass secure boot, extract the secret key, disrupt a program counter or to manipulate the behavior of firmware in the system.

Consider the following C code snippet that executes a firmware image if the image is authenticated:

```
// authenticate the firmware image
auth_check = authenticate(image)

// if authentication is valid, then execute the
    image
if (auth_check) {
    execute_firmware(&image)
}
```

By inducing a voltage glitch at the precise time, a fault can be induced to skip the authentication check, thereby allowing an unauthenticated firmware to be executed.

Similarly, let us look at how Differential Fault Analysis could be performed to attack RSA. By injecting fault, a bit is flipped in the private key, d, at position i.

$$M = S^d mod N$$

$$M' = S^{d'} mod N$$

$$\text{If } d_i = 0, \text{ then } \frac{M'}{M} = S^{2^i} mod N$$

$$\text{Else, } \frac{M'}{M} = \frac{1}{S^{2^i}} mod N$$

By analysing the effect of the fault, we can identify both i and d_i.

A. Countermeasures

1) **Redundancy based countermeasures**: Critical operations are executed repeatedly or in multiple hardware resources. These calculations are checked for self-consistency, and if the system detects any inconsistency then, it can be safely assumed fault has been injected.
2) **Information redundancy measures**: Adding additional information checkers and predictors to catch faults. For example, adding a parity checker and parity predictor can help identify and rectify errors introduced by fault injection.
3) **Hardware hardening and Tamper detection**: Hardware-based countermeasures, such as tamper-evident packaging, shielded components, or physically unclonable functions (PUFs)[5], can make it more challenging for attackers to access and manipulate hardware components. Brownout detection circuitry and Clock monitors can be used to detect voltage and clock glitching. Phase locked loops can also be used to detect EM fault injection[6].

While redundancy based countermeasures provide the best security due to difficulty in creating multiple identical faults, it is vulnerable to attacks at comparison step. Information redundancy measures, on the other hand, fails to provide 100% fault coverage.

V. Conclusion

In this report, we presented an overview of prevailing side-channel attack vectors that pose significant threats to the security of cyber-physical systems (CPS). The proposed mitigations and countermeasures have demonstrated a noteworthy capacity to decrease the probability of successful attacks but at a trade-off between enhanced security and increased latency, elevated economic costs, and potential reductions in performance efficiency.

As novel attack vectors emerge, ongoing research and development efforts are essential to remain ahead of potential threats. This includes not only improving existing defenses but also exploring techniques that reduce the tradeoff between security and system performance.

ACKNOWLEDGMENT

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks . . .”. Instead, try “R. B. G. thanks. . .”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

REFERENCES

Please number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use “Ref. [3]” or “reference [3]” except at the beginning of a sentence: “Reference [3] was the first . . .”

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors’ names; do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should be cited as “unpublished” [4]. Papers that have been accepted for publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, “Title of paper if known,” unpublished.

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.