Brief Report
Volume 15:5, 2022

Journal of Computer Science & Systems Biology

ISSN: 0974-7230 Open Access

A Comprehensive Examination of Fault Injection Attacks on IOT Network

John Hausman*

Department of Information Science, University of Melbourne, Australia

About the Study

As IoT systems become more widely used in fields such as healthcare, smart homes, and autonomous vehicles, their security becomes increasingly important. Despite the fact that the attack surface for such systems is vast, significant work has been done to categorise, analyze, and counter them. Fault injection attacks (FIA) inject faults into the hardware devices of an IoT system, causing the software to behave abnormally. The attacker takes advantage of this abnormal behaviour for a variety of reasons, including obtaining personal information, disrupting programme [1-3] flow to circumvent critical security safeguards, and illegal system access and control. Faults introduced into hardware components can be transient or persistent, remaining in the system and exploiting it repeatedly.

These are active attacks that take place while the system is in use. Fault injection attacks differ from other IoT system attacks in that they span multiple layers of the system. The attack is carried out at the physical layer on the hardware devices of the IoT system, affecting the operation of software components and programmes on other layers of the system. Device drivers, the operating system, and application software are examples of software that can be affected. For example, the authors of investigated how fault injection attacks on cryptographic devices are carried out in order to trick the encryption algorithm into using a zero-encryption key. The attacker can then decrypt and steal sensitive data using a zero key.

Future Perspective

These types of attacks are extremely dangerous to safety-critical IoT devices. Because these attacks begin at the physical layer and affect software at multiple layers of the IoT architecture, the methods proposed in the literature to counter fault injection attacks range from attack detection using system-level physical and network properties to software vulnerability analysis to mitigate the effects of such attacks. Frameworks proposed in detect fault injection attacks by monitoring the electromagnetic field around the IoT system or by using physical system properties such as voltage, temperature, and clock frequency. These frameworks analyse data using various methods such as formal analysis, machine learning, and deep learning to detect or predict attacks. The authors proposed a framework in which a separate sensor board [4,5] comprised of various digital sensors was used to continuously monitor the properties of the IoT system and an AI core was used to predict any abnormal events. On the other hand, studies like looked for flaws in IoT software that could be exploited by fault injection attacks.

The goal of software vulnerability analysis techniques is to test IoT software and identify exploitable vulnerabilities by replicating actual fault injection attacks on the IoT system or simulating the attacks directly on the IoT software. The authors proposed combining simulation-based software vulnerability detection with hardware-level verification of the discovered flaws. While attack detection methods have limitations, such as the need for a separate physical hardware setup to monitor system-level properties, simulation-based software vulnerability analysis techniques are not always capable of completely protecting against all system-level threats due to fault injection attacks. This paper presents a systematic literature review (SLR) of various frameworks proposed to combat fault injection attacks on IoT systems. The following are the main contributions of the paper: analysis of primary studies that propose frameworks to counter fault injection attacks on IoT systems using attack detection and software vulnerability analysis identifies limitations and research gaps for each category.

To address the limitations and improve the security of IoT systems against fault injection attacks, we propose hybrid attack detection methods at the software level that combine concepts from both categories, such as the use of software fault injection, machine learning, and code instrumentation tools. Fault injection attacks inject flaws into an IoT system's hardware and devices with the intent of changing the software's behaviour. These attacks on IoT software call into question the widely held belief that hardware flaws have no bearing on IoT software performance. These attacks can be carried out by introducing flaws into various hardware components, such as the external clock generator, voltage source, and I/O devices connected to the IoT system. Fault injection techniques, which include clock glitch, voltage glitch, electromagnetic field injection, and optical injection, among many others, are used to carry out such attacks. Because integrated circuits latch data and control signals at the rising or falling edge of the clock, clock glitches cause propagation delays in the logic blocks, causing the IoT system software to function abnormally for a short period of time and produce an unexpected output. EMFI and optical attacks use electromagnetic fields and light, respectively, to inject faults into the system. Such methods may inject transient glitches or long-lasting faults, such as changes to the memory region.

Conflict of Interest

None.

Acknowledgement

None.

References

1. Qasem, Abdullah, Paria Shirani and Mourad Debbabi. "Automatic vulnerability detection in embedded devices and firmware: survey and layered taxonomies." *ACM Comput Surv* (CSUR) 54 (2021): 1-42.
2. Lou, Xiaoxuan, Tianwei Zhang and Jun Jiang. "A survey of microarchitectural side-channel vulnerabilities, attacks, and defenses in cryptography." *ACM Comput Surv* (CSUR) 54 (2021): 1-37.
3. Potestad-Ordóñez, Francisco Eugenio, Erica Tena-Sánchez and Antonio José Acosta-Jiménez, et al. "Hardware Countermeasures Benchmarking against Fault Attacks." *Appl Sci* 12 (2022): 2443.

***Address for Correspondence:** John Hausman, Department of Information Science, University of Melbourne, Australia, E mail: jhausman@wc.edu*

Date of Submission: 07-May-2022, Manuscript No. jcsb-22-68090; **Editor assigned:** 09-May-2022, Pre QC No. P-68090; **Reviewed:** 23-May-2022, QC No. Q-68090; **Revised:** 28-May-2022, Manuscript No. R-68090; **Published:** 02-Jun-2022, DOI: 10.37421/0974-7230.2022.15.414

4. Shah, Imdad Ali, Samina Rajper and Noor ZamanJhanjhi. "Using ML and data-mining techniques in automatic vulnerability software discovery." *Int J* 10 (2021).

5. Kitchenham, Barbara, O. Pearl Brereton and David Budgen. "Systematic literature reviews in software engineering–a systematic literature review." *Inf Softw Technol* 51 (2009): 7-15

How to cite this article: Hausman, John. "A Comprehensive Examination of Fault Injection Attacks on IOT Network." J Comput Sci Syst Biol 15 (2022):414.