IGS | YOUR DIGITAL TRANSFORMATION PARTNER

Part 2

HARDWARE CYBERSECURITY ATTACKS

Think you know cybersecurity? Think again.

Exploring the Taxonomy of Hardware Attacks

Goals Of A Hardware Attack

- Steal - an attacker wants to take possession of sensitive information or resources.
- Corrupting - an attacker modifies data or functionality for their advantage
- Inhibiting - an attacker prevents proper access or use of a service or data.

The Attack Domain

- Logical Domain - Attacks exploiting vulnerabilities in software layers running on top of hardware.
- Physical Domain - Attacks directly performed on the hardware device itself.

The Attack Types

- Microprobing Attacks
- Reverse Engineering
- Data Remanence Attacks
- Side-Channel Attacks
- Fault Attacks
- Test-Infrastructure-Based Attacks

The Attack Methods

- Invasive Attacks

Physical intrusions involving actions like desoldering or disconnection of internal components.

- Non-Invasive Attacks

Passive - Analyzing and measuring physical entities of the attacked hardware
Active - Forcing the hardware into abnormal states to achieve the attacker's goal

STAY AHEAD OF THE GAME; FORTIFY BEFORE FIGHT!

With an endpoint and workload security solution; we can help you secure endpoints, servers, and cloud workloads.

We can aid you secure your critical corporate workloads without the hassle to set up or managing your security infrastructure.

We can help ensure sustained development by integrating security technologies into your existing DevOps procedures.

We'll help you explore enhanced and linked detection, investigation, and response across security levels.

Fortify your business with us today!

References;
1. Prinetto and Roascio, Hardware Security, Vulnerabilities, and Attacks: A Comprehensive Taxonomy (2020)