Low-Energy Chip to Prevent Side Channel Attacks

For Prelims: Side Channel Attacks, Internet of Things.

For Mains: IT & Computers Significance of Low Energy Chip in Countering Side Channel Attacks.

Why in News

Recently, two Indian researchers have built a **low-energy security chip** that is designed to prevent **Side-Channel Attacks (SCAs) on** IoT (Internet of Things) **devices**.

- IoT is a computing concept **that describes the idea of everyday physical objects being connected to the internet** and being able to identify themselves to other devices.
- It is being used to **create smart infrastructure in various verticals** such as Power, Automotive, Safety & Surveillance, Remote Health Management, Agriculture, Smart Homes and Smart Cities etc, using connected devices.

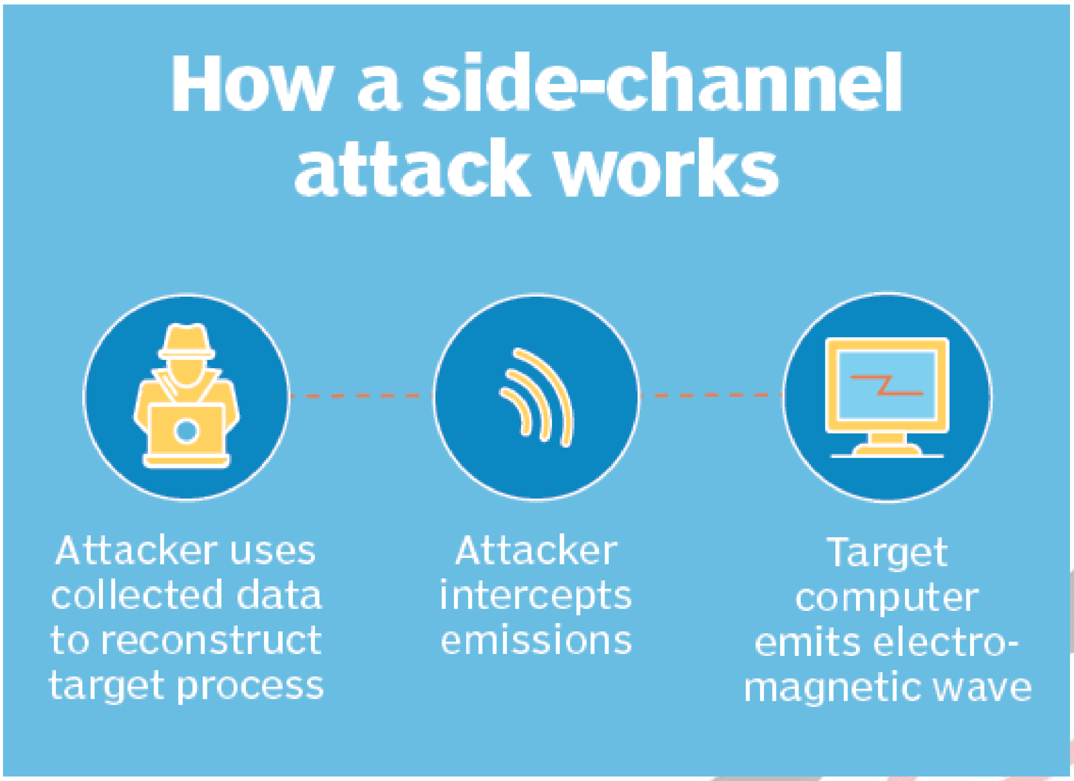
What is a Security Chip?

- Security Chip means the **application specific integrated circuit** that **instantiates the Security Feature** after being embedded in the device.

What is SCA?

- A SCA is **a security exploit that aims to gather information** from or influence the program execution of a system by **measuring or exploiting indirect effects of the system or its hardware** -- rather than targeting the program or its code directly.
- Typically, SCAs aim to **extract sensitive information like cryptographic keys, proprietary machine learning models and parameters** by measuring things like timing information, power consumption and electromagnetic leaks of a system.
    - An SCA **may also be referred to as a sidebar attack** or an implementation attack.
    - It can be applied to any data that you want to keep secret.
        - **For example,** it can be used on your smartwatch to extract your ECG and heart rate signal,”
    - **Types of SCAs**: Timing attack, Electromagnetic (EM) attack, Acoustic, Power, Optical, memory Cache, hardware weaknesses.
- Even though SCAs are difficult to execute on most modern systems, the increasing sophistication of machine learning algorithms, greater computing power of devices and measuring devices with increasing sensitivities are making SCAs more of a reality.

//


How a side-channel attack works
Attacker uses collected data to reconstruct target process
Attacker intercepts emissions
Target computer emits electro-magnetic wave

What is the Significance of New Architecture?

- **Uses Much Less Power:**
  - Since SCAs are difficult to detect and defend against, countermeasures against them have notoriously been very computing power and energy-intensive. This is where the new chip architecture comes in.
  - The **chip is smaller than the size of a thumbnail and uses much less power than traditional security measures against SCAs.**
- **Easily be Incorporated:**
  - It has been built to be **easily incorporated into smartwatches, tablets, and a variety of other devices.**
  - It can be used in any sensor node which connects user data. For example, **it can be used in monitoring sensors in the oil and gas industry,** it can be used in self-driving cars, in fingerprint matching devices and many other applications.
- **Near-Threshold Computing help reveal nothing:**
  - The chip uses near-threshold computing, **a computing method where the data to be worked on is first split into separate, unique and random components.** The chip then conducts operations separately on each component in a random order before aggregating the results for a final result.
  - Due to this method, the **information leak from the device through power-consumption measurements are random and would reveal nothing but gibberish in an SCA.**
    - However, this method is energy and computation power-intensive while also requiring more system memory to store information.

What are the Issues?

- The implementation of this chip architecture in a system would require **at least a five-fold increase in energy consumption** 1.6 times the silicon area of an insecure implementation.
- Also, the architecture **only protects against energy consumption-based SCAs** and doesn’t defend against electromagnetic SCAs.

PYQ

When the alarm of your smartphone rings in the morning, you wake up and tap it to stop the alarm which causes your geyser to be switched on automatically. The smart mirror in your bathroom shows the day’s weather and also indicates the level of water in your overhead tank. After you take some groceries from your refrigerator for making breakfast, it recognises the shortage of stock in it and places an order for the supply of fresh grocery items. When you step out of your house and lock the door, all lights, fans, geysers and AC machines get switched off automatically. On your way to office, your car warns you about traffic congestion ahead and suggests an alternative route, and if you are late for a meeting, it sends a message to your office accordingly. (2018)

In the context of emerging communication technologies, which one of the following terms best applies to the above scenario?

(a) Border Gateway Protocol
(b) Internet of Things
(c) Internet Protocol
(d) Virtual Private Network

Ans: (b)

Source:IE

PDF Refernece URL: https://www.drishtiias.com/printpdf/low-energy-chip-to-prevent-side-channel-attacks