How hardware design choices can make the life of attackers difficult in IOT Security

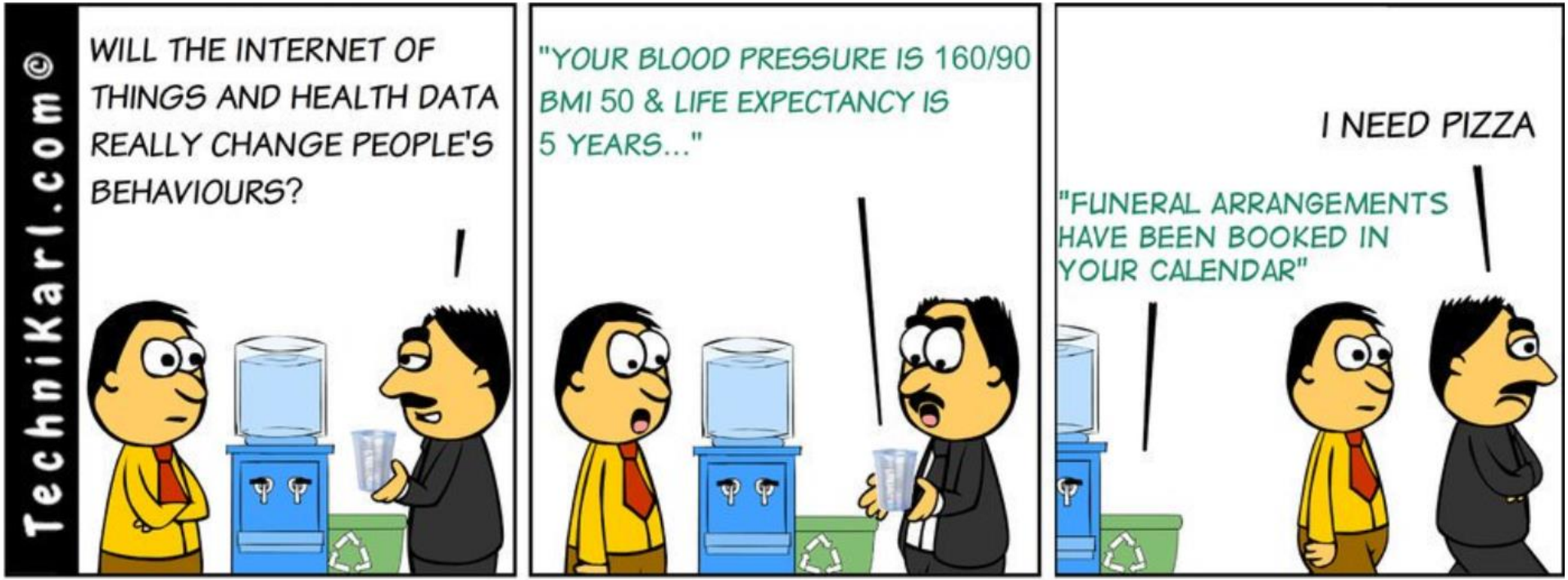
IOT

IoT Edge Node & Building blocks

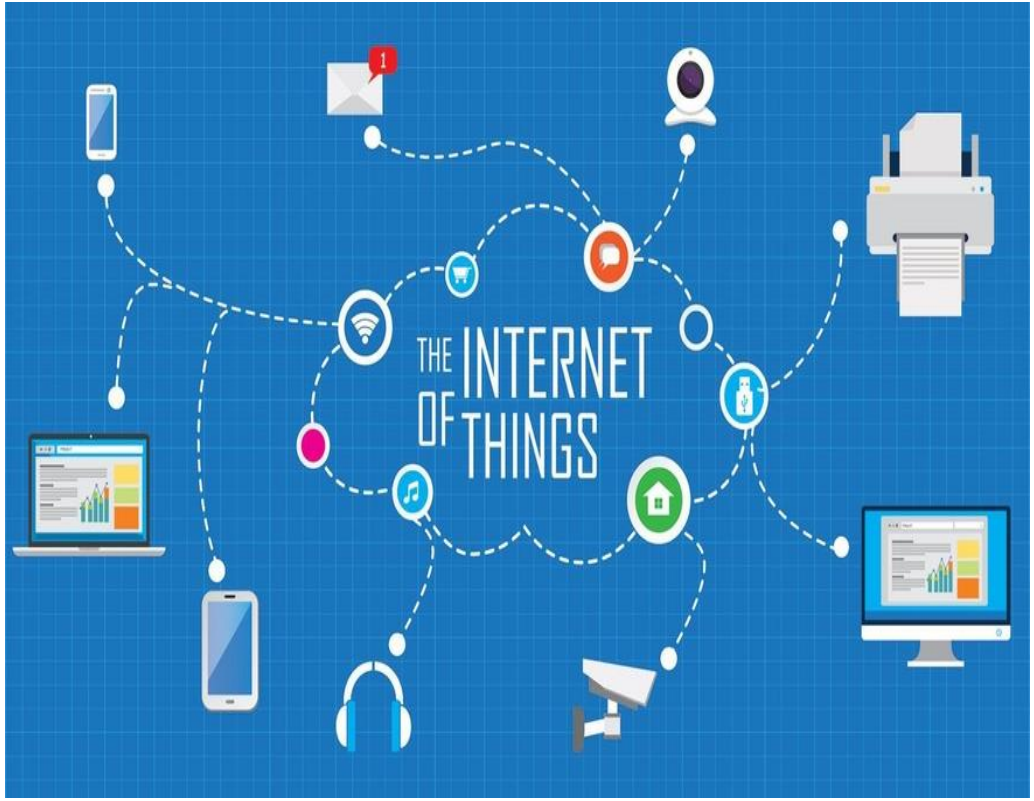
Examples of IoT Hacking

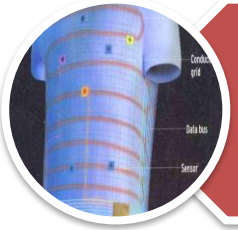
Chip level Attacks: An overview

Hardware Solutions



IOT





Shirt with super powers can tell you when you're ill

The kettle that the boiled water is cooling and you should hurry up and make that cup of tea before it gets too cold.

Your Kids toothbrush lets you know that they have brushed their teeth for two minutes, that they have cavity?

A network of Internet connected objects with Unique Identifiers and unique data

Creativity is limitless in IoT

There are 3.04 trillion trees in the world

Assume you can interact with them and connect to them

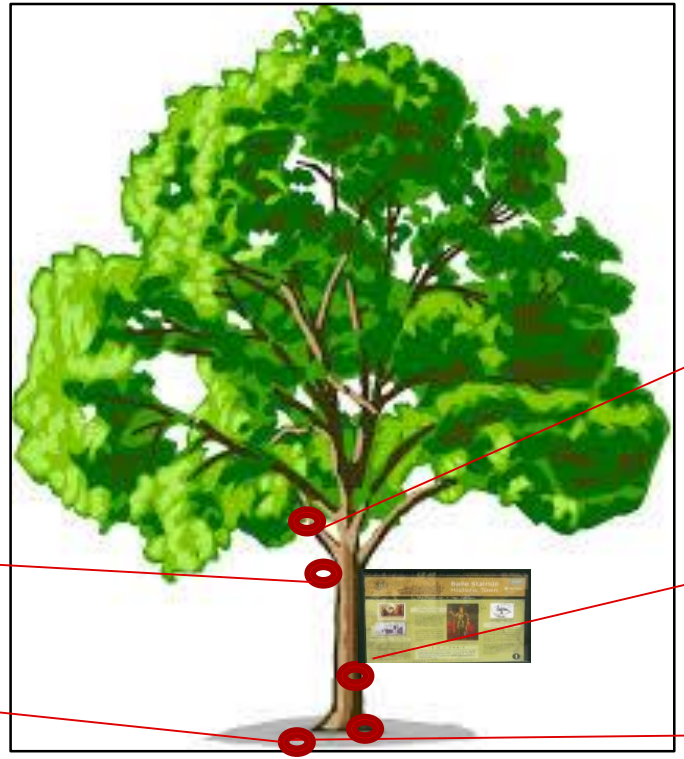


Image Sensors, Proximity Sensor, Pedestrian count, Auto FB tags with User enabled control

Solar enabled smart lighting

Digital map info, navigation, Traffic alerts

Environment and Seismic Sensors

Water level detector

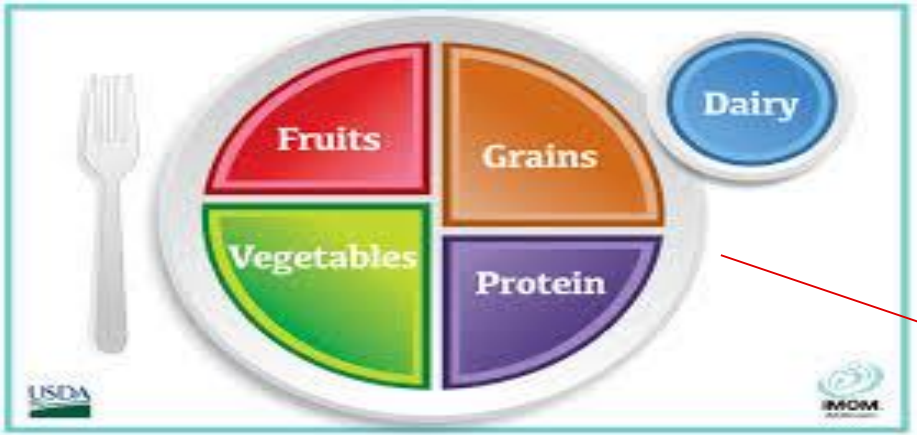
IoT – when applied on "things" – that are naturally around us – leads to innovations and opportunities

Creativity is limitless in IoT

There are 7 billion people in the world.

~0.2 billion people are DIET CONSCIOUS

CREATE "SMART PLATES"

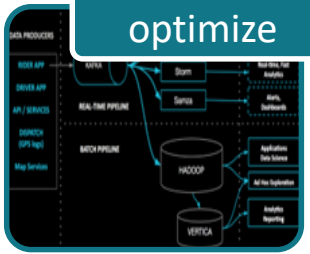


Weighs, warns, analyzes based on health, Customizes based on people

IoT – when applied on "things" – that are needed by us in day to day life – leads to innovations and opportunities

Monetizing IoT

Connect Things



Data Gather optimize

Drive Services

Interconnect Services

Uber

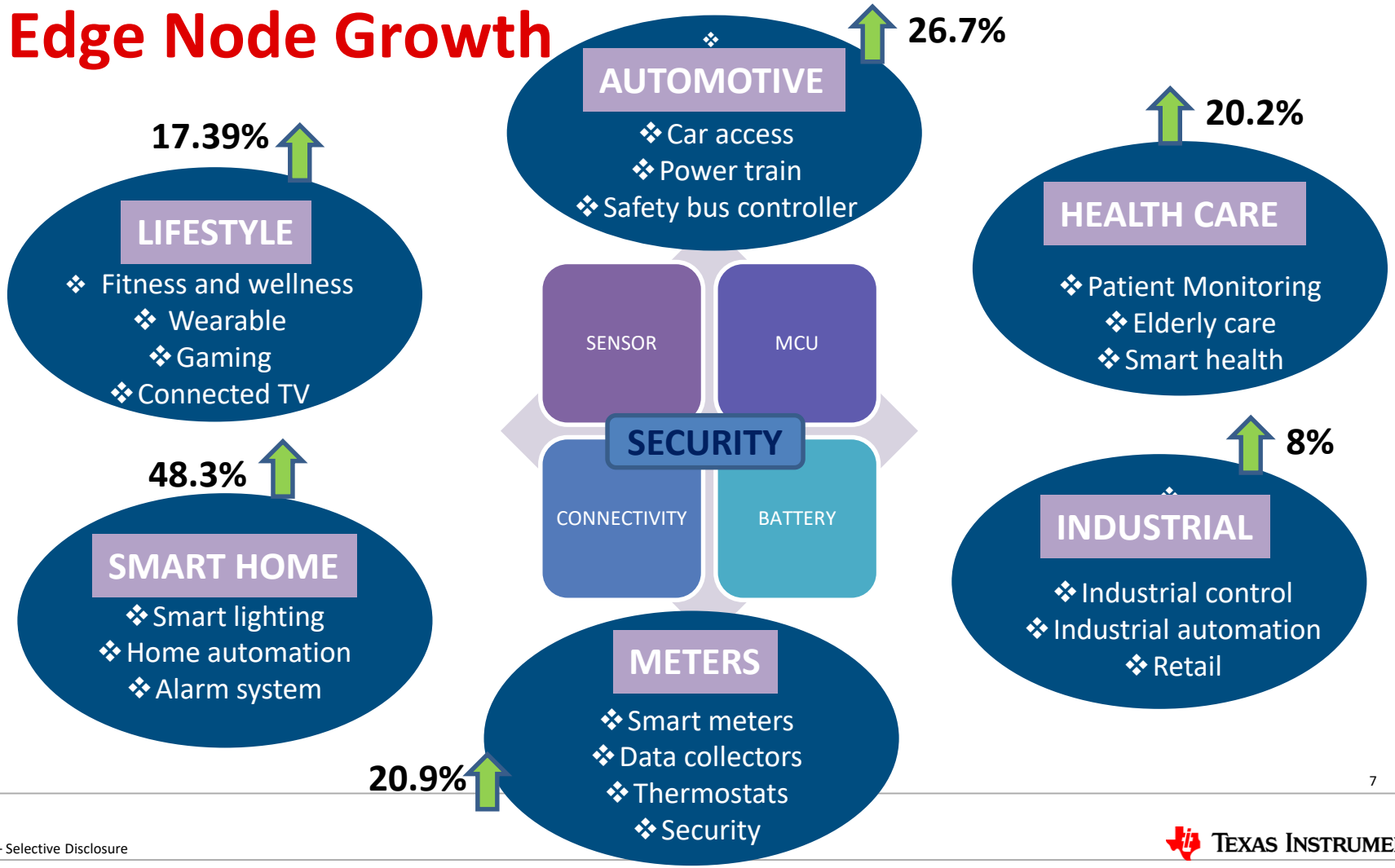
Uber Eats

Uber Health

UberCHOPPER
Powered by Helistar Aviation

IoT service can be MONETIZED via a strong ecosystem of interconnect services

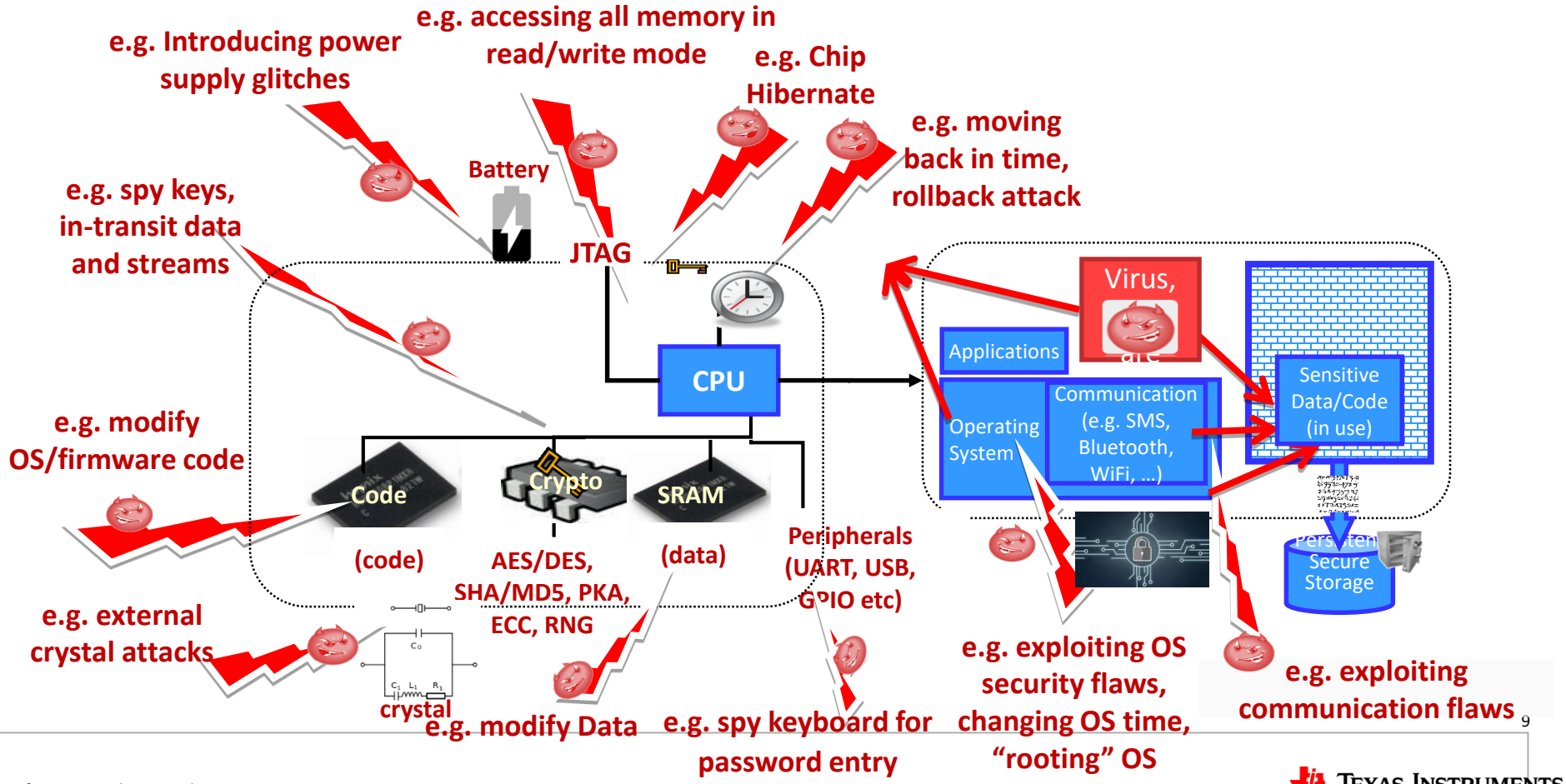
IoT Edge Node Growth



Examples of IoT Hacking

- ***Hacker remotely raises home temperature by 12 degree Celsius on smart thermostat => Demand ransom money to release the control of thermostat***
- ***The Hackable Cardiac Devices from St. Jude => Life threatening for a patient***
- ***The Owlet WiFi Baby Heart Monitor Vulnerabilities => Misleading information leading to incorrect diagnosis***
- ***The TRENDnet Webcam Hack => Leak private information***

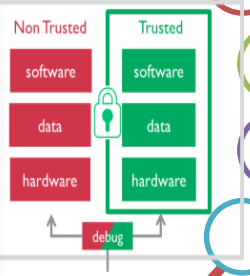
Chip level Attacks : An overview



Hardware design solutions for security

REGION BASED MEMORY PROTECTION

ROLL BACK ATTACK PROTECTION



FIRMWARE ATTACK PROTECTION

SECURITY & PERFORMANCE

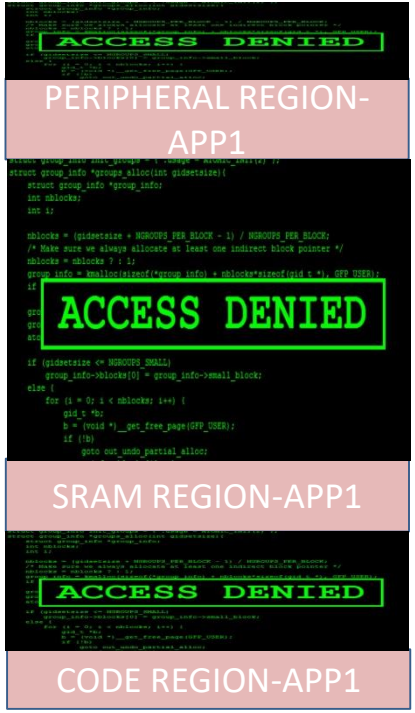
TAMPER DETECTION

TAMPER PROTECTION

- Code Protection
- Peripheral Protection
- Data Protection
- Debug Protection
- Secure Hash Algorithm(SHA-256), True Random number generator (RNG)
- Elliptic curve digital signature Algorithm (ECDSA)
- Public Key Authentication (PKA), Crypto accelerators
- Battery backup for Chip Hibernate modes
- On chip Clock Monitor with Battery backup
- On chip Voltage Monitor with Battery backup
- On chip Temperature Monitor with Battery backup, Temperature Sensors

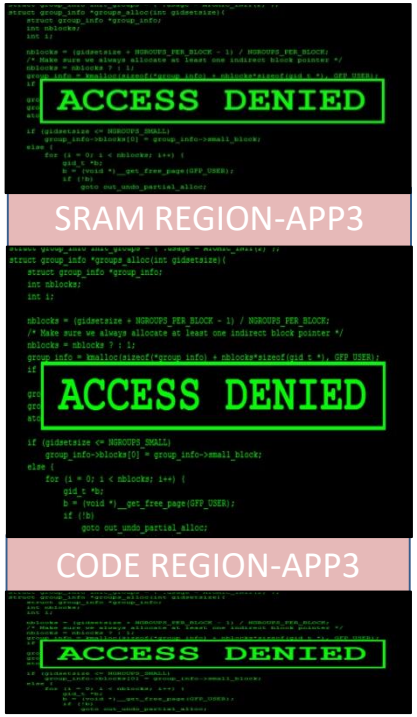
Why Memory Protection ?

UBER



OLA

MERU



Multiple parallel threads are required to be supported with isolated environment

Region based Memory Protection (TrustZone)

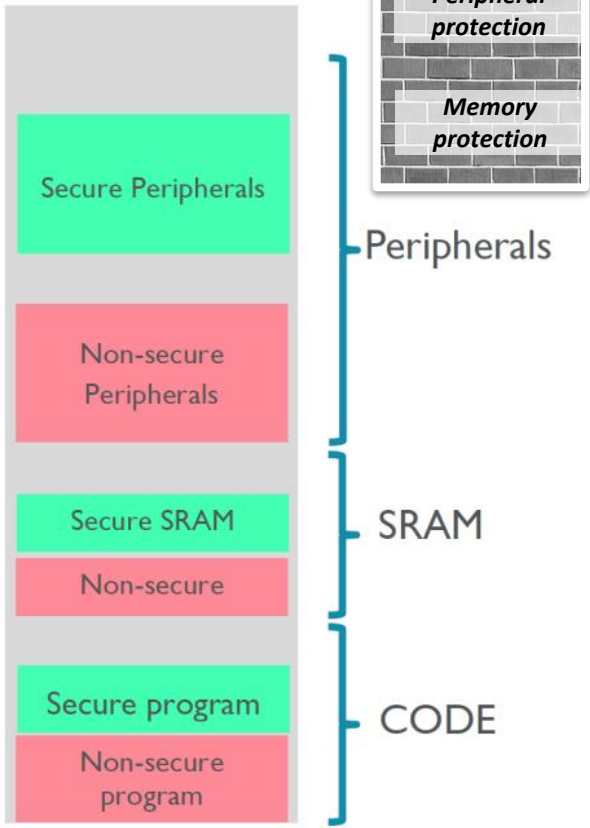
ARMv8-M system with TrustZone provides programmable hardware that supports region based memory protection [S(Secure)/NS(Non-secure)]

Maximum 8 distinct memory regions are allowed to be programmed

Allows CODE, SRAM and Peripheral regions to be programmed as Secure or Non-secure

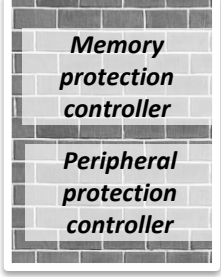
Each Application/Process/thread owns some Peripherals, SRAM and CODE regions

Each Application/Process/thread belongs to either Secure or Non-secure state



*Source ARM

Region Based Memory Protection



SRAM REGION-APP1

CODE REGION-APP1

PERIPHERAL REGION-APP1

UBER

3

SRAM REGION1-APP2

CODE REGION APP2

SRAM REGION2-APP2

SRAM REGION3-APP2

PERIPHERAL REGION-APP2

OLA

5

SRAM REGION-APP3

CODE REGION APP3

MERU

2

?

PERIPHERAL REGION-APP2

PERIPHERAL REGION-APP1

SRAM REGION3-APP2

SRAM REGION2-APP2

SRAM REGION1-APP2

SRAM REGION-APP1

CODE REGION-APP2

CODE REGION-APP1

MPC (Memory Protection controller) & PPC (Peripheral protection controller) enables granular memory partitioning with Protection

*Source ARM

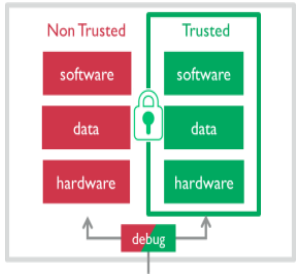
Roll back Attacks Protection

Rolling the time backwards by tampering Real time clock

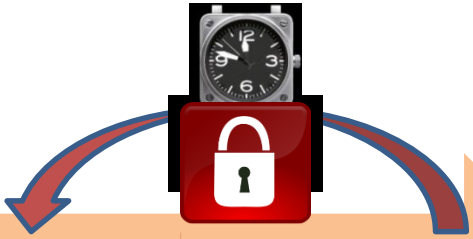
Hacker installed an older firmware version

Device is **NOW vulnerable** to **security THREATS** ☹☹

Hardware-reinforced debug port protection



Peripheral protection controller (secure clock)



Firmware v1 (2015) | Firmware v2 (2016) | Firmware v3 (2017) | Firmware v4 (2018) | Firmware v5 (2019)

5 security Vulnerabilities in V3

All security Vulnerabilities resolved in V5

Peripheral Protection

Secure storage

Battery Backup

Security & Performance

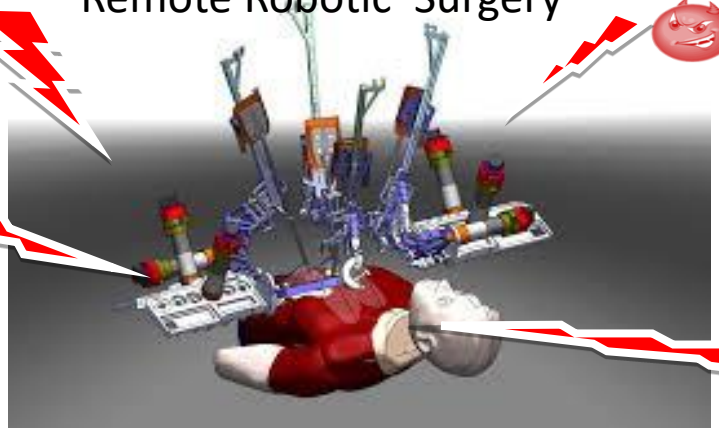
Hardware Crypto Accelerators
ECDSA, PKI, TRNG

Digital Signature

Eves Dropping into Patient Medical Records, Data Manipulation

Man in the middle attacks on by rogue devices – manipulating the robotic remote commands

Remote Robotic Surgery



Public key Infrastructure(PKI); TRNG(True Random Number generator)

Hibernating the operation devices to lose security information

Sluggishness of the IoT device

BATTERY BACKUP FOR SECURE KEYS

Hardware Crypto Accelerators for FAST ENCRYPTION & DECRYPTION

UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

December 23 2015, in Ivano-Frankivsk region of Western Ukraine, hackers brought down 30 power substations, leaving more than 230,000 residents in the dark.

The hackers managed to get worker credentials, some of them for VPNs the grid workers used to remotely log in to the power grid network.

Then they wrote malicious firmware to replace the legitimate firmware on serial-to-Ethernet converters at more than a dozen substations.

Their malicious firmware Rendered the converters thereafter inoperable and unrecoverable, unable to receive commands. You have to be at that site and manually replace converters.

What is Firmware Attack ?

To ensure that the target embedded device runs only authorized firmware or uses only authorized configuration data, we need to provide a way to verify both authenticity and integrity of the information. This means making sure that the data is trusted and not subsequently modified, otherwise it can lead to :-

Output confidential and sensitive data

Force the device to operate incorrectly

Induce unpredictable device behavior

Firmware Attack Protection

Hardware-reinforced debug port protection

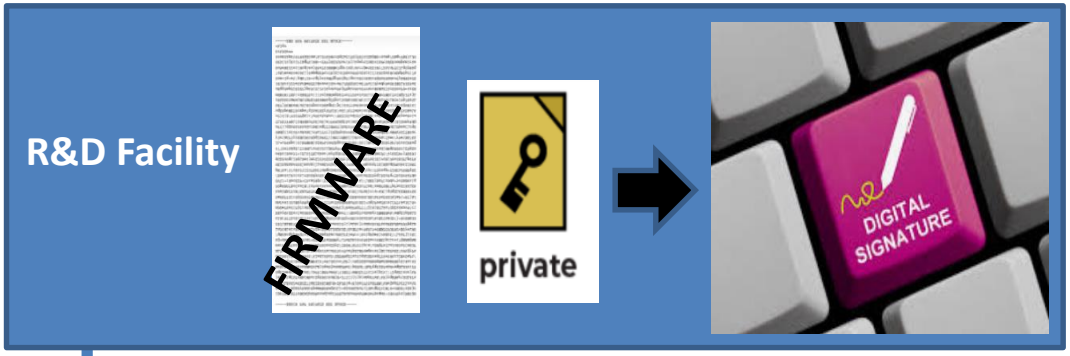
Hardware unique key-based cryptography secure boot, Code protection

SHA-256

PKI

ECDSA

Random Number Generator

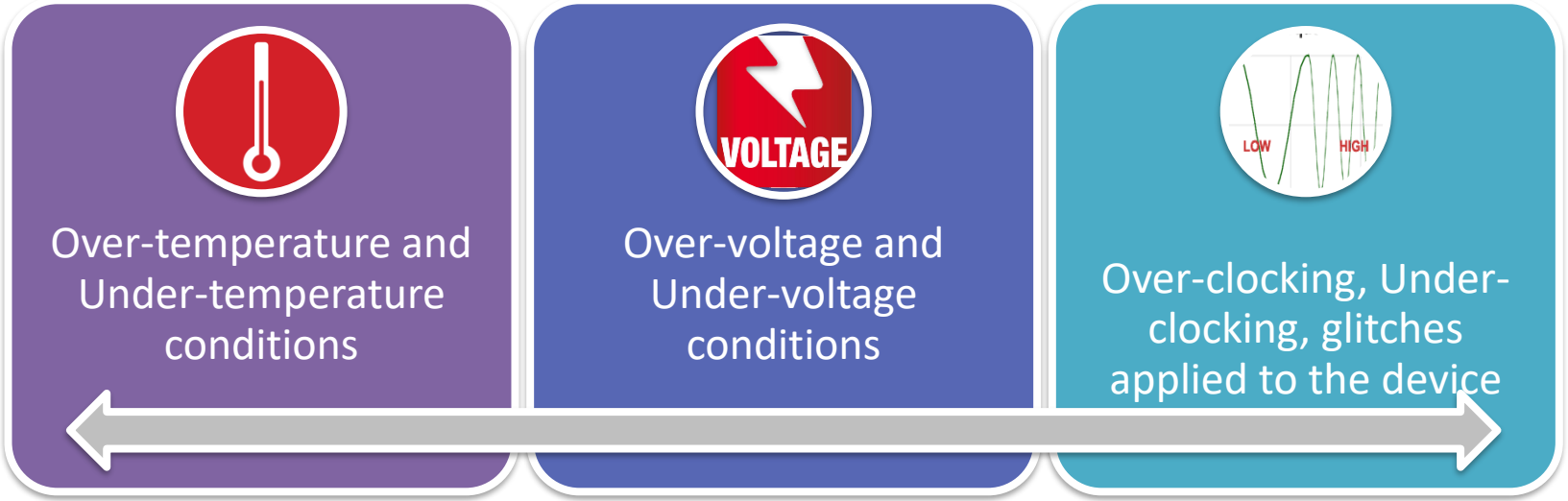


Secure Boot and Secure Download

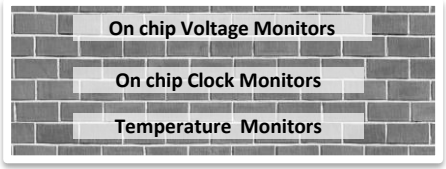
What is TAMPER ?

Tamper refers to intentional alteration or manipulation to the system such that it compromises the secrets in the system or enables unauthorized operation of the system.

To alter the device environmental or operational conditions with the intent to operate the MCU or other components in an unintended way, following types of attacks can be used :-



Tamper Protection



- On-Chip TAMPER Sensors
- Voltage Monitors
- Temperature Monitors
- Clock Monitors

TAMPER DETECTION

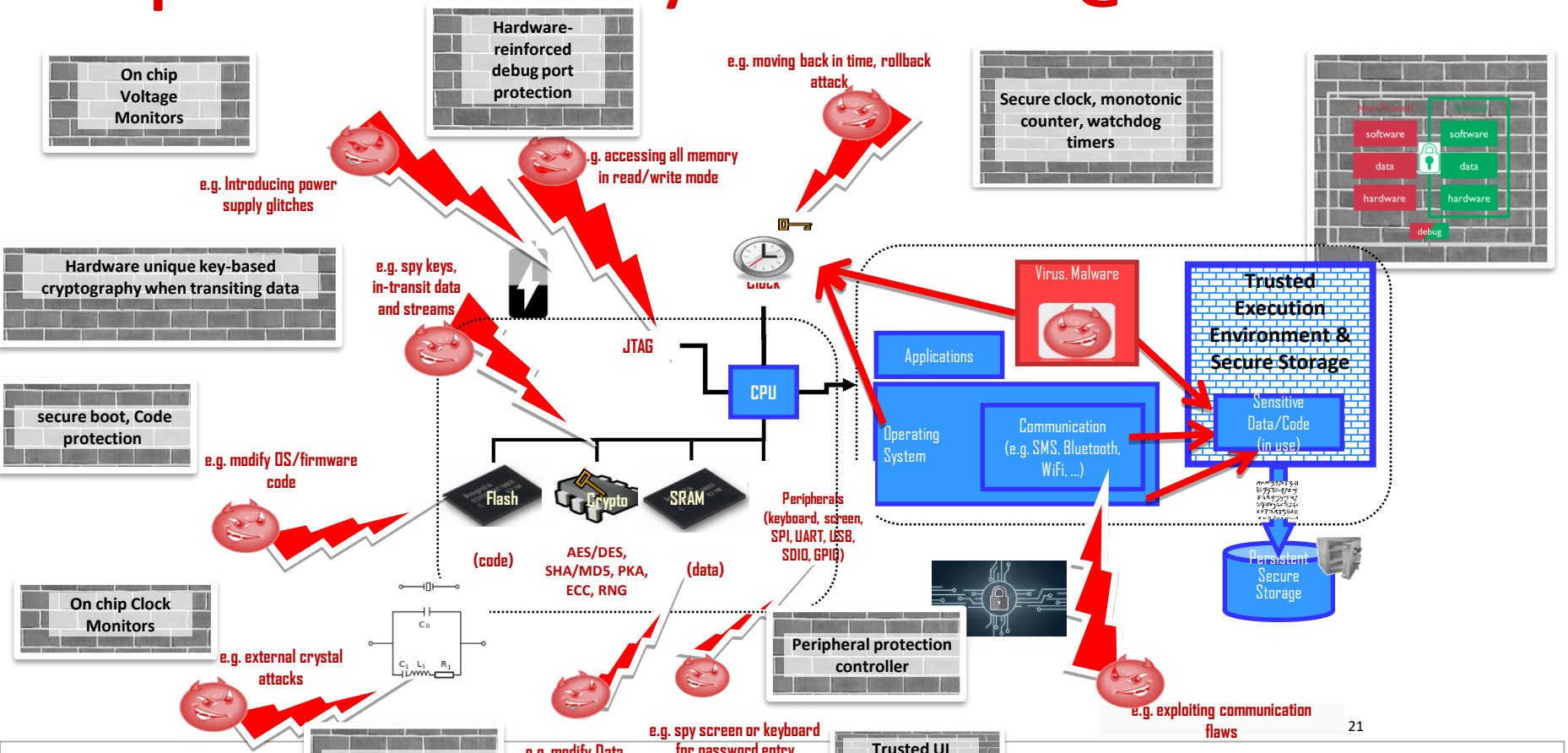
TAMPER EVIDENCE

- Tamper Event Timestamp
- Tamper Event Source

TAMPER RESPONSE

- Enter fail-safe applications mode
- Reset Device
- Erase keys

Chip level Attacks :H/W Solutions @ Glance



Key Takeaways

IoT is a Huge Opportunity, but IoT Security is a Huge Problem.

The Key to IoT security and Performance is strong Hardware Foundation.

Mitigate IoT security Threats by using an effective combination of Software and Hardware solutions.

Thank You