EECE-4710 "IoT and TinyML"

IoT Security

Cristinel Ababei

MARQUETTE UNIVERSITY

BE THE DIFFERENCE.

1

1

Internet of Things (IoT)
Threat of Opportunity?

2

2

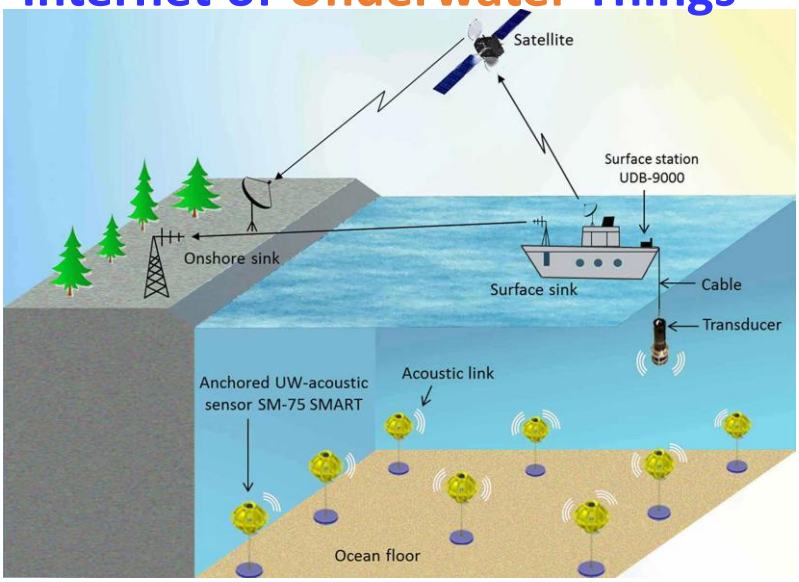
Recall: What is IoT?

Internet of Things (**IoT**): is the network of physical objects or "things"—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data.

3

3

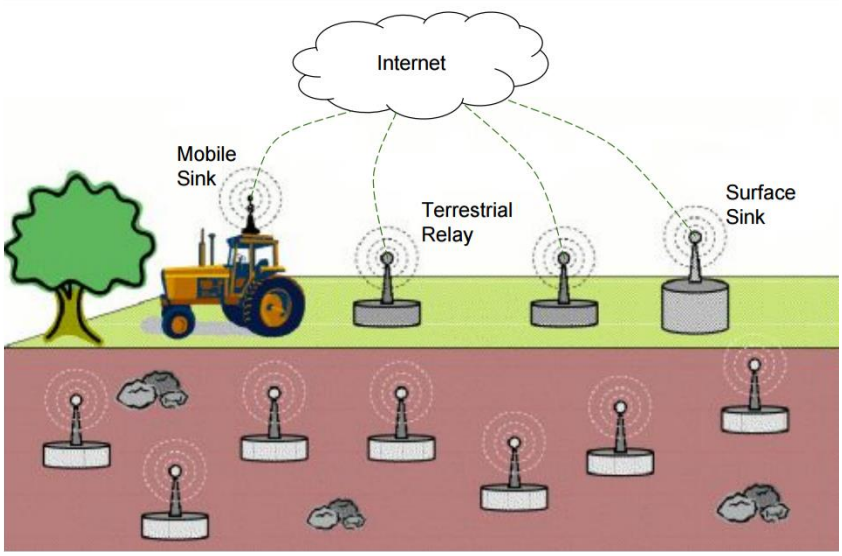
Internet of Underwater Things



Source: I.F. AKYILDIZ

4

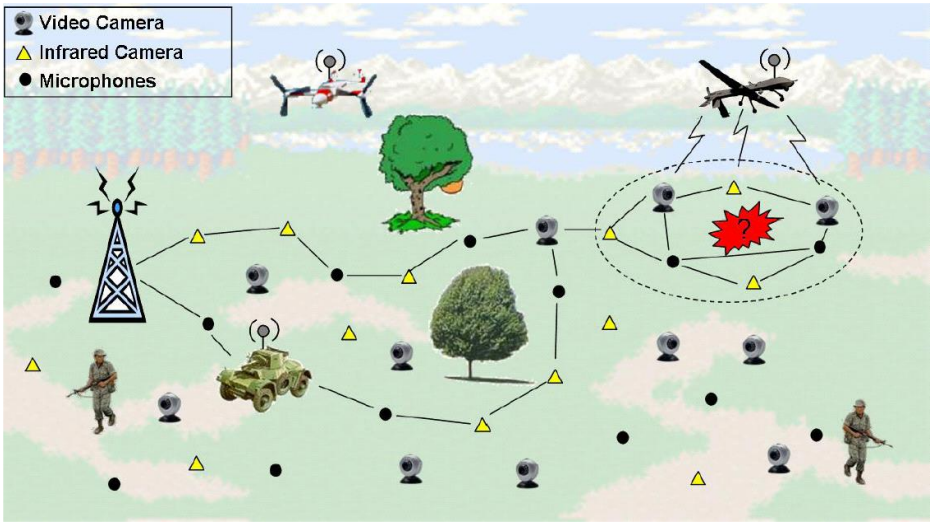
Internet of Underground Things



Source: I.F. AKYILDIZ

5

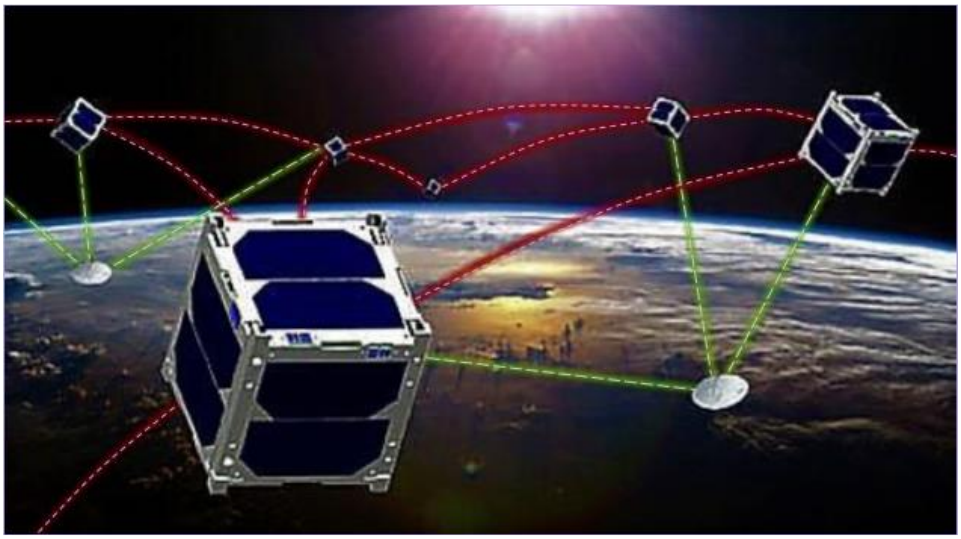
Internet of Battlefield Things



Source: I.F. AKYILDIZ

6

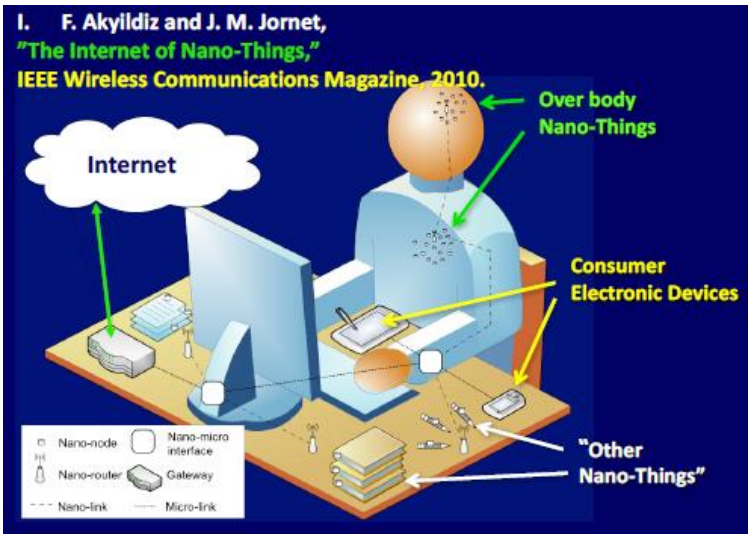
Internet of Space Things



Source: I.F. AKYILDIZ

7

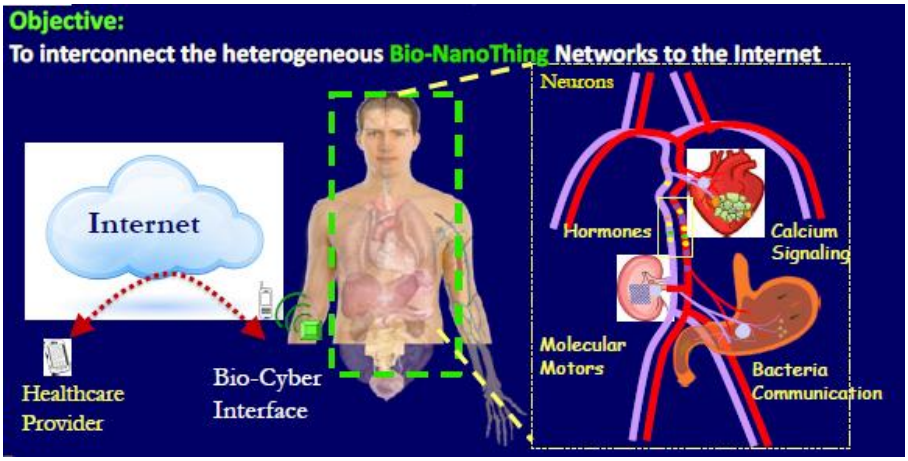
Internet of Nano Things



Source: I.F. AKYILDIZ

8

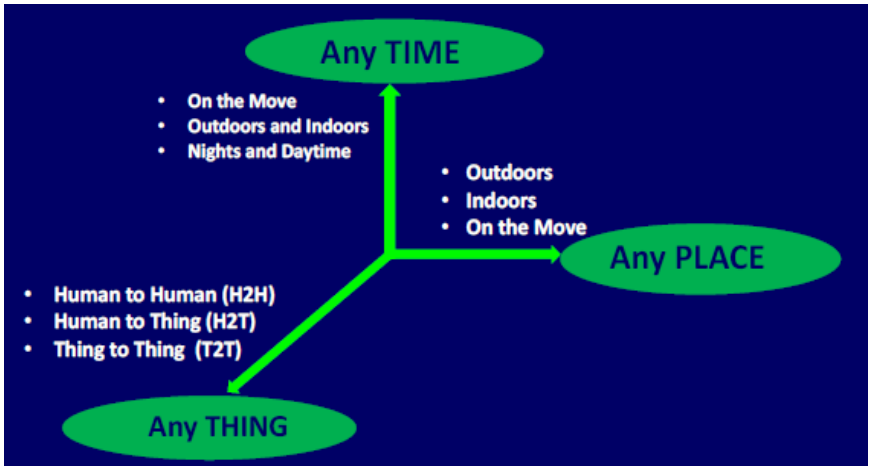
Internet of Bio-Nano Things



Source: I.F. AKYILDIZ

9

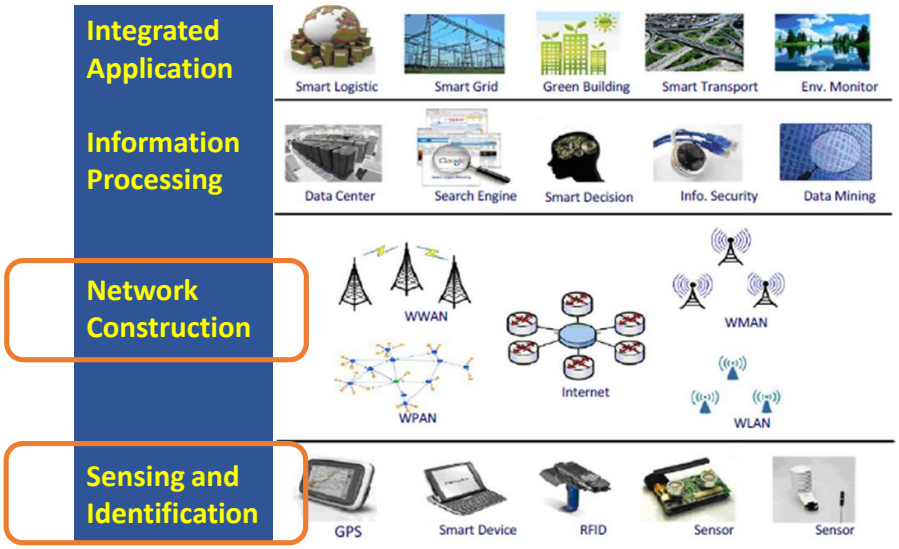
IoT: Perspectives



Source: I.F. AKYILDIZ

10

4-layer Model of IoT



Source: I.F. AKYILDIZ

11

11

Technological Challenges of IoT

- Scalability
- Technological standardization
- Inter operability
- Discovery
- Software complexity
- Data volumes and interpretation (tinyML emerges)
- Power supply (energy harvesting?)
- Interaction and short-range communication
- Wireless communication
- Fault tolerance

12

12

Why be Concerned about IoT?

- It is just another computer, right?
  - All the same issues we have with access control, vulnerability management, patching, monitoring, etc.
  - Imagine your network with 1,000,000 more devices
  - Any compromised device is a foothold on the network
  - Are highly portable devices captured during vulnerability scans?
  - Where is your network perimeter?
  - Are consumer devices being used in areas – like health care – where reliability is critical?

13

13

Criticisms and Controversies of IoT

Scholars, social observers, and pessimists have doubts about the promises of the ubiquitous computing revolution, in areas as:

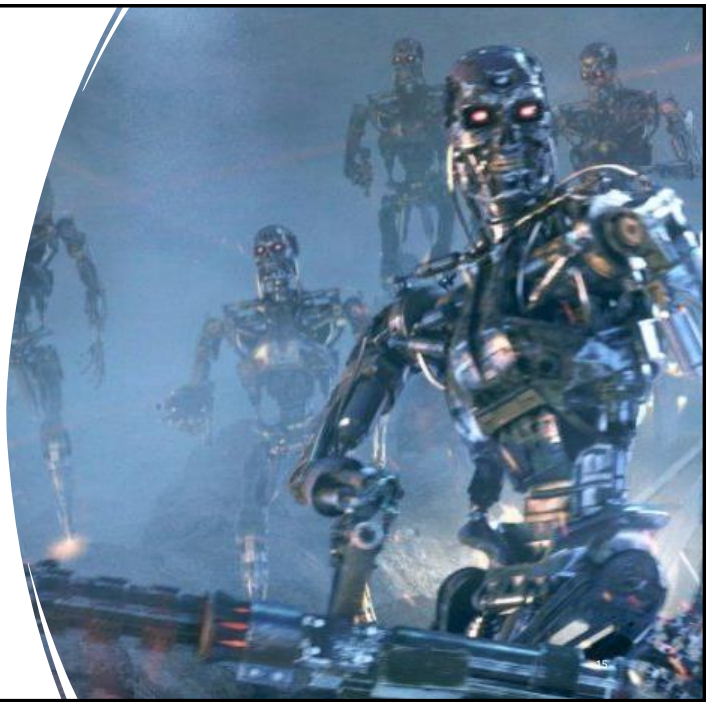
- Security
- Privacy
- Autonomy and Control
- Social control
- Political manipulation
- Environmental impact
- Influences human moral decision making

14

14

Threat vs. Opportunity?

- If misunderstood and misconfigured, IoT poses risk to our data, privacy, and safety
- If understood and secured, IoT will enhance communications, lifestyle, and delivery of services



15

IoT Security
(1) Network Level

16

The Question:

Who needs security in a wireless channel anyway?

The Answer:

Everybody! So, how do you provide the appropriate level of security within the acceptable price and "inconvenience" margin

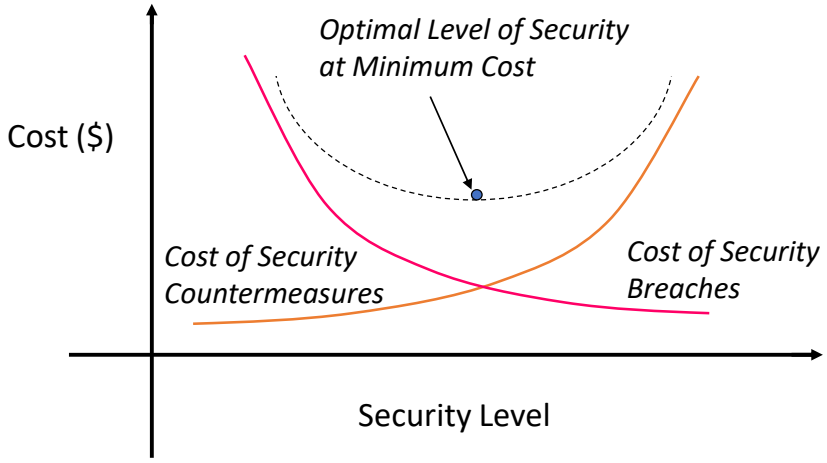
→Risk Management!

Source: Peter L. Fuhr

17

Optimization of Security vs. Cost

- Risk reduction is balanced against the cost of security counter measures to mitigate the risk.



Source: Peter L. Fuhr

18

What is IoT Security?

- IoT devices can be deployed by any business center, thereby bypassing typical network security controls and processes.
- All these network-connected IoT devices – printers, cameras, sensors, lighting, **HVAC**, appliances, infusion pumps, handheld scanners (the list goes on and on) – are using different hardware, chipsets, operating systems and firmware that introduce vulnerabilities and risk.
- **IoT Security:** is the practice/act of securing Internet devices and the networks they're connected to from threats and breaches by protecting, identifying, and monitoring risks all while helping fix vulnerabilities from a range of devices that can pose security risks (to your business).

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security

19

19

What Are the Challenges of IoT Security?

- Overarching challenge for security in IoT is that as large numbers of diverse IoT devices continue to connect to the network, a dramatic expansion of the attack surface is happening in parallel
- Ultimately the entire network security posture is diminished to the level of integrity and protection offered to the least secure device

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security

20

20

What Are the Challenges of IoT Security?

- **98% of all IoT device traffic is unencrypted -** putting personal and confidential data at severe risk.
- **51% of threats for healthcare organizations involve imaging devices -** disrupting the quality of care and allowing attackers to exfiltrate patient data stored on these devices.
- **72% of healthcare VLANs mix IoT and IT assets -** allowing malware to spread from users' computers to vulnerable IoT devices on the same network.

Source: https://unit42.paloaltonetworks.com/iot-threat-report-2020/

21

21

Challenges that are unique to IoT security

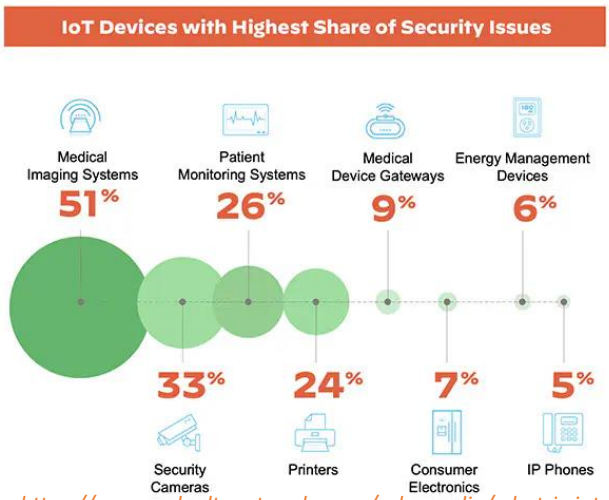
- Inventory – not having clear visibility and context for what IoT devices are in the network and how to securely manage new devices.
- Diversity – the sheer diversity of IoT devices in terms of their limitless forms and functions.
- Threats – lack of well-embedded security into IoT device operating systems that are hard or impossible to patch.
- Data volume – overseeing vast amounts of data generated from both managed and unmanaged IoT devices.
- Ownership – new risks associated with the management of IoT devices by disparate teams within the organization.
- Operations – the unification crisis wherein IoT devices are critical to core operations yet difficult for IT to integrate into the core security posture.

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security

22

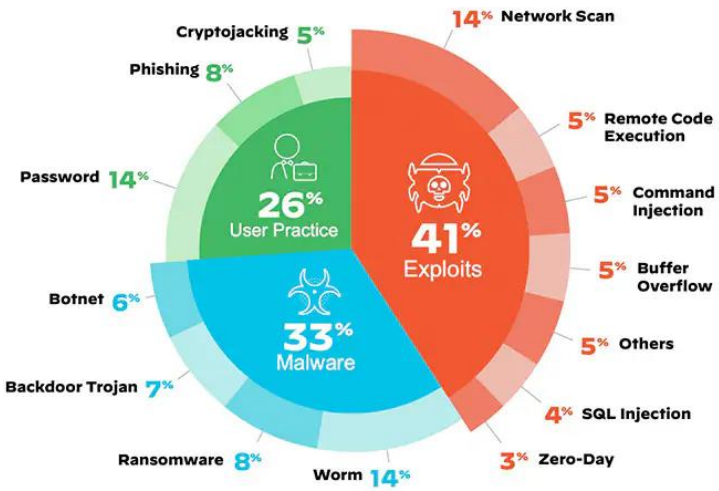
22

Which IoT Devices Have the Highest Share of Security Issues?



Source: https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security

What Are the Top IoT Security Threats?



Source: https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security

Most frequent attacks on IoT devices

- **Exploits** executed using techniques such as:
  - Network scanning
  - Remote code execution
  - Command injection and others.
- **41% of attacks** exploit device vulnerabilities
  - Attacks scan through network-connected devices in an attempt to exploit known weaknesses.
  - After compromising the first device, lateral movement is opened-up to access other vulnerable devices and compromise them one by one.

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security

25

25

Exploits – 41%

- **Scanning attack** is a method used by threat actors to identify vulnerabilities in a network or system. Scanning attacks typically involve using automated tools to scan for open ports, vulnerabilities, and other weaknesses that can be exploited to gain unauthorized access and/or launch a cyber attack.
- **Remote code execution (RCE)** refers to a class of cyberattacks in which attackers remotely execute commands to place malware or other malicious code on your computer or network.
- **Command injection** is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell.
- **Buffer overflow** condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code.
- **SQL injection** attack consists of insertion or “injection” of a SQL query via the input data from the client to the application.
- **"Zero-day"** is a broad term that describes recently discovered security vulnerabilities that hackers can use to attack systems. The term "zero-day" refers to the fact that the vendor or developer has only just learned of the flaw – which means they have “zero days” to fix it. A zero-day attack takes place when hackers exploit the flaw before developers have a chance to address it.

26

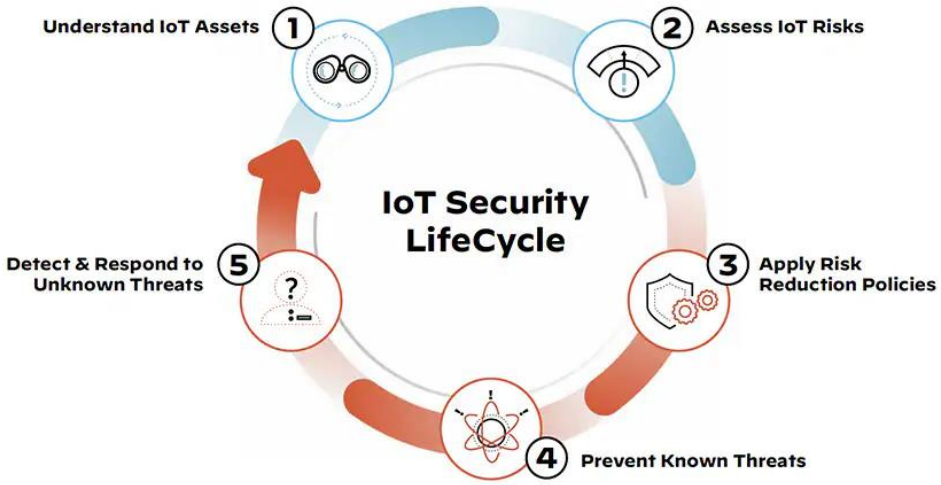
26

Malware – 33%

- Worm
  - A worm virus refers to a malicious program that replicates itself, automatically spreading through a network. In this definition of computer worms, the worm virus exploits vulnerabilities in your security software to steal sensitive information, install backdoors that can be used to access the system, corrupt files, and do other kinds of harm.
- Ransomware
  - Ransomware is a type of malware designed to extort money from its victims, who are blocked or prevented from accessing data on their systems.
  - Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off.
- Backdoor Trojan
  - Backdoor Trojans are malicious software programs that provide unauthorized access to a computer in order to launch a remote attack. Remote attackers can use a hacked machine to send commands or gain complete control.
- Botnet
  - A botnet attack is any attack leveraging a botnet—a group of bots and devices linked together to perform the same task—for distribution and scaling. Botnet attacks are used by cybercriminals to carry out intense scraping, DDoS (distributed denial of service), and other large-scale cybercrime.

What Are the Best Practices for IoT Security?

- Lifecycle approach encompasses five critical stages of IoT security



Source: https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security

Incorporate IoT security into standard practice, process and procedure

1. Identify all managed and unmanaged devices.
2. Accurately assess and identify vulnerabilities and risks associated with all devices.
3. Automate Zero Trust policies and enforcement of those policies. Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction. It is rooted in the principle of “never trust, always verify,”.
4. Take swift action on preventing known threats.
5. Rapidly detect and respond to unknown threats.

Source: https://www.paloaltonetworks.com/zero-trust

29

29

How to Secure IoT Devices in the Enterprise

1. **Employ Device Discovery for Complete Visibility**
2. **Apply Network Segmentation for Stronger Defense**
3. **Adopt Secure Password Practices**
4. **Continue to Patch and Update Firmware When Available**
5. **Actively Monitor IoT Devices at All Times**

Source: https://www.paloaltonetworks.com/cyberpedia/how-to-secure-iot-devices-in-the-enterprise

30

30

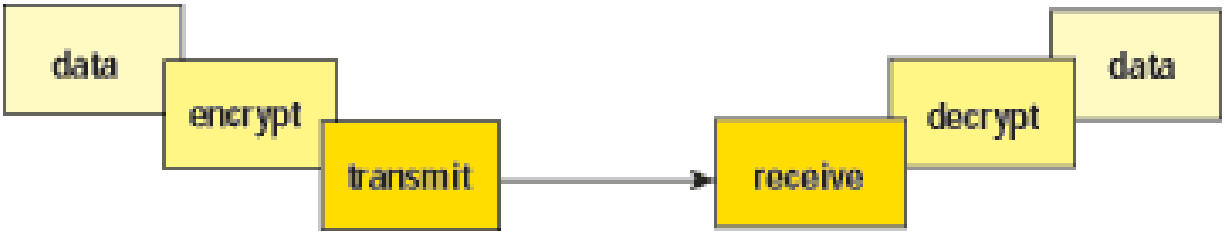
Addressing TIPPSS is essential to achieving safety, security, and scalability

- **Trust**: Allow only designated people/services device or data access
- **Identity**: Validate the identity of people, services, and "things"
- **Privacy**: Ensure device, personal & sensitive data is kept private
- **Protection**: Protect devices and users from harm
- **Safety**: Provide safety for devices, infrastructure and people
- **Security**: Maintain security of data, devices, people, etc.

31

31

Wired Data Security - Encryption



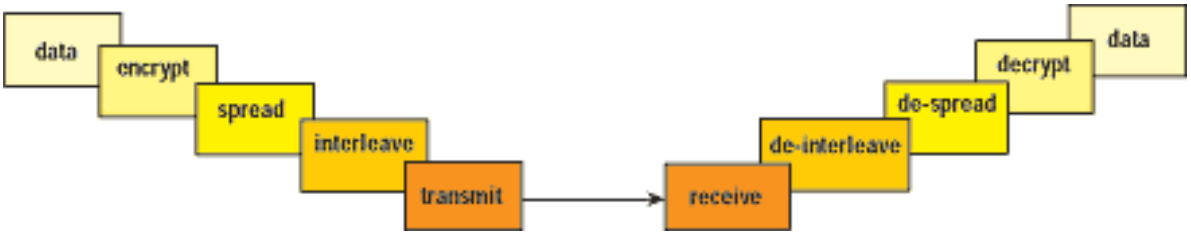
The "traditional" method involved encrypting the data prior to transmission over a potentially insecure channel. The level of protection rests on the encryption algorithm. (There are a few other factors… such as the physical media.)

Source: Peter L. Fuhr

32

32

Wireless Data Security: Encryption, Spreading, Interleaving



Wireless networks use a variety of techniques to enhance security, such as spreading and interleaving. These techniques can make the signal virtually undetectable without prior knowledge about the network. This can improve the security of the network by orders of magnitude.

33

33

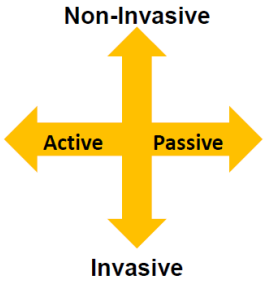
IoT Security
(2) Device Level

34

34

Taxonomy of Physical Attacks

- Two orthogonal criteria



- **Active**: perturbate and conclude
- **Passive**: observe and infer

- **Invasive**: open package, contact chip
- **Semi-Invasive**: open package, no contact
- **Non-Invasive**: no modifications

(a) Side-channels: passive and (typically) non-invasive
(b) Circuit modification: active and invasive
(c) Fault injection: active, different degrees of invasion

Source: Josep Balasch, KU Leuven

35

35

(a) Side-channel Leakage

Physical attacks ≠ Cryptanalysis

(gray box, physics) (black box, maths)

- Does not tackle the algorithm's math

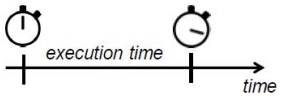
- Observe physical quantities in the device's vincinity and use additional information during cryptanalysis

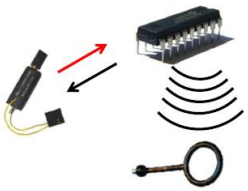
36

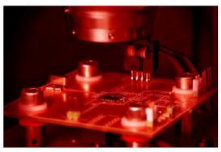
36

Side-channels (not exhaustive)

- Passive:
  - Timing
    - Overall or "local" execution time
  - Power, Electromagnetic (EM) radiation
    - Predominant CMOS technology
    - Dynamic power consumption
    - Electric current induces an EM field
  - More exotic but shown to be practical
    - Sound, temperature, …
- Invasive: Photonic emissions





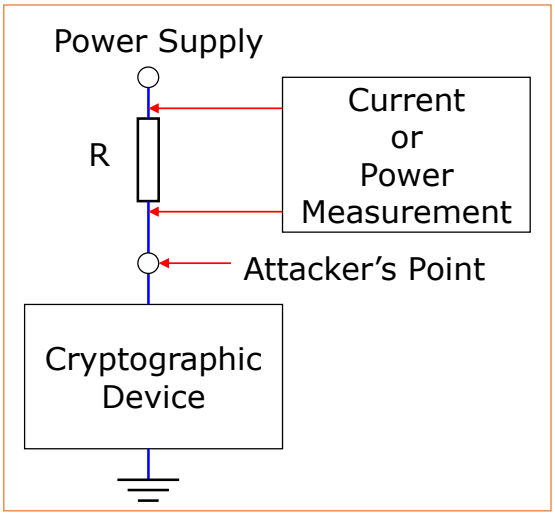


37

37

What is a Power Analysis Attack?

Side-channel attacks exploit correlation between secret parameters and variations in timing, power consumption, and other emanations from cryptographic devices to reveal secret keys



Source: Pascal Paillier

38

38

Power Analysis

- What can we see looking at a curve?
- Information in:
  - Repetitive patterns: typically coarse, structure of algorithm and implementation (e.g. loops)
  - Time: what happens when, program flow
  - Amplitude: what happens at a given moment in time, data flow
    - The same operation, executed with different operand values, consumes more or less power
- Examples: trace inspection

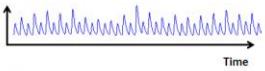
39

39

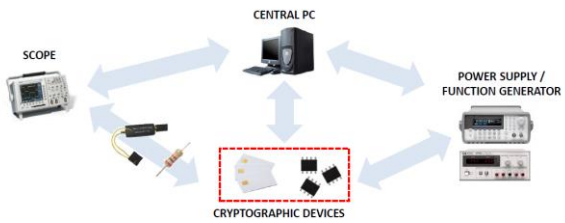
Power Measurements, Simple Power Analysis (SPA), Differential Power Analysis (DPA)

Measuring power consumption

- Not average power over time, not peak power
- Instantaneous power over time
  - Trace or curve, many samples

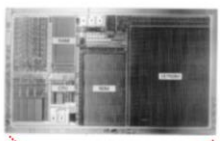


- Typical (automated) measurement setup



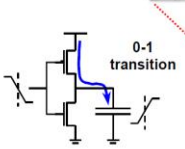
Measuring power consumption (II)

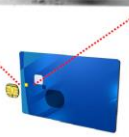
- Logic: constant supply voltage, supply current varies
- Predominant technology: CMOS
  - Low static power consumption
  - Relatively high dynamic power consumption
  - Power consumption depends on input



- CMOS inverter:

Input	Output	Current
0→0	1→1	Low
0→1	1→0	Discharge
1→0	0→1	Charge
1→1	0→0	Low





40

40

Simple Power Analysis (SPA)

SPA: Simple Power Analysis attacks (I)

- Anything but simple (except in examples ☺)
- Visual inspection of a few traces, worst/best case: single shot [KJJ99]
- Often exploits direct key dependencies
  - Input/output not need to be known, but useful for verification
- Require: expertise, experience, detailed knowledge about target device and implementation
- Examples in following slides: patterns, amplitude, timing

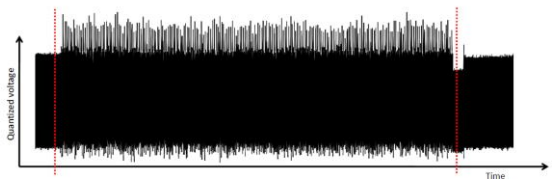
SPA: Simple Power Analysis attacks (II)

- **Patterns** (over many-cycle sequences) show, e.g.:
  - Symmetric crypto algorithms
    - Number of rounds (resp. key length), loops
    - Memory accesses (sometimes higher power consumption)
  - Asymmetric crypto algorithms
    - Key length
    - Implementation details (e.g. RSA with CRT)
    - Key (if careless implementation, e.g. RSA/ECC)

SPA: Simple Power Analysis attacks (III)

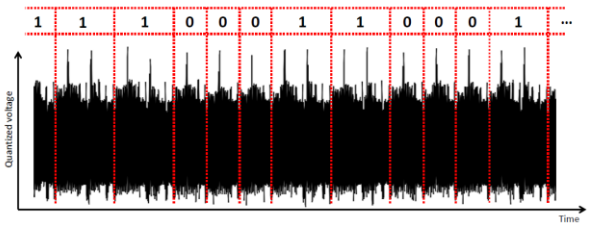
```
ECC POINT MULTIPLICATION
(left-to-right binary method)
INPUT: k=(k_{t-1},...,k_0)_2, P ∈ E(F_q)
OUTPUT: Q = kP
Q ← ∞
FOR i=t-1 TO 0
    Q ← 2Q              ; point doubling
    IF k_i == 1
        Q ← Q + P       ; point addition
RETURN Q
```

- Conditional, key-dependent operation
- Different algorithms to compute point addition and point doubling
- Implementation on 8-bit µC with Montgomery co-processors (affine points)



SPA: Simple Power Analysis attacks (IV)

- Zoom-in until patterns appear:
  - Always point doubling
  - Sometimes point addition

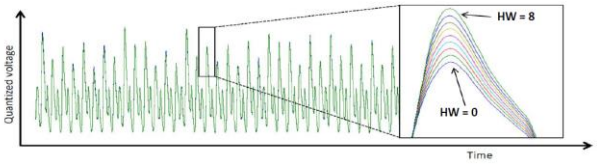


SPA: Simple Power Analysis attacks (V)

- **Amplitude** of a certain cycle can show:
  - Exact operand values (extreme case)
  - Often: Hamming weight or Hamming distance of operand(s)
  - Operation being executed in software scenarios
    - Reverse-engineering of implementation details, and e.g. proprietary algorithms

SPA: Simple Power Analysis attacks (VI)

- Example: Load from Memory instruction (LD)
- Power consumption depends on HW of the read value



- Suppose we have a 'dictionary' that translates power consumption values into HW
- Example: SPA attack on the AES key schedule [M02]
  - Extract HWs of round keys, generate list of suitable round keys
  - Requires 1 plaintext/ciphertext pair to check remaining candidate keys

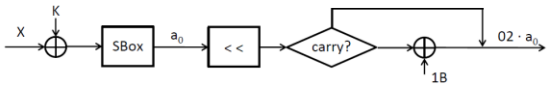
SPA: Simple Power Analysis attacks (VIII)

- **Timing**, e.g. when an operation is executed, can show:
  - Data-dependent branches in software implementations
  - Execution of additional operations

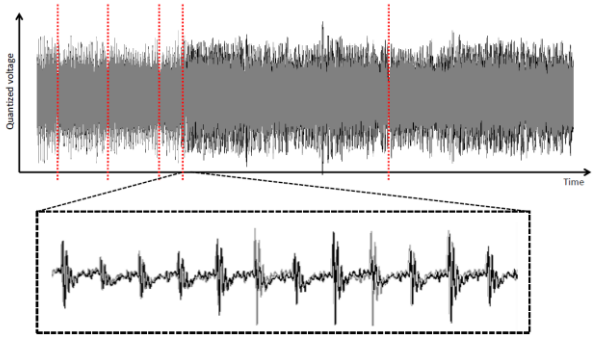
- Example: bad implementation of AES MixColumns [KQ99]

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

  - Multiplications by 02 in GF(2^8):
    - Shift one bit to the left
    - If carry occurs, XOR the result with 1B



SPA: Simple Power Analysis attacks (IX)



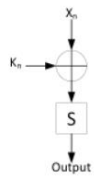
Differential Power Analysis (DPA)

- DPA is a much more powerful attack than SPA.
- Much more difficult to prevent too.
- While SPA attacks use primarily visual inspection to identify relevant power fluctuations, DPA attacks use statistical analysis and error correction techniques to extract information correlated to secret keys.
- Implementation of a DPA attack involves two phases:
  1. Data collection - may be performed as described previously by sampling a device's power consumption during cryptographic operations as a function of time
  2. Data analysis - a number of cryptographic operations using the target key are observed

Source: https://cryptome.org/jya/dpa.htm

Differential Power Analysis (DPA)

$$\text{Output} = S[X_n \oplus K_n]$$



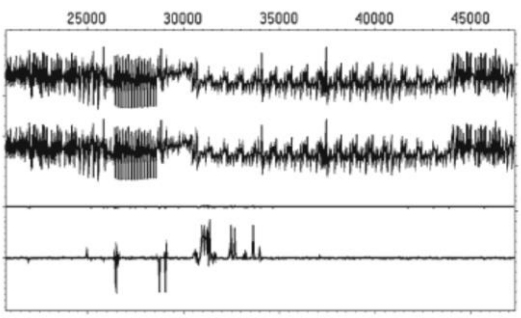


Figure 4: Typical DPA result. This example shows correlation.
(From: Intro to Differential Power Analysis[1])

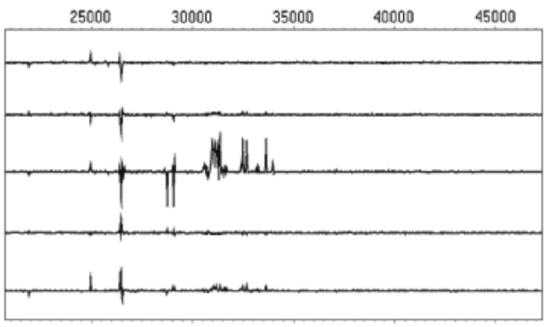


Figure 5: DPA result for different key values.
(From: Intro to Differential Power Analysis[1])

Source: https://anysilicon.com/side-channel-attacks-differential-power-analysis-dpa-simple-power-analysis-spa-works/

Countermeasures (I)

- You cannot prevent the adversary from trying to mount an attack
- Active:
  - You can try to make it more difficult
    - "Hide" sensitive parts of the chip: Epoxy, metal layers, glue logic, etc.
  - You can try to detect an attack and raise an alarm
    - Security sensors: power, clock, light, temperature, wire mesh
    - Perform error check before outputting the result: add redundancy
  - Reaction to alarm: depends on security policy
    - Stop computing, reset, erase memory, self-destruct: Security vs usability

Countermeasures (II)

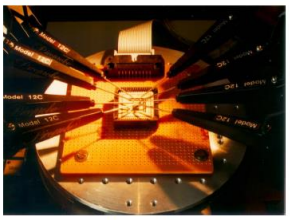
- Passive:
  - Try to eliminate side-channels, reduce information leakage, turn leaked information useless
    - Execution time independent of secret values
    - Sequence of operations independent of secret values
    - Hiding countermeasures
      - Time domain: dummy operations, shuffling, ...
      - Amplitude domain (SNR): background noise, , secure logic styles,...
    - Masking countermeasures to prevent known inputs
      - Boolean masks, secret sharing schemes, ...
    - Design algorithms using gray-box model:
      - Leakage-resilient cryptography

47

47

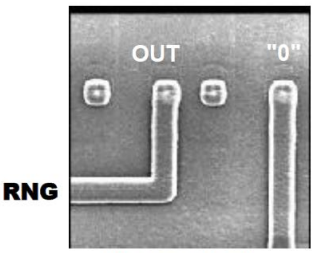
(b) Invasive Attacks

- Passive: micro-probing
  - Probe the bus with a very thin needle
  - Read out data from bus or individual cells directly
  - Several needles concurrently



source: Helena Handschuh

- Active: circuit modification
  - Connect or disconnect security mechanism
    - Disconnect security sensors
    - RNG stuck at a fixed value
    - Reconstruct blown fuses
  - Cut or paste tracks with laser or focused ion beam
  - Add probe pads on buried layers



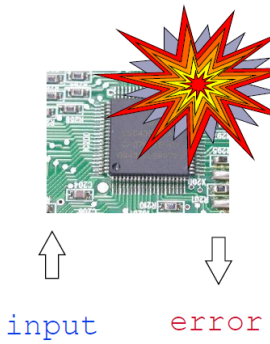
[www.fa-mal.com]

48

48

(c) Fault Injection Attacks (I)

- Non-(semi)invasive: apply combination of strange environmental conditions
  - Vcc
  - Glitch
  - Clock
  - Temperature
  - UV
  - Light
  - X-Rays
  - ...



- And bypass security mechanisms or infer secrets

slide source: Helena Handschuh 49

49

Fault Injection Attacks (II)

- Invasive: exploit faulty behavior provoked by physical stress applied to the device
  - Laser fault injection allows to target a relatively small surface area of the target device
  - Laser pulse frequency ~ 50Hz
  - Fully automated scan of chip surface
  - Once you have a weak spot: perturbate and exploit

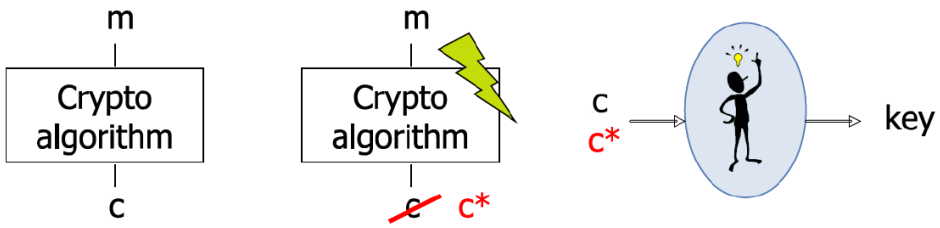
source: www.new-wave.com

50

50

Differential Fault Analysis

- Ask for a cryptographic computation twice
  - With any input and no fault (reference)
  - With the same input and fault injection
- Infer information about the key from the output differential



- Sometimes a single fault injection is enough!

51

Summary

- Security as a design dimension
  - Adding security against implementation attacks consumes resources
    - Extra area, time, power, product development, …
- Attacker will go for the easiest entry point
  - If strong crypto algorithm, try other weaknesses
  - Monitor power consumption, EM radiation, time, …
  - Inject glitches: clock, voltage, lasers, …
- Threat of power analysis attacks:
  - Passive and non-invasive, low-cost equipment, …
  - Arms-race between attacks and countermeasures

52

52

Credits

- https://www.crowdstrike.com/cybersecurity-101/remote-code-execution-rce/
- https://heimdalsecurity.com/blog/scanning-attack-what-it-is-and-how-to-protect-your-organization-against-it/
- https://owasp.org/www-community/attacks/Command_Injection
- https://owasp.org/www-community/vulnerabilities/Buffer_Overflow
- https://www.fortinet.com/resources/cyberglossary/buffer-overflow
- https://owasp.org/www-community/attacks/SQL_Injection
- https://portswigger.net/web-security/sql-injection
- https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit
- https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-zero-day-attack
- https://www.proofpoint.com/us/threat-reference/ransomware
- https://en.wikipedia.org/wiki/Ransomware
- https://www.fortinet.com/resources/cyberglossary/worm-virus
- https://www.malwarebytes.com/computer-worm
- https://www.tutorialspoint.com/what-are-backdoor-trojans
- https://gridinsoft.com/backdoor
- https://www.paloaltonetworks.com/cyberpedia/what-is-botnet
- https://usa.kaspersky.com/resource-center/threats/botnet-attacks
- …

53