



2 Days Training on IoT Architecture and Simulation using ns-3

CHAPTER 12 – IoT Security

Muhammad Saufy Rohmad
EE, UiTM
CompuThings




Introduction

- As architects, we are responsible for understanding the IoT stack of technologies and securing them.
- This has been particularly difficult for many IoT deployments with security often being thought of last.
- Level of IoT security:
 - physical devices
 - communication systems
 - networks




Attack and Threat Terms

- The following are the terms and definitions of different attacks or malevolent cyber threats:
 - **Amplification attack:** Magnifies the bandwidth sent to a victim. Often an attacker will use a legitimate service such as NTP, Steam, or DNS to reflect the attack upon a victim. NTP can amplify 556x and DNS amplification can escalate the bandwidth by 179x.
 - **ARP spoof:** A type of attack that sends a falsified ARP message resulting in linking the attacker's MAC address with the IP of a legitimate system.
 - **Banner scans:** A technique typically used to take inventory of systems on a network that can also be used by an attacker to gain information about a potential attack target by performing HTTP requests and inspecting the returned information of the OS and computer (for example, nc www.target.com 80).



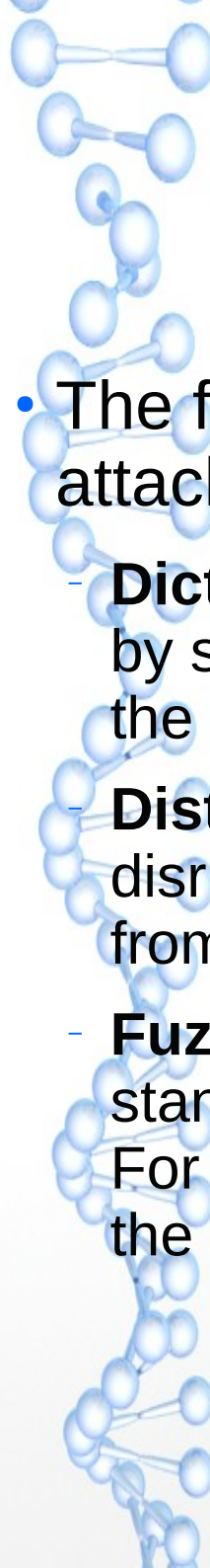
Attack and Threat Terms(2)

- The following are the terms and definitions of different attacks or malevolent cyber threats:
 - **Botnets:** Internet-connected devices infected and compromised by malware working collectively by common control, mostly used in unison to generate massive DDoS attacks from multiple clients. Other attacks include email spamming and spyware.
 - **Brute force:** A trial and error method to gain access to a system or bypass encryption.
 - **Buffer overflow:** Exploits a bug or defect in running software that simply overruns a buffer or memory block with more data than allocated. This overrun can write over other data in adjacent memory addresses. An attacker can lay malicious code in that area and force the instruction pointer to execute from there. Compiled languages such as C and C++ are particularly susceptible to buffer overflow attacks since they lack internal protection. Most overflow bugs are the result of poorly constructed software that does not check the bounds of input values.



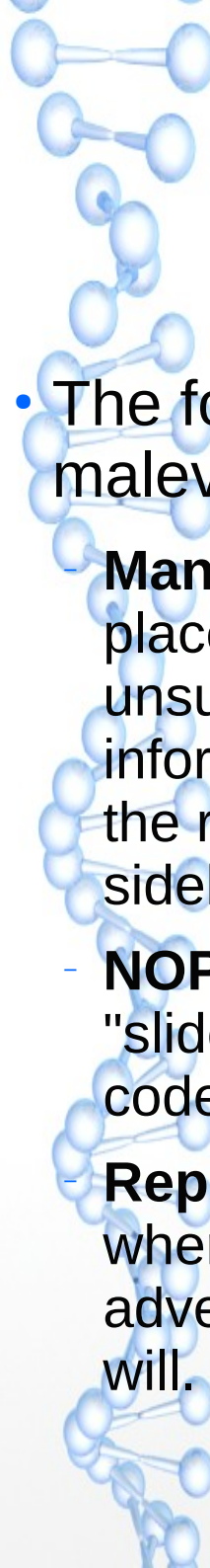
Attack and Threat Terms(3)

- The following are the terms and definitions of different attacks or malevolent cyber threats:
 - **C2:** Command and control server that marshals commands to botnets.
 - **Correlation power analysis attack:** Allows one to discover secret encryption keys stored in a device through four steps. First, examine a target's dynamic power consumption and record it for each phase of the normal encryption process. Next, force the target to encrypt several plaintext objects and record their power usage. Next, attack small parts of the key (subkeys) by considering every possible combination and calculating the Pearson correlation coefficient between the modeled and actual power. Finally, put together the best subkey to obtain the full
 - key.



Attack and Threat Terms(4)


- The following are the terms and definitions of different attacks or malevolent cyber threats:
 - **Dictionary attack:** A method of gaining entry to a network system by systematically entering words from a dictionary file containing the username and password pairs.
 - **Distributed Denial of Service (DDoS):** An attack attempting to disrupt or make an online service unavailable by overwhelming it from multiple (distributed) sources.
 - **Fuzzing:** A fuzzing attack consists of sending malformed or non-standard data to a device and observing how the device reacts. For example, if a device performs poorly or shows adverse effects, the fuzz attack may have exposed a weakness.



Attack and Threat Terms(5)

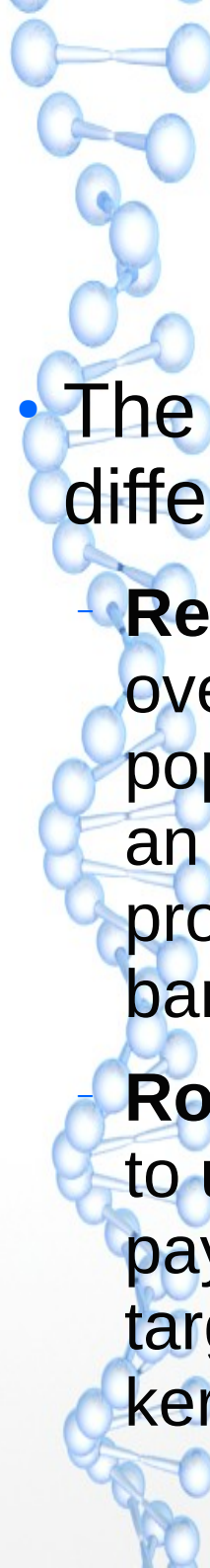
- The following are the terms and definitions of different attacks or malevolent cyber threats:

- **Man-in-the-Middle Attack (MITM):** A common form of attack that places a device in the middle of a communication stream between two unsuspecting parties. The device listens, filters, and appropriates information from the transmitter and retransmits selected information to the receiver. A MITM may be in the loop acting as a repeater or can be sideband listening to the transmission without intercepting the data.
- **NOP sleds:** A sequence of injected NOP assembly instructions used to "slide" a CPU's instruction pointer to the desired area of malicious code. Usually part of a buffer overflow attack.
- **Replay attack (also known as a playback attack):** A network attack where data is maliciously repeated or replayed by the originator or an adversary who intercepts the data, stores the data, and transmits it at will.




Attack and Threat Terms(6)

- The following are the terms and definitions of different attacks or malevolent cyber threats:
 - **RCE exploit:** Remote code execution that enables an attacker to execute arbitrary code. This usually comes in the form of a buffer overflow attack over HTTP or other network protocols that injects malware code.
 - **Return-Oriented Programming (ROP Attack):** This is a difficult security exploit an attacker may use to potentially subvert protections with non-executing memory or executing code from read-only memory. If an attacker gains control of a process stack through a buffer overflow or some other means, they may jump to legitimate and unchanged sequences of instructions already present. The attacker looks for sequences of instructions to call gadgets that can be pieced together to form a malevolent attack.



Attack and Threat Terms(7)

- The following are the terms and definitions of different attacks or malevolent cyber threats:
 - **Return-to-libc:** A type of attack that starts with a buffer overflow where the attacker injects jumps to libc or other popularly used libraries in the processes' memory space in an attempt to call system routines directly. Bypasses the protection offered by non-executable memory and guard bands. This is a specific form of ROP attack.
 - **Rootkit:** Typically malicious software (although often used to unlock smartphones) used to enable other software payloads to be undetectable. Rootkits use several targeted techniques such as buffer overflows to attack kernel services, hypervisors, and user mode programs.



Attack and Threat Terms(8)

- The following are the terms and definitions of different attacks or malevolent cyber threats:
 - **Side Channel Attack:** An attack used to gain information from a victim's system by observing the secondary effects of the physical system rather than find runtime exploits or zero-day exploits. Examples of side channel attacks include correlation power analysis, acoustic analysis, and reading data residue after it has been deleted from memory.
 - **Spoofing:** Malicious party or device impersonates another device or user on a network.
 - **SYN flood:** Occurs when a host sends a TCP:SYN packet which a rogue agent will spoof and forge. This will cause the host to create half-open connections to many non-existent addresses causing the host to exhaust all resources.
 - **Zero-Day exploits:** Security defects or bugs in commercial or production software unknown to the designer or manufacturer.



Defence Terms

- The following are the terms and definitions of different cyber defense mechanisms and technologies:
 - **Address Space Layout Randomization:** Also known as ASLR, this defense mechanism protects memory and thwarts buffer overflow attacks by randomizing where an executable is loaded in memory. A buffer overflow injecting malware can not predict where it will be loaded in memory, thus manipulating the instruction pointer will becomes extremely challenging. Protects against return-to-libc attacks.



Defence Terms(2)

- The following are the terms and definitions of different cyber defense mechanisms and technologies:
 - **Black hole (sinkhole):** After detecting a DDoS attack, routes are established from the affected DNS server or IP address to force rogue data to a black hole or a non-existent endpoint. Sinkholes perform further analysis to filter out good data.
 - **Data Execution Prevention (DEP):** Marks an area as executable or non-executable. This prevents an attacker from running code maliciously injected into such a region via a buffer overflow attack. The result is a system error or exception.
 - **Deep Packet Inspection (DPI):** A method of inspecting each packet (data and possibly header information) in a data stream to isolate intrusions, viruses, spam, and other criteria being filtered.



Defence Terms(3)

- The following are the terms and definitions of different cyber defense mechanisms and technologies:
 - **Firewall:** A network security construct that grants or rejects network access to packet streams between an untrusted zone and a trusted zone. Traffic can be controlled and managed through access control lists (ACL) on routers. Firewalls can perform stateful filtering and provide rules based on destination ports and traffic state.
 - **Guard bands and non-executable memory:** Protects regions of memory that are writeable and not executable. Protects against NOP sleds. Intel: NX bit, ARM XN bit.
 - **Honeypots:** Security tool to detect, deflect, or reverse engineer malicious attacks. Honeypots appear as legitimate websites or accessible nodes in a network but are actually isolated and monitored. Data and interactions with the device are logged.



Defence Terms(4)

- The following are the terms and definitions of different cyber defense mechanisms and technologies:
 - **Instruction-Based Memory Access Control:** A technique to separate the dataportion of a stack from the return address portion. This technique helps protect against ROP attacks and is particularly useful in constrained IoT systems.
 - **Intrusion Detection System (IDS):** A network construct to detect threats in anetwork through the out-of-band analysis of the packet stream therefore not in-line with the source and destination so as to affect real-time response.
 - **Intrusion Prevention System:** Blocks threats to a network via true in-line analysis and statistical or signature detection of threats.
 - **Milkers:** A defensive tool that emulates an infected botnet device and attaches to its malevolent host allowing one to understand and "milk" the malware commands being sent to the controlled botnet.



Defence Terms(5)

- The following are the terms and definitions of different cyber defense mechanisms and technologies:
 - **Port scanning:** A method to find an open and accessible port on a local network.
 - **Public Key Infrastructure (PKI):** Provides a definition of hierarchies of verifiers to guarantee the origin of a public key. A certificate is signed by certificate authorities.
 - **Public key:** A public key is generated with a private key and is accessible to external entities. A public key can be used to decrypt hashes.
 - **Private key:** A private key is generated with a public key, never released externally, and stored securely. It is used to encrypt hashes.



Defence Terms(6)

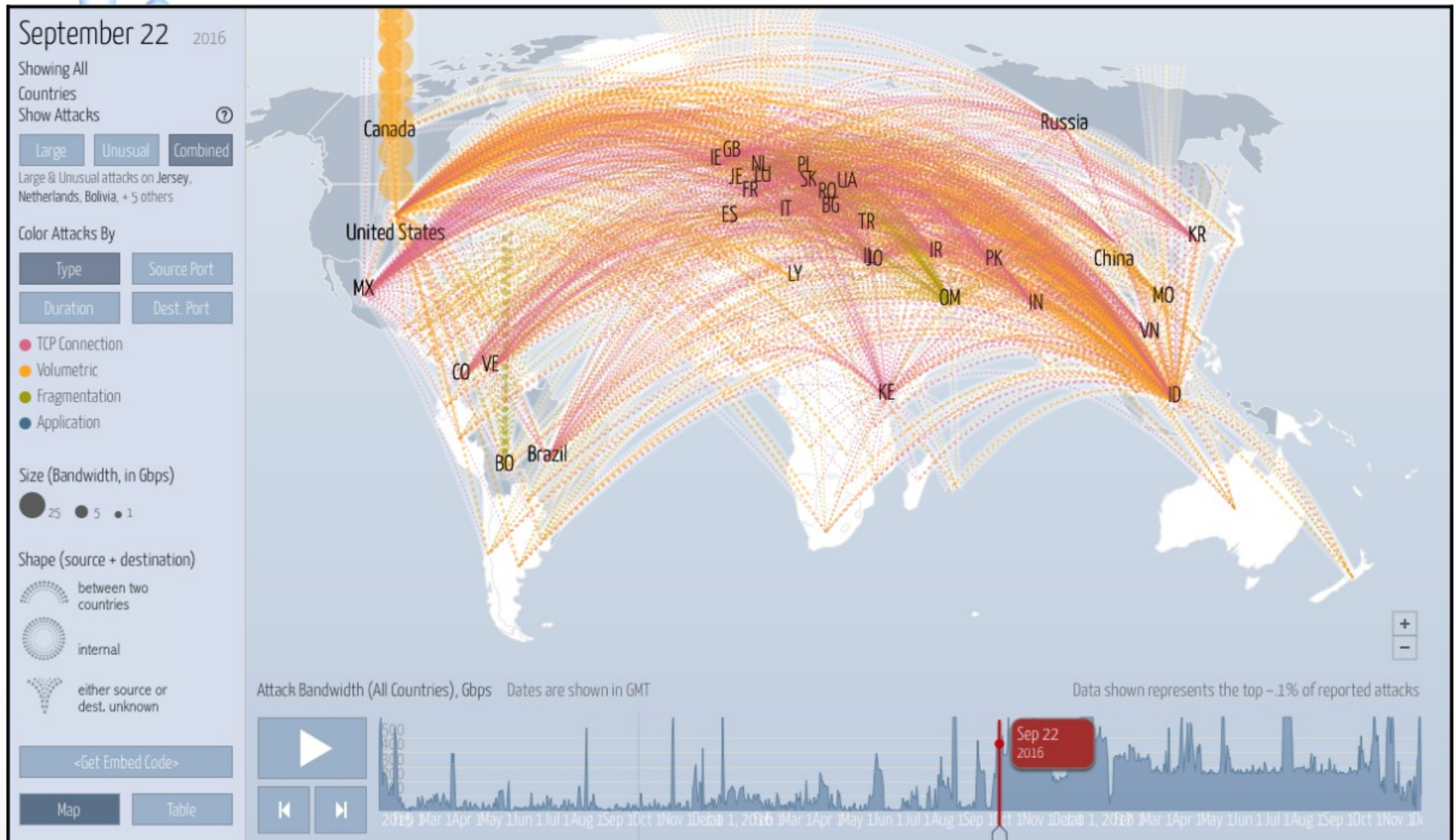
- The following are the terms and definitions of different cyber defense mechanisms and technologies:
 - **Root of Trust (RoT):** Starts execution on a cold booting device from an immutable trusted source of memory (such as ROM). If early boot software/BIOS can be changed without control, then no Root of Trust exists. The Root of Trust is usually the first phase in a multi-phase secure boot.
 - **Secure Boot:** A series of boot steps for a device that starts at a Root of Trust and proceeds through OS and application loading where each component signature is verified as authentic. Verification is performed through public keys loaded at previous trusted boot stages.
 - **Stack canaries:** Guards process stack space from stack overruns and prevents the execution of code from a stack.
 - **Trusted Execution Environment:** A secure area of a processor that ensures code and data residing within this zone is protected. This is usually an execution environment on the main processor core where the code for secure booting, monetary transfers, or private key handling will be executed with a higher level of security than the majority of the code.



IoT Attack

- Three forms of prevalent attacks:
 - **Mirai:** The most damaging denial of service attack in history that spawned from insecure IoT devices in remote areas.
 - **Stuxnet:** A nation-state cyber weapon targeting industrial SCADA IoT devices controlling substantial and irreversible damage to Iran's nuclear program.
 - **Chain Reaction:** A research method to exploit PAN area networks using nothing but a lightbulb—no internet needed.

Mirai DDoS Attack

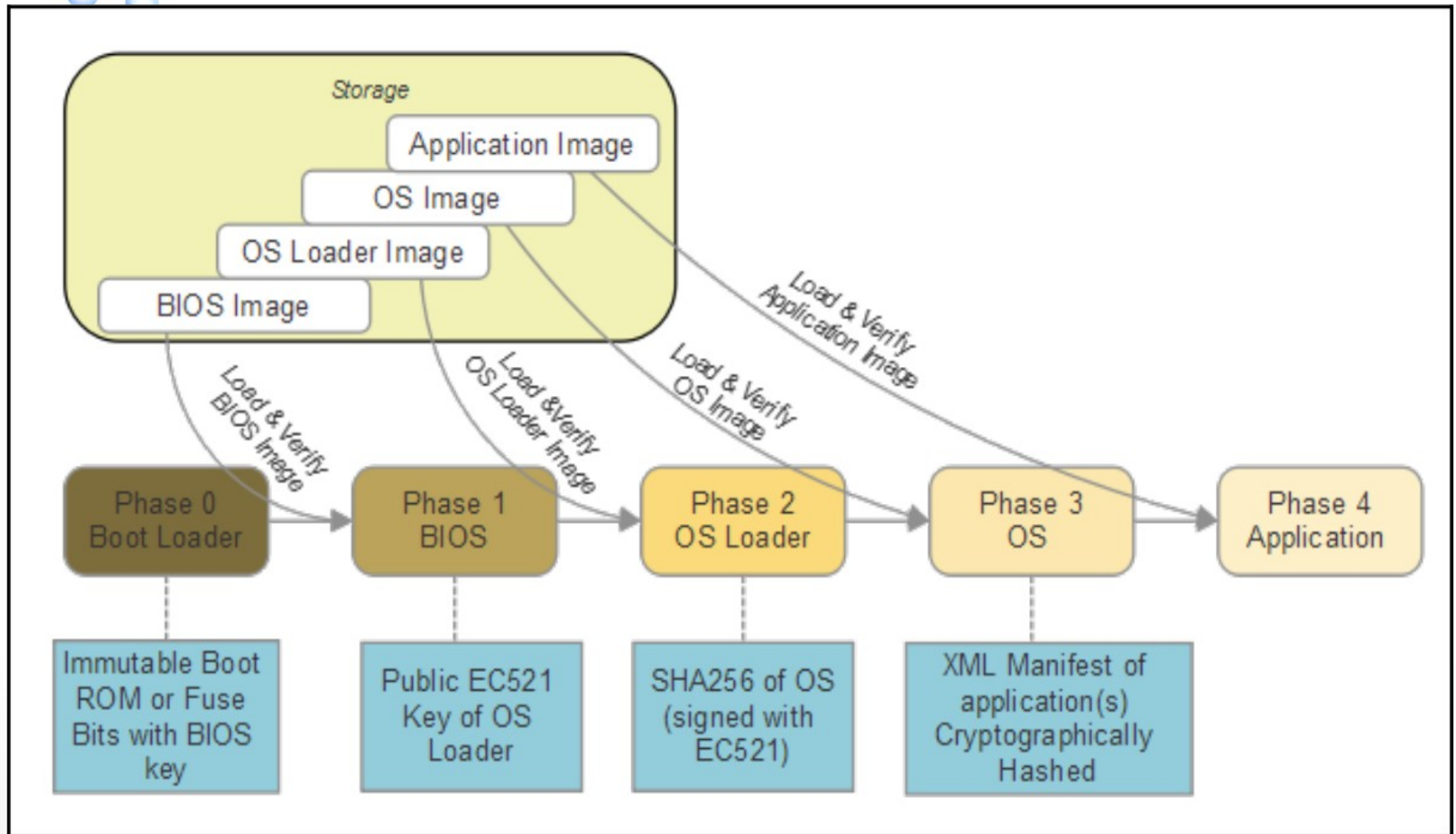




Physical and Hardware Security

- Root of Trust. An RoT can have different starting methods such as:
 - Boot from ROM or a non-writable memory to store the image and root key
 - One-time programmable memory using fuse bits for root key storage
 - Boot from a protected memory region that loads code into a protected memory store

Root of Trust





Root of Trust in ARM

- ARM TrustZone: ARM sells a security silicon IP block for SOC manufacturers that provides a hardware Root of Trust as well as other security services.
- TrustZone divides hardware into secure and non-secure "worlds". TrustZone is a separated microprocessor from the non-secure core.
- It runs a Trusted OS specially designed for security that has a well-defined interface to the non-secure world. Protected assets and functions reside in the trusted core and should be lightweight by design.
- The switching between worlds is done through hardware context switching, eliminating the need for secure monitor software. Other uses for TrustZone are to manage system keys, credit card transactions, and Digital Rights Management.
- TrustZone is available for A "application" and M "microcontroller" CPUs. This form of secure CPU, Trusted OS, and RoT is called a Trusted Execution Environment (TEE).



Root of Trust in Intel

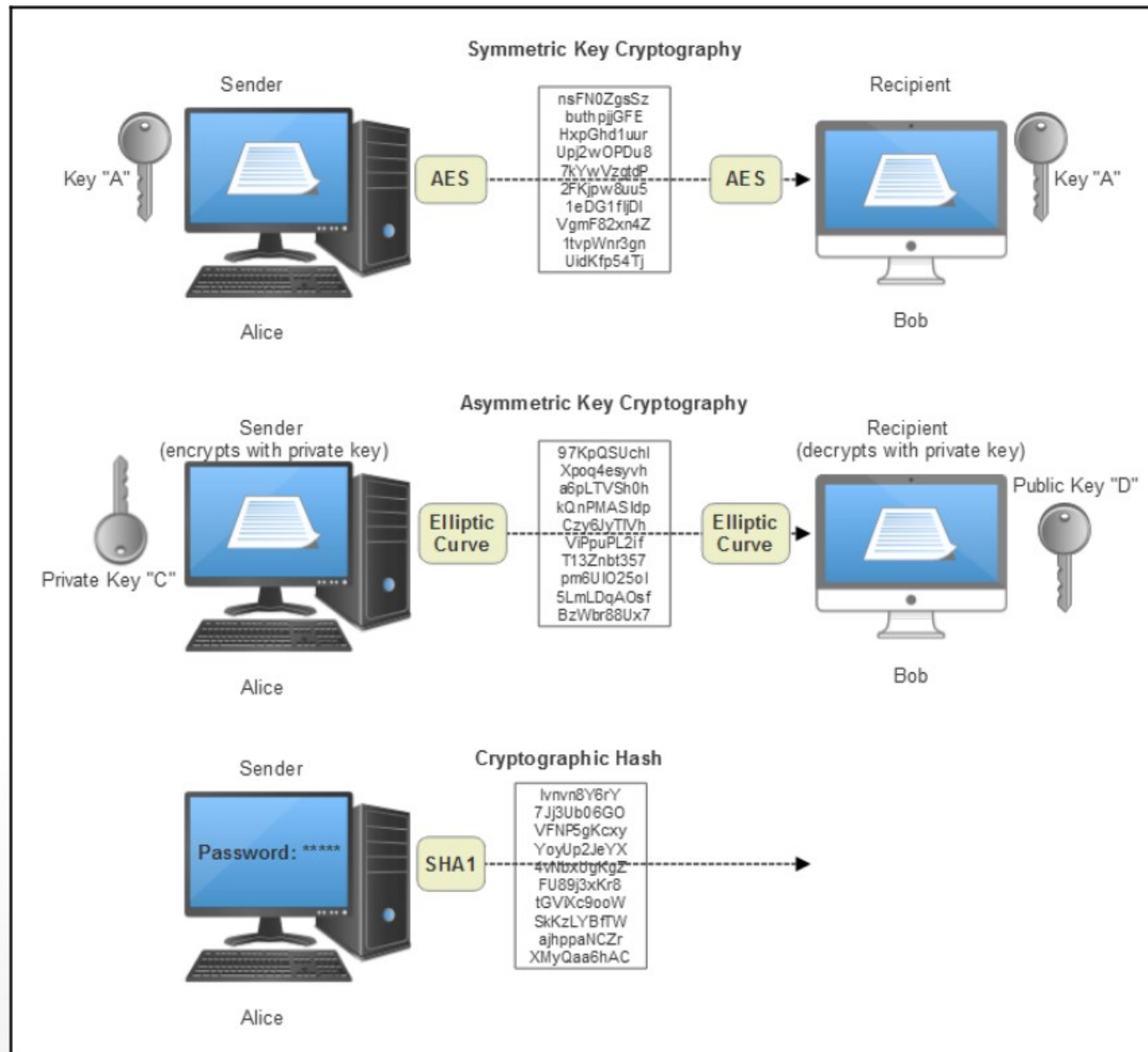
- Intel Boot Guard: This is a hardware-based mechanism that provides a verified boot which cryptographically verifies the initial boot block or uses a measuring process for validation.
- Boot Guard requires a manufacture to generate a 2048-bit key for verifying the initial block. The key is split into a private and public portion.
- The public key is imprinted by programmatically "blowing" fuse-bits during manufacturing. These are one-time fuses and immutable.
- The private portion generates the signature of the subsequently verified portion of the boot phase.



Cryptography

- **Symmetric key encryption:** Encryption and decryption keys are identical. RC5, DES, 3DES, and AES are all forms of symmetric key encryption.
- **Public Key encryption:** Encryption key is published publicly for anyone to use and encrypt data. Only the receiving party has a private key used to decrypt the message. This is also known as asymmetric encryption. Asymmetric cryptography manages data secrecy, authenticates participants, and forces non-repudiation. Well-known internet encryption and message protocols such as Elliptic Curve, PGP, RSA, TLS, and S/MIME are considered public keys.
- **Cryptographic hash:** Maps data of an arbitrary size to a bit string (called the digest). This hash function is designed to be "one way". Essentially, the only way to recreate the output hash is to force every possible input combination (it cannot be run in reverse). MD5, SHA1, SHA2, and SHA3 are all forms of one-way hashes.

Cryptography(2)





Blockchain and Cryptocurrency in IoT

- Blockchains are public, digital, and decentralized ledgers or cryptocurrency transactions.
- The original cryptocurrency blockchain was Bitcoin but there are over 700 new currencies on the market such as Ethereum, Ripple, and Dash.
- The power of a blockchain is that there is no single entity controlling the state of transactions.



Blockchain and Cryptocurrency in IoT

- Blockchain secure cryptocurrencies are particularly relevant to IoT. Some example use cases include:
 - **Machine to machine payments:** The IoT needs to ready itself for machine exchanging services for currency.
 - **Supply chain management:** In this case, the movement and logistics in managing inventory, moving goods, and logistics can replace paper-based tracking with blockchain immutability and security. Every container, movement, location, and state can be tracked, verified, and certified. Attempts to forge, delete, or modify tracking information becomes impossible.
 - **Solar energy:** Imagine residential solar as a service. In this case, solar panels installed on a customer home are generating energy for the home. Alternatively, they can also send energy back to the grid to power someone else (perhaps in exchange for carbon credits).



Summary

- This chapter detailed the risks of security in the IoT. With well-known attacks such as Mirai and Stuxnet, which target IoT devices as their intended hosts, architects should design security into an IoT deployment from the start.
- The IoT makes for the best play space to launch an attack. The systems are usually less security mature than server and PC systems.
- IoT security threats need to be taken seriously, as the ramifications could have a pronounced impact on a device, a city, or a nation.