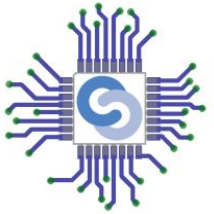


Embedded Systems Laboratory

Internet of Things

Lecture 6 - Security Attacks in IoT

Attacks against IoT

- Attacks against IoT critical apps
- Remote location, unsupervised
  - modify & destroy nodes
- Resource constrained
  - easily compromised
- Connected to the Internet
- Security solutions
  - No CPU intensive solutions
  - Lightweight solutions

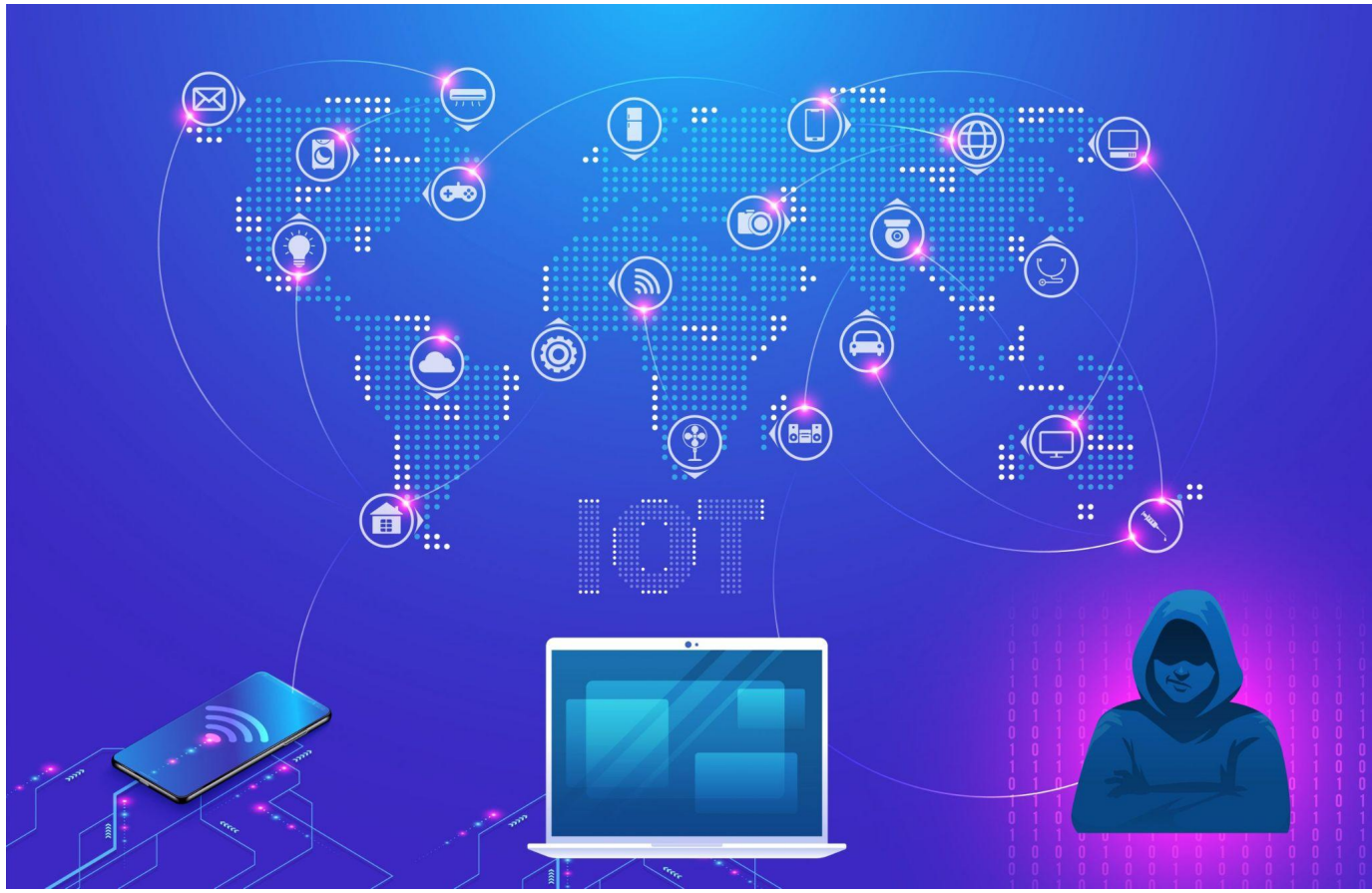
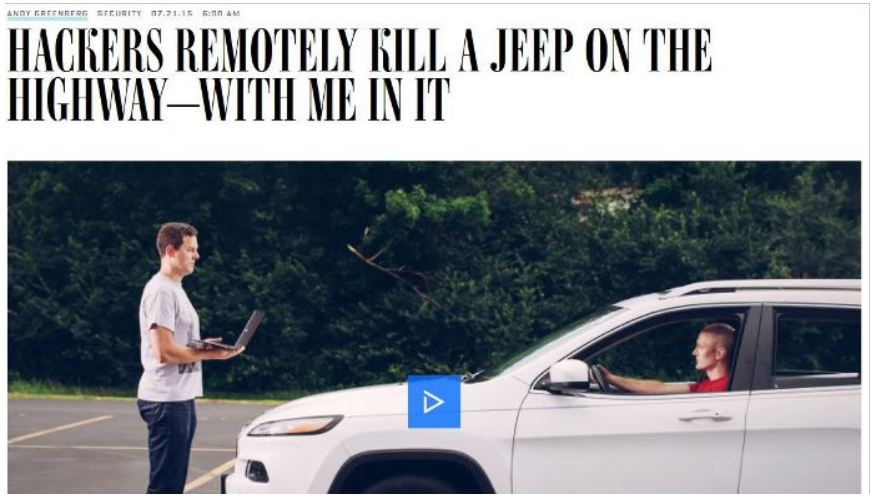


Image source: https://www.einfochips.com/blog/botnet-attacks-how-iot-devices-become-part-victim-of-such-attacks/

Attacks against IoT

Log4j zero-day flaw: What you need to know and how to protect yourself

The Log4j vulnerability affects everything from the cloud to developer tools and security devices. Here's what to look for, according to the latest information.



IoT Botnet – DDoS attack

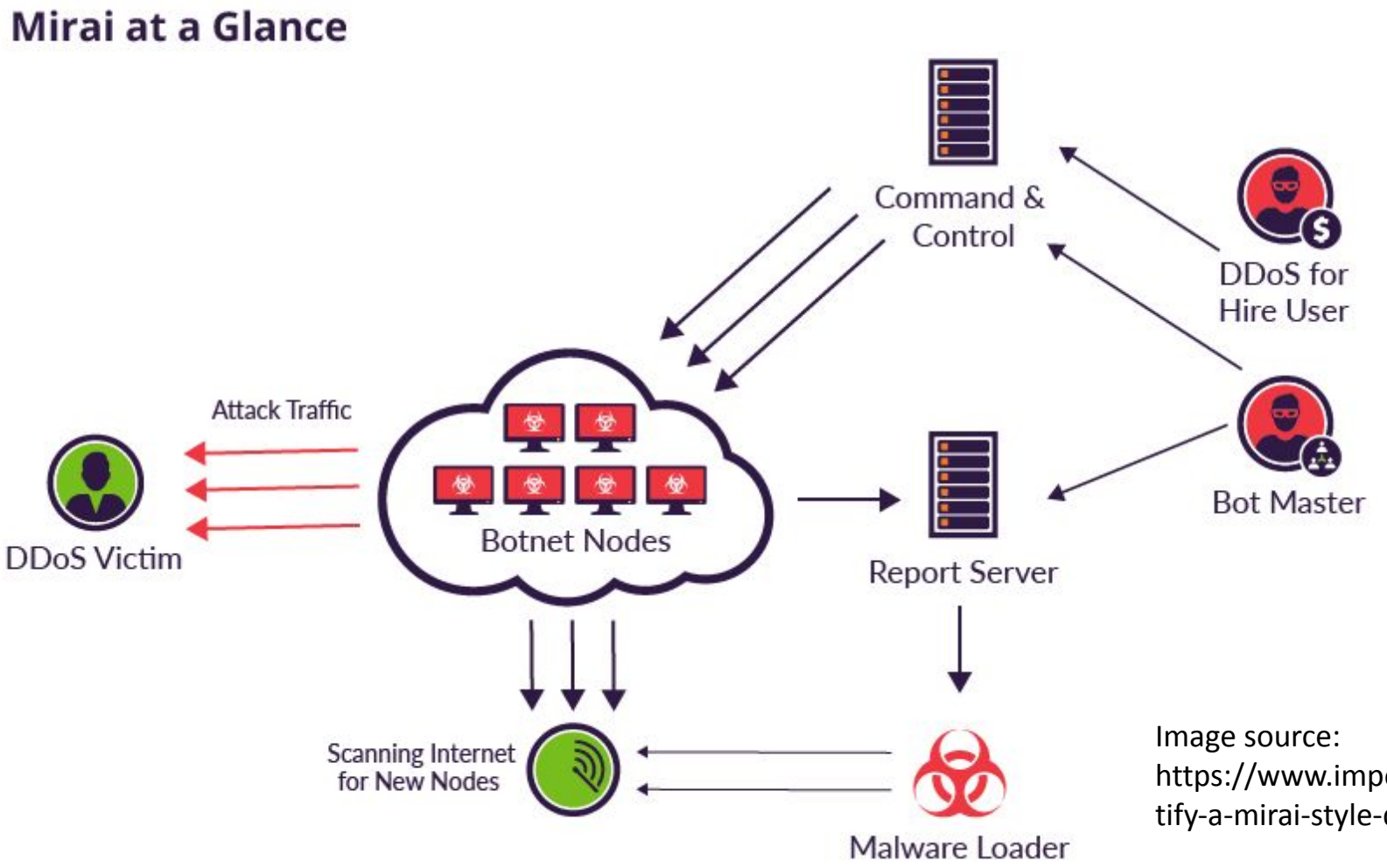
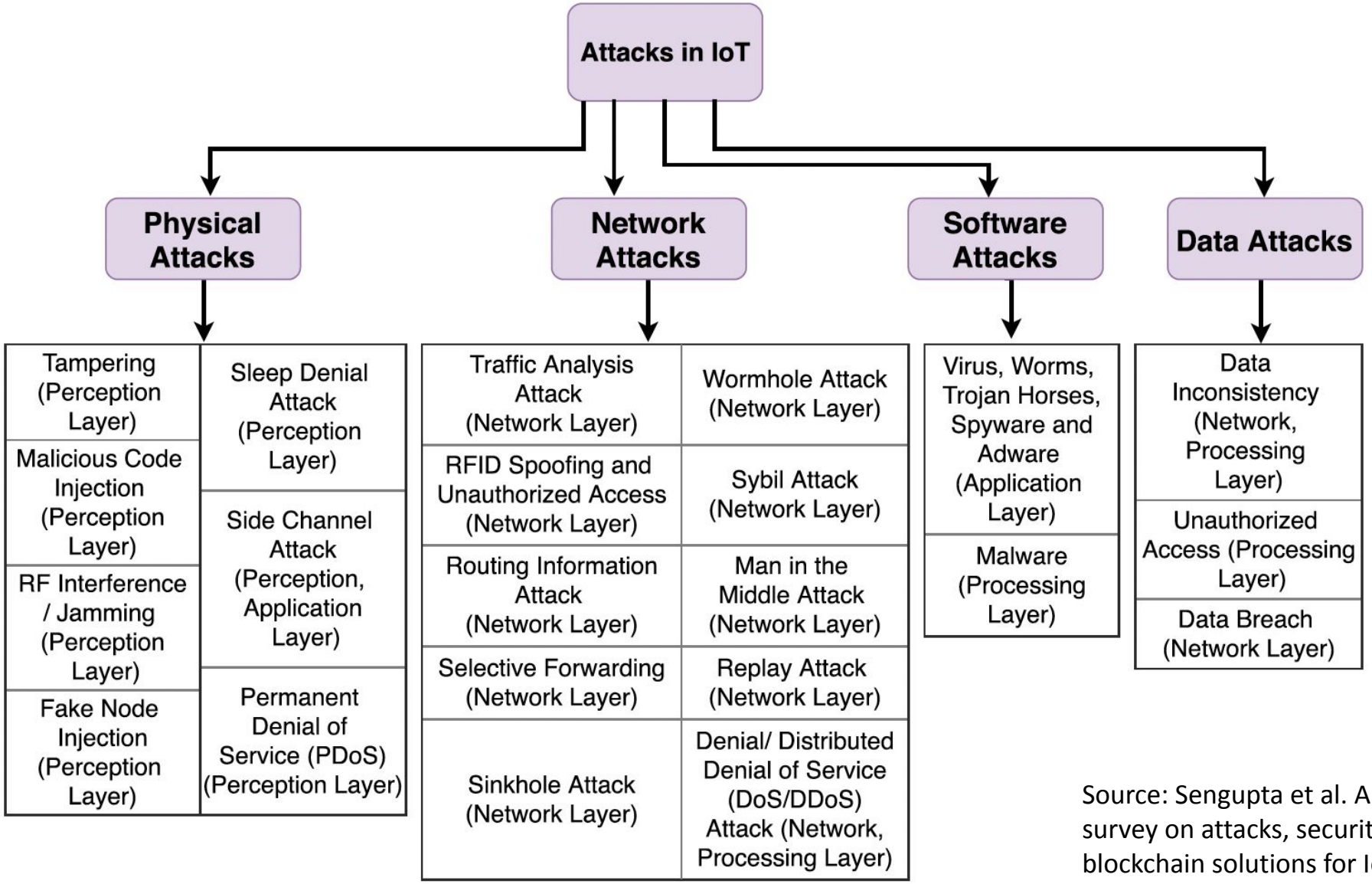


Image source: https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/

Attacks classification



Source: Sengupta et al. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT.

Physical Attacks

- Attacker is in the proximity of the devices
- Tampering
  - Physical modification
  - Device, communication channel
- Malicious Code Injection
  - Inject malicious code
  - Modify node behavior
  - Launch other attacks

Physical Attacks

- RF Interference/Jamming
  - Generate noise on the wireless channel
  - Prevent the device from communicating
  - DoS
- Fake Node Injection
  - Insert a malicious node
  - Capture traffic
  - Launch other attacks

Physical Attacks

- Sleep Denial Attack
  - Duty cycling
  - Prevent nodes from sleeping
  - Deplete battery
  - DoS
- Permanent Denial of Service (PDoS)
  - Phlashing
  - Destroy/disable device
  - Firmare, BIOS corruption

Physical Attacks

- Side Channel Attack
  - Use external information to learn about the implementation
  - Attack the physical effects of an implementation
  - Passive:
    - Power analysis attack
    - Electromagnetic analysis attack
  - Active:
    - Electromagnetic fault injection
    - Temperature variation

Physical attacks, effects and countermeasures.

Attack Name	Effects	Countermeasures Proposed	Countermeasure References
Tampering and Malicious Code Injection	Access to sensitive information and Gain access; DoS	PUF based Authentication	Aman et al. (2017)
RF Interfer-ence/Jamming	DoS; Hinder/Jam Communication	CUTE Mote	Gomes et al. (2017)
Fake Node Injection	Control data flow; Man in the Middle	PAuthKey	Porambage et al. (2014)
Sleep Denial	Node shutdown	CUTE Mote; Support Vector Machine (SVM)	Gomes et al. (2017) and Hei et al. (2010)
Side Channel Attack	Collect Encryption Keys	Masking technique; Authentication using PUF	Aman et al., 2017 and Choi and Kim (2016)
Permanent Denial of Service (PDoS)	Resource Destruction	NOS Middleware	Sicari et al. (2018)

Countermeasures against Physical Attacks

Source: Sengupta et al. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT.

Network Attacks

- Traffic Analysis Attack
  - intercept packets
  - steal private information
- RFID Spoofing
  - steal RFID tag information
  - spoof RFID packets
- RFID Unauthorized Access
  - read/modify/delete data
  - lack of authentication

Network Attacks

- Routing Information Attacks
  - falsify/modify routing information
  - routing loops
  - fake routing messages
  - compromise routing protocol
- Selective Forwarding
  - route only some packets, drop packets, modify packets
  - data that reaches the destination is incomplete
  - compromises communication

Network Attacks

- Sinkhole Attack
  - propagate fake routing info
  - pose itself as gateway/sink
  - all traffic go through that node
- Wormhole Attack
  - low latency link for tunneling packets
  - to a distant part of the network
  - compromise routing protocol

Network Attacks

- Sybil Attack
  - asume multiple identities and locations
  - compromise network, routing protocol
  - unfair resource allocation
- Man in the Middle (MitM) Attack
  - intercept and modify traffic between 2 entities
  - extract private information
  - modify packets

Network Attacks

- Replay Attack
  - retransmit some intercepted packets
  - overload network, DoS
- Denial of Service (DoS) Attack
  - disrupt normal functionality
  - target network, devices, application
- Distributed Denial of Service (DDoS) Attack
  - carried by multiple malicious nodes
  - target server, other device, the whole network

Countermeasures against Network Attacks

Network attacks, effects and countermeasures.

Attack Name	Effects	Countermeasures Proposed	Countermeasure References
Traffic Analysis Attack	Data Leakage (Network Information)	Privacy preserving traffic obfuscation framework	Liu et al. (2018)
RFID Spoofing and Unauthorized Access	Data Manipulation and Modification (Read, Write, Delete)	SRAM based PUF	Guin et al. (2018)
Routing Information Attacks	Routing Loops	Hash Chain Authentication;	Glissa et al. (2016)
Selective Forwarding	Message Destruction	Hash Chain Authentication; Monitor based approach	Glissa et al. (2016) and Pu and Hajjar (2018)

Source: Sengupta et al. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT.

Countermeasures against Network Attacks

Network attacks, effects and countermeasures.

Attack Name	Effects	Countermeasures Proposed	Countermeasure References
Sinkhole Attack	Data alteration or leakage	Hash Chain Authentication; Intrusion Detection	Glissa et al. (2016) and Cervantes et al. (2015)
Wormhole Attack	Packet tunneling	Clustering based Intrusion Detection System	Shukla (2017)
Sybil Attack	Unfair resource allocation; Redundancy	Trust aware Protocol	Airehrour et al. (2019)
Man in the Middle Attack	Data Privacy violation	Secure MQTT; Inter-device Authentication	Singh et al. (2015) and Park and Kang (2015)
Replay Attack	Network congestion; DoS	Signcryption	Ashibani and Mahmoud (2017)
DoS/DDoS Attack	Network Flooding; Network Crash	EDoS Server; SDN based IoT framework	Adat and Gupta (2017) and Yin et al. (2018)

Source: Sengupta et al. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT.

Software Attacks

- Exploit software vulnerabilities
- Malicious applications
  - viruses, worms, trojans, spyware
  - adware, backdoors, rootkits
- Actions
  - Steal sensitive information
  - Modify and destroy data
  - Disable devices, affect system functionality
  - Infect Cloud apps
- Hardware trojans - modified integrated circuits

Countermeasures against Software Attacks

Software attacks, effects and countermeasures.

Attack Name	Effects	Countermeasures Proposed	Countermeasure References
Virus, Worms, Trojan Horses, Spyware and Adware	Resource Destruction	Lightweight framework; High Level Synthesis (HLS)	Liu et al., 2016 and Konigsmark et al. (2016)
Malware	Infected Data	Malware Image Classification; Lightweight Neural Network Framework	Naeem et al. (2018) and Su et al. (2018)

Source: Sengupta et al. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT.

Data Attacks

- Data collected by IoT nodes and stored in Cloud
- Data Inconsistency
  - Attack on data integrity
  - Data in tranzit or stored data
- Unauthorized Access
  - Data access, data ownership without authorization
- Data Breach/Memory Leak
  - disclosure of sensitive, confidential data

Countermeasures against Data Attacks

Data attacks, effects and countermeasures.

Attacks	Effects	Countermeasures Proposed	Countermeasure References
Data Inconsistency	Data Inconsistency	Chaos based scheme; Blockchain architceture	Song et al. (2017) and Machado and Fröhlich (2018)
Unauthorized Access	Violation of Data Privacy	Blockchain-based ABE; Privacy Preserving ABE	Rahulamathavan et al. (2017) and Zheng et al. (2018)
Data Breach	Data Leakage	Two Factor Authentication; DPP; ISDD	Gope and Sikdar (2018), Gai et al. (2018) and Sengupta et al. (2019)

Source: Sengupta et al. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT.

Real-life Attacks

- Edimax IP Cameras (Ling et al., 2017)
  - device scanning, brute force, device spoofing
  - take control over cameras
  - device spoofing to obtain passwords
  - device scanning to identify online cameras
- Smart Home/Smart Metering Systems (Wurm et al., 2016)
  - brute force attacks to obtain passwords
  - meters used to launch ransomware attacks

Real-life Attacks

- Virtual Private Assistants - VPA (Zhang et al., 2018)
  - Amazon Echo and Google Home
  - third-parties may publish new skills (function)
  - attackers publish malicious skills
  - voice squatting
  - voice masquerading
- Attack on DNS Service provider called Dyn (more info)
  - DDoS - IoT Botnet
  - affected services of Twitter, Etsy, Github, Soundcloud, Spotify, Shopify, and Intercom
  - disrupted access to PayPal, BBC, Wall Street Journal, CNN, HBO Now, New York Times, Financial Times, etc.

Real-life Attacks

- Mirai IoT Botnet (more info)
  - Mirai infected devices searched for other vulnerable devices
  - used default passwords and infected other devices
  - shut down huge portions of the Internet
  - recommendations: change default passwords, security updates
- Jeep Hack (more info)
  - take total control of a Jeep SUV using the vehicle's CAN bus
  - exploiting a firmware update vulnerability
  - control the vehicle remotely
  - speed up, slow down, veer off the road

Tampering Attack Case Study

- Itron Centron CL200 smart meter
- Analyzed EEPROM & extracted Device ID
- Malicious meter
  - impersonates legitimate meter - uses the same ID
  - sends fake data
  - stealing from the utility company

Source: T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17-25, 2020.

Figure 2. (a) Itron Smart Meter (credit: Itron). (b) Compromised meter readings.

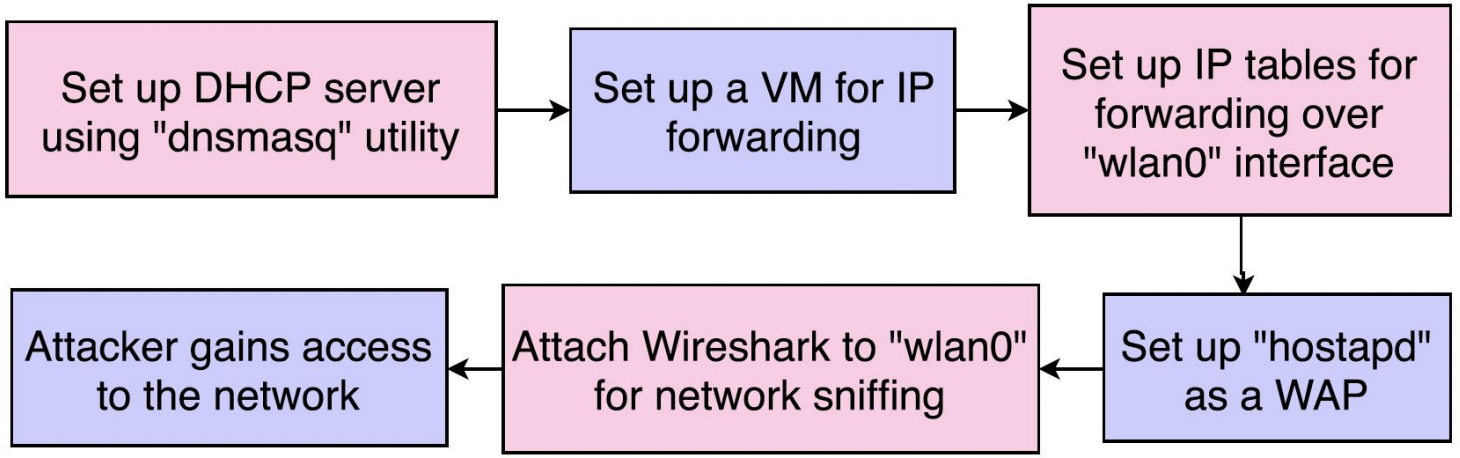
Tampering Attack Case Study

- Problem: EEPROM is vulnerable to illegitimate reading and writing
- Solution: PUFs to secure EEPROM data
  - digital fingerprint
  - allow only authenticated devices to modify data
  - challenge-response scheme
    - unique response for each challenge
  - unique identification
  - protection against tampering

Eavesdropping Attack Case Study

- Fitbit Aria Smart Scale
- Sends data through a wireless AP to the Fitbit server
- MitM attack using Kali Linux
  - DHCP server (dnsmasq tool) - assign IP address to device
  - VM & iptables - forward IP packets through wlan0
  - hostapd as virtual wireless AP - register device to it
  - acts as wireless AP and receives all packets from device
  - Wireshark on wlan0 to intercept packets
  - extract private data

Source: T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17-25, 2020.



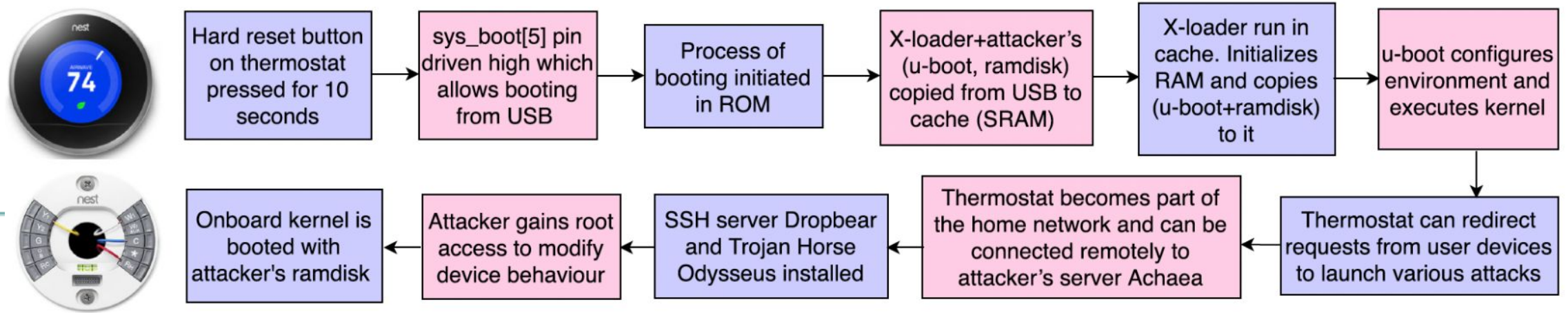
Eavesdropping Attack Case Study

- No encrypted communication channel with the server
- Attacker may steal the user's private data
  - Solution: encrypt traffic end-to-end
- Standard encryption methods may not be fit for resource-constrained devices
  - Solution: lightweight & robust encryption

Malicious Code Injection Case Study

- Google Nest Thermostat
- Exploit vulnerabilities in the boot process
  - hard reset - firmware update mode
  - upload custom images from USB in ROM
  - X-loader, u-boot (modified), ramdisk (custom)
  - modifies existing file system & obtains root access
  - Dropbear SSH server to obtain remote access on the device
  - Odysseus malware to connect to server

Source: T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17-25, 2020.



Malicious Code Injection Case Study

- Attackers gain remote root access to the device
- Device acts as a bot
- May gain access to other household devices
  - obtain private data, control devices
- Problem: no integrity verification of images loaded in ROM
- Solution: chain-of-trust based secure boot
  - special hardware is required

Malicious Node Insertion

- Edimax IP camera system
  - IP camera, controller, registration and command relay servers
  - each camera must register to a registration server before joining the network
- Infected IoT device (Mirai malware) - bot
- TCP SYN message to discover IP cameras in the network
- Bot registers to the server using the camera's MAC address
  - Bot impersonates the camera and registers to the server
- Bot sends TCP requests to server
  - Server responds with authentication information

Malicious Node Insertion

- Bot extracts password and has access to the camera
- Download a malware on the camera
- Propagate the malware in the network
  - Network of bots = Botnet
- 65000 IoT devices infected by Mirai in 20 hours
- Solution: identity management, symmetric encryption (secret key)

Bibliography

- Sengupta, Jayasree, Sushmita Ruj, and Sipra Das Bit. "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT." Journal of Network and Computer Applications 149 (2020): 102481. (pdf)
- T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17-25, 2020. (pdf)