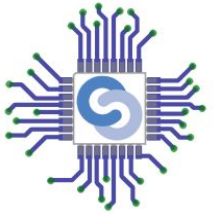


Embedded Systems Laboratory

Internet of Things

Lecture 7 - Security Attacks in IoT

Attacks against IoT

Attacks against IoT

IoT Sensor Node Crunch

Embedded Systems Laboratory

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.

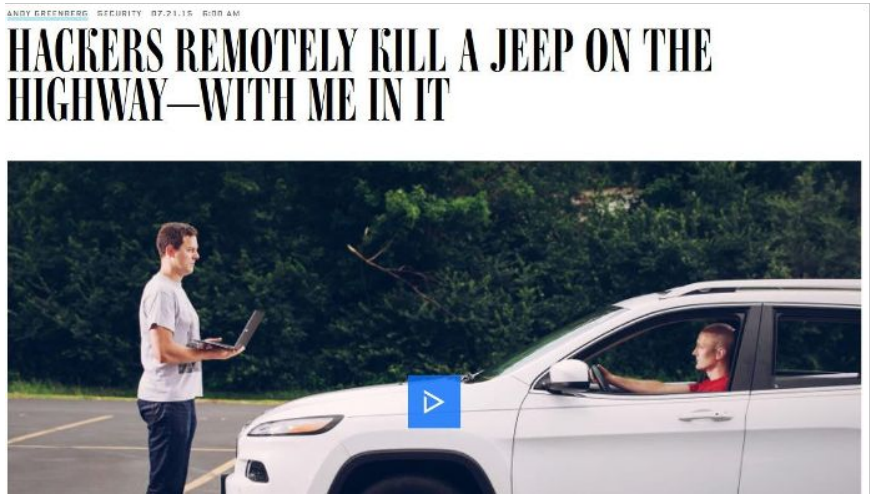
Written by **Liam Tung**, Contributor
on December 14, 2021 | Topic: **Security**

RELATED

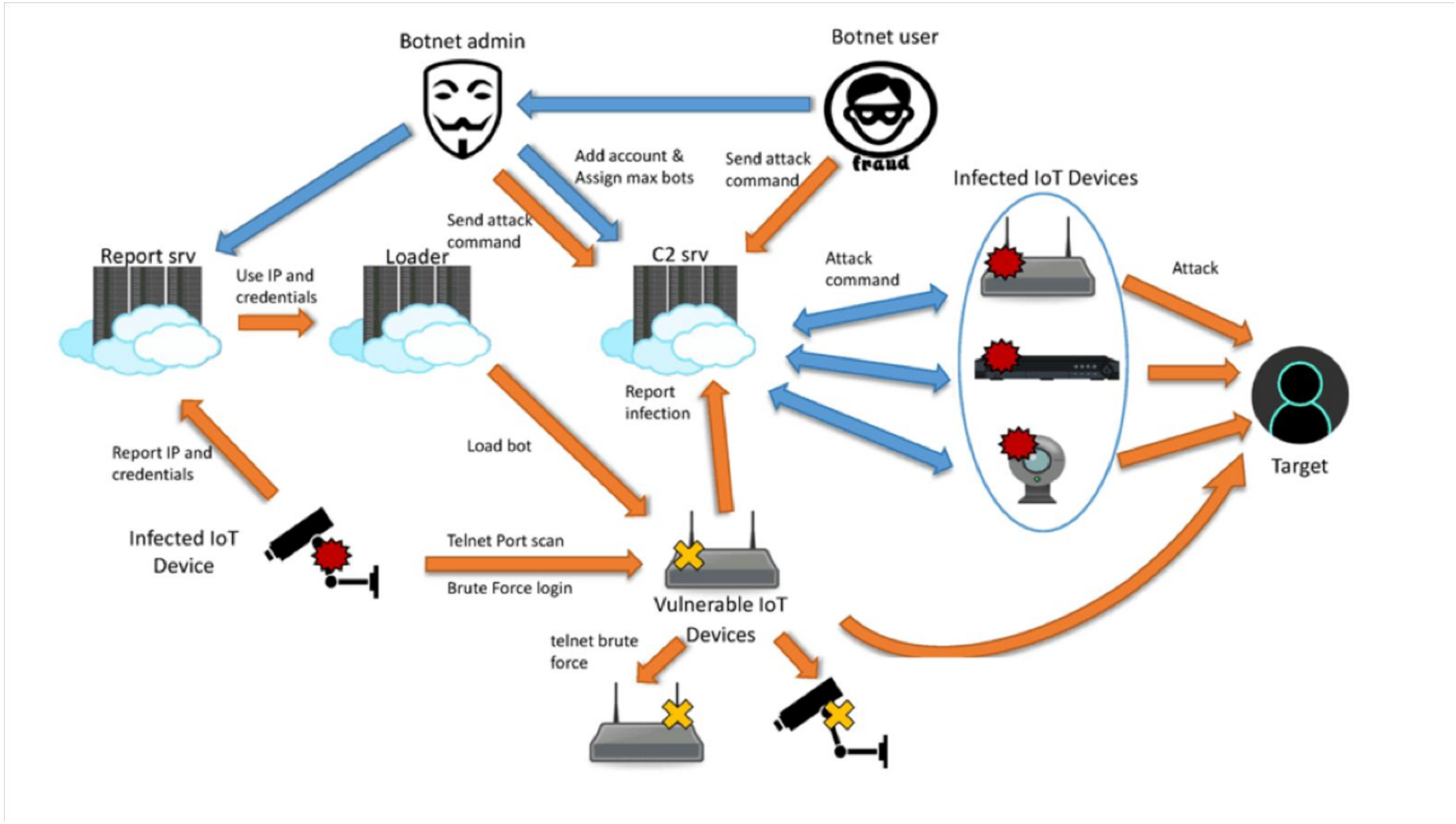
Meta targets user information, database scraping in bug bounty expansion

by Tom Spring

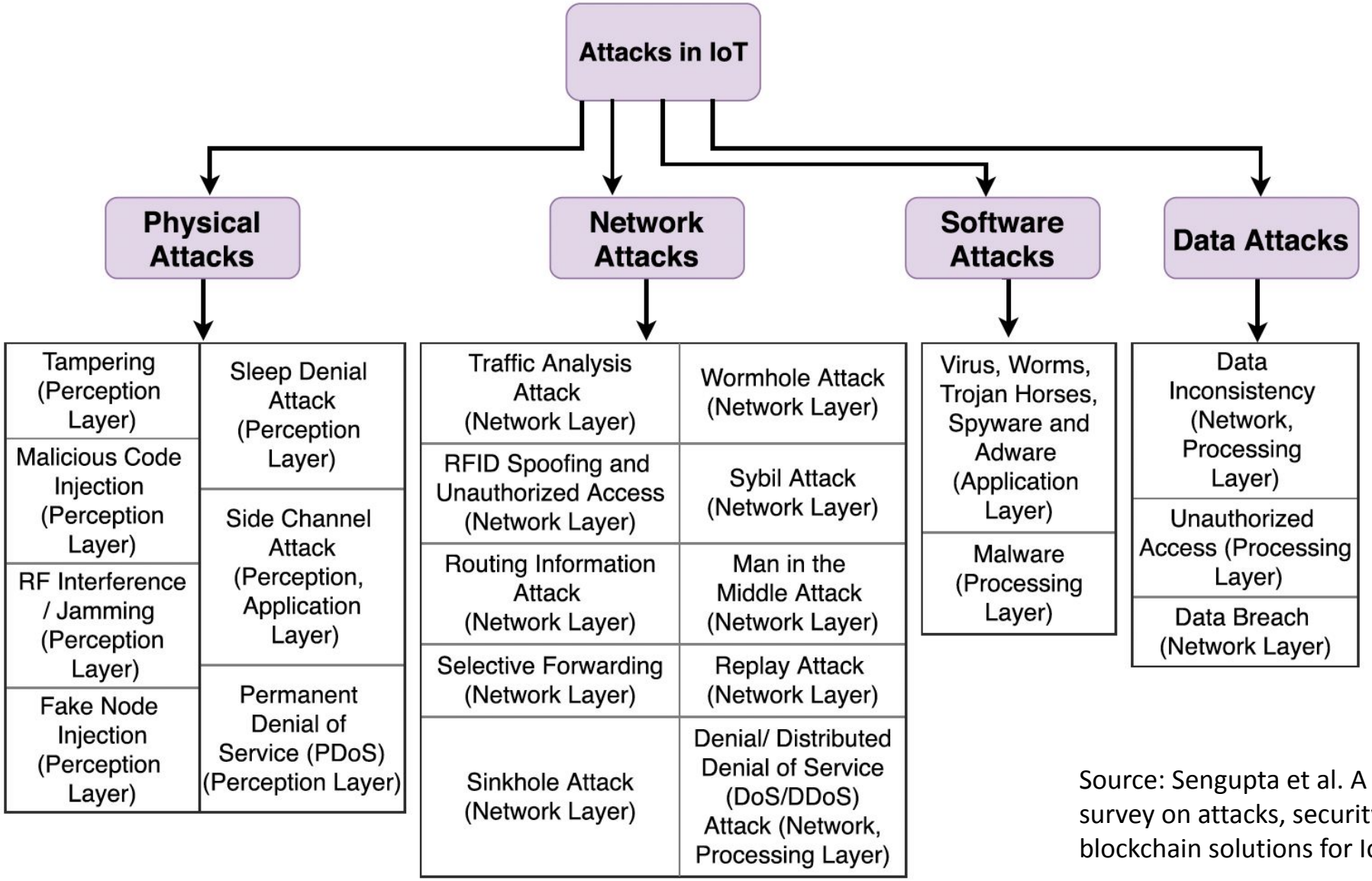
August 11, 2016 , 11:27 am



IoT Botnet – DDoS attack



Attacks classification



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

Physical Attacks

- Tampering
  - Physical modification
- Malicious Code Injection
  - Modify node behavior
- RF Interference/Jamming
  - Prevent the device from communicating
- Fake Node Injection
  - Capture traffic
  - Launch attacks

Physical Attacks

- Sleep Denial Attack
  - Prevent nodes from sleeping
  - Deplete battery
- Side Channel Attack
  - Attack the physical effects of an implementation
  - Power analysis attack
  - Electromagnetic analysis attack
  - Electromagnetic fault injection
  - Temperature variation
- Permanent Denial of Service (PDoS)
  - Phlashing
  - Destroy/disable device

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)

IoT Sensor Node Crunch

Embedded Systems Laboratory

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
- RFID Spoofing
  - steal RFID tag information
  - spoof RFID packets
- RFID Unauthorized Access
  - read/modify/delete data
  - lack of authentication
- Routing Information Attacks
  - falsify/modify routing information
- Selective Forwarding
  - route only some packets, drop others

Network Attacks

- Sinkhole Attack
  - pose itself as gateway/sink
- Wormhole Attack
  - low latency link for tunneling packets
- Sybil Attack
  - Asume multiple identities and locations
- Man in the Middle (MitM) Attack
  - Intercept and modify traffic

Network Attacks

- Replay Attack
  - retransmit some intercepted packets
  - overload network
- Denial of Service (DoS) Attack
  - disrupt normal functionality
  - target network, devices, application
- Distributed Denial of Service (DDoS) Attack
  - a type of DoS
  - carried by multiple nodes

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

- Exploits
- Viruses
- Worms
- Trojans
- Spyware
- Adware
- Backdoors
- Rootkits

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 Inconsistency
  - Attack on data integrity
  - Data in tranzit or stored data
- Unauthorized Access
  - Data access, data ownership without authorization
- Data Breach
  - 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

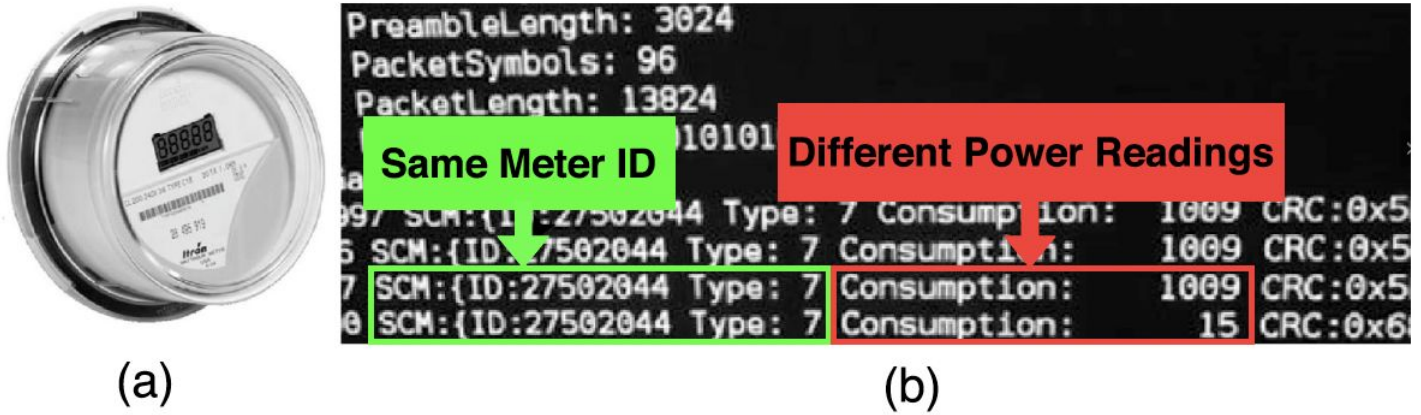
- Edimax IP Cameras (Ling et al., 2017)
  - device scanning, brute force, device spoofing
  - obtain passwords
  - take control over cameras
- Smart Home/Smart Metering Systems (Wurm et al., 2016)
  - brute force attacks to obtain passwords
  - smart meters launch attacks
- Virtual Private Assistants - VPA (Zhang et al., 2018)
  - Amazon Echo and Google Home
  - third-parties may publish new skills (function)
  - malicious skills
  - voice squatting
  - voice masquerading

Real-life Attacks

- Attack on DNS Service provider called Dyn (more info)
  - IoT Botnet
  - affected services of Twitter, Etsy, Github, Soundcloud, Spotify, Shopify, and Intercom
  - disrupted access to PayPal, BBC, Wall Street Journal, Xbox, CNN, HBO Now, Starbucks, New York Times, The Verge, and Financial Times
- 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
- Jeep Hack (more info)
  - take total control of a Jeep SUV using the vehicle's CAN bus
  - exploiting a firmware update vulnerability
  - 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
- EEPROM is vulnerable to illegitimate reading and writing
- Solution: PUFs
- Challenge-response scheme



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.

Eavesdropping Attack Case Study

- Fitbit Aria Smart Scale
- Sends data & statistics through a wireless AP to the Fitbit server
- MitM attack using Kali Linux
- Attacker obtains SSID & shared key
- Connects to user's network
- May steal private information
- Solution: encrypted communication channel to server
- Lightweight & robust encryption

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.

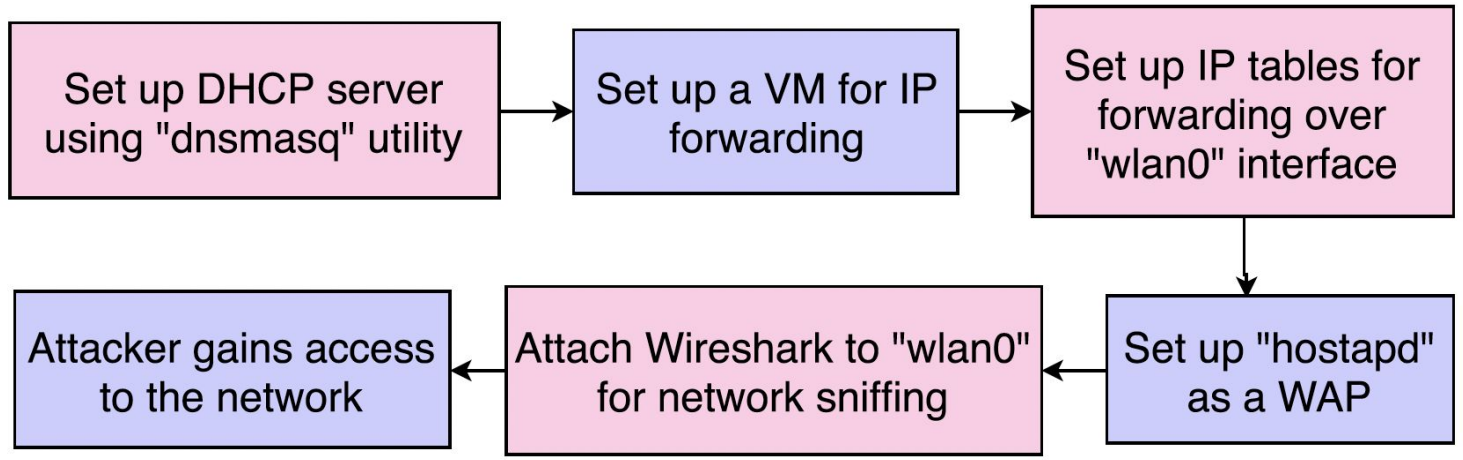


Figure 3. Attack vector on Fitbit aria.

Malicious Code Injection Case Study

- Google Nest Thermostat
- Vulnerabilities in the boot process
- Attackers gain remote access to the device
- May gain access to the home network
- Solution: chain-of-trust based secure boot
- Hardware for secure boot

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.

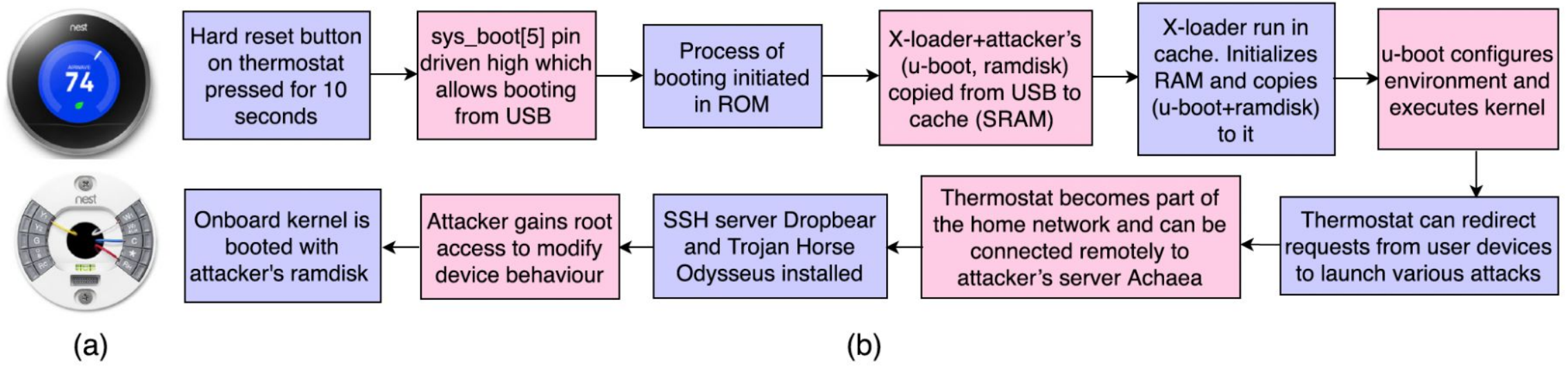


Figure 4. (a) Nest thermostat front (upper image) and back (lower image) plates (credit: Nest). (b) Attack flow.

Malicious Node Insertion

- Edimax IP camera system
  - IP camera, controller, registration and command relay servers
- Infected IoT device (Mirai malware) - bot
- TCP SYN message to guess MAC address
- Bot impersonates the camera and registers to the server
- Bot sends TCP requests to command relay server
- Server responds with authentication information
- Attacker gains access to the IP camera
- Botnet
- Solution: identity management, encryption

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)