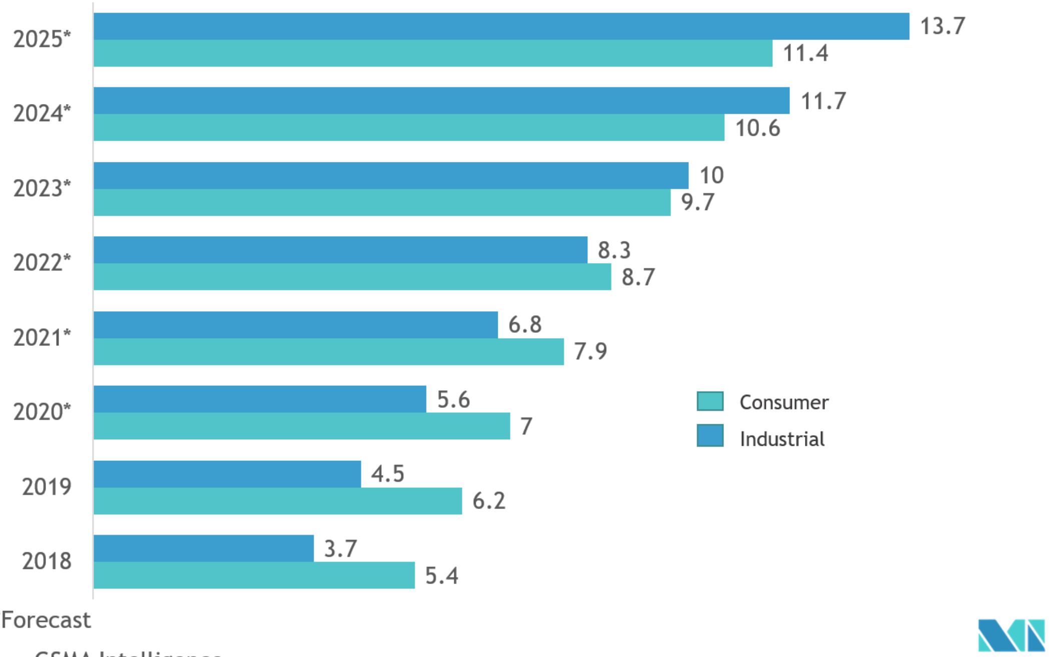
Consumer IoT Device Security

IoT Consumer Market

Number of Industrial and Consumer IoT Connected Objects,
In billions, Global in 2016, 2017, and 2021*

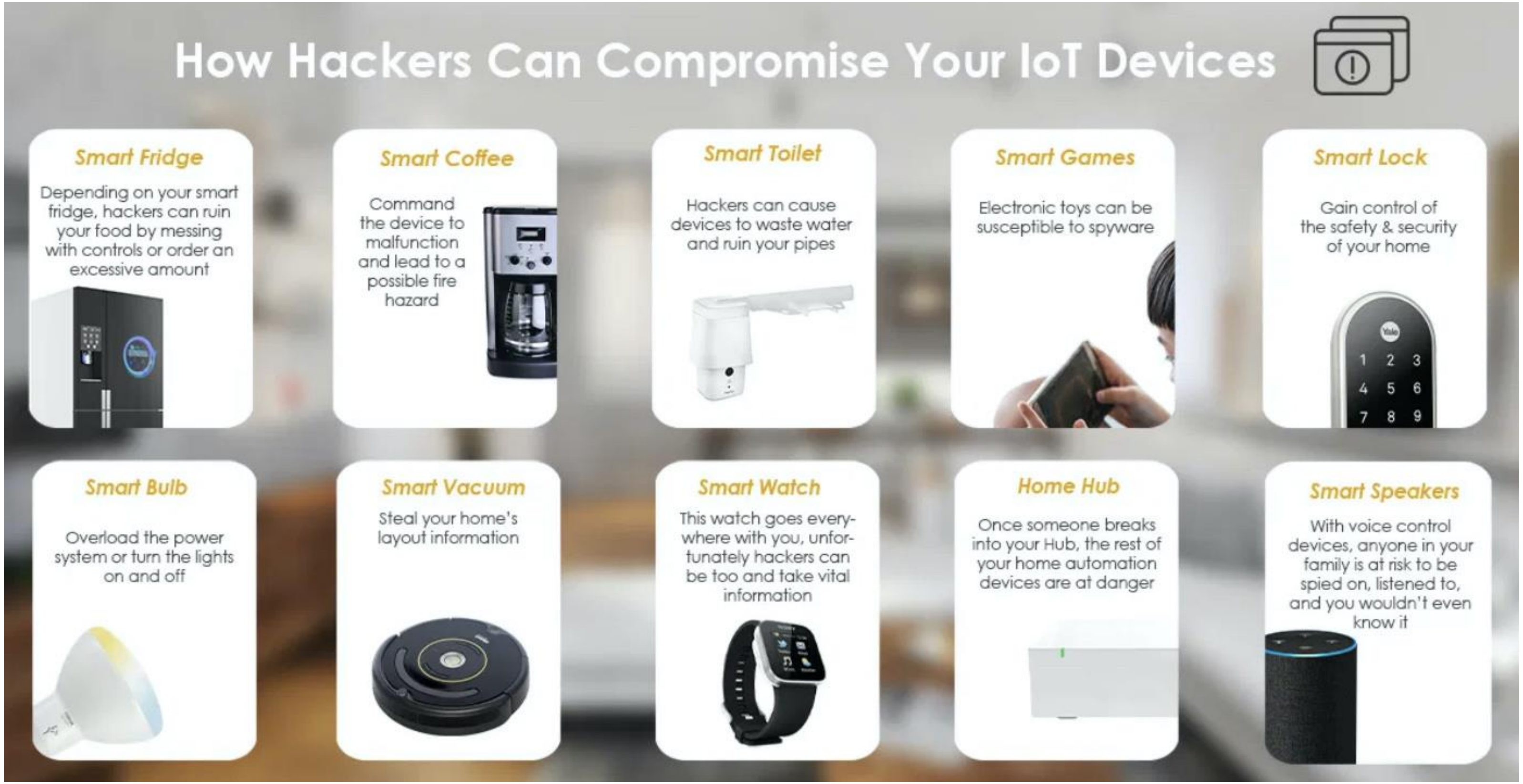


*Forecast

Source: GSMA Intelligence

https://www.mordorintelligence.com/industry-reports/consumer-iot-market

IoT Consumer Devices



How Hackers Can Compromise Your IoT Devices

Smart Fridge

Depending on your smart fridge, hackers can ruin your food by messing with controls or order an excessive amount

Smart Coffee

Command the device to malfunction and lead to a possible fire hazard

Smart Toilet

Hackers can cause devices to waste water and ruin your pipes

Smart Games

Electronic toys can be susceptible to spyware

Smart Lock

Gain control of the safety & security of your home

Smart Bulb

Overload the power system or turn the lights on and off

Smart Vacuum

Steal your home's layout information

Smart Watch

This watch goes everywhere with you, unfortunately hackers can be too and take vital information

Home Hub

Once someone breaks into your Hub, the rest of your home automation devices are at danger

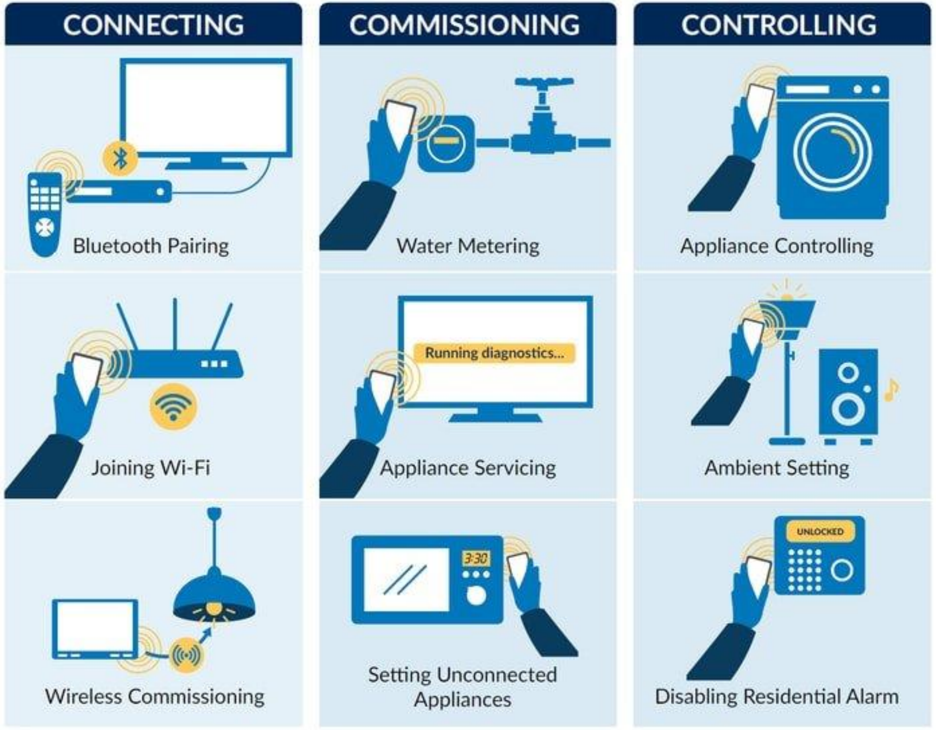
Smart Speakers

With voice control devices, anyone in your family is at risk to be spied on, listened to, and you wouldn't even know it

https://community.iotex.io/t/totw-7-how-to-keep-your-iot-devices-safe-from-hackers/646

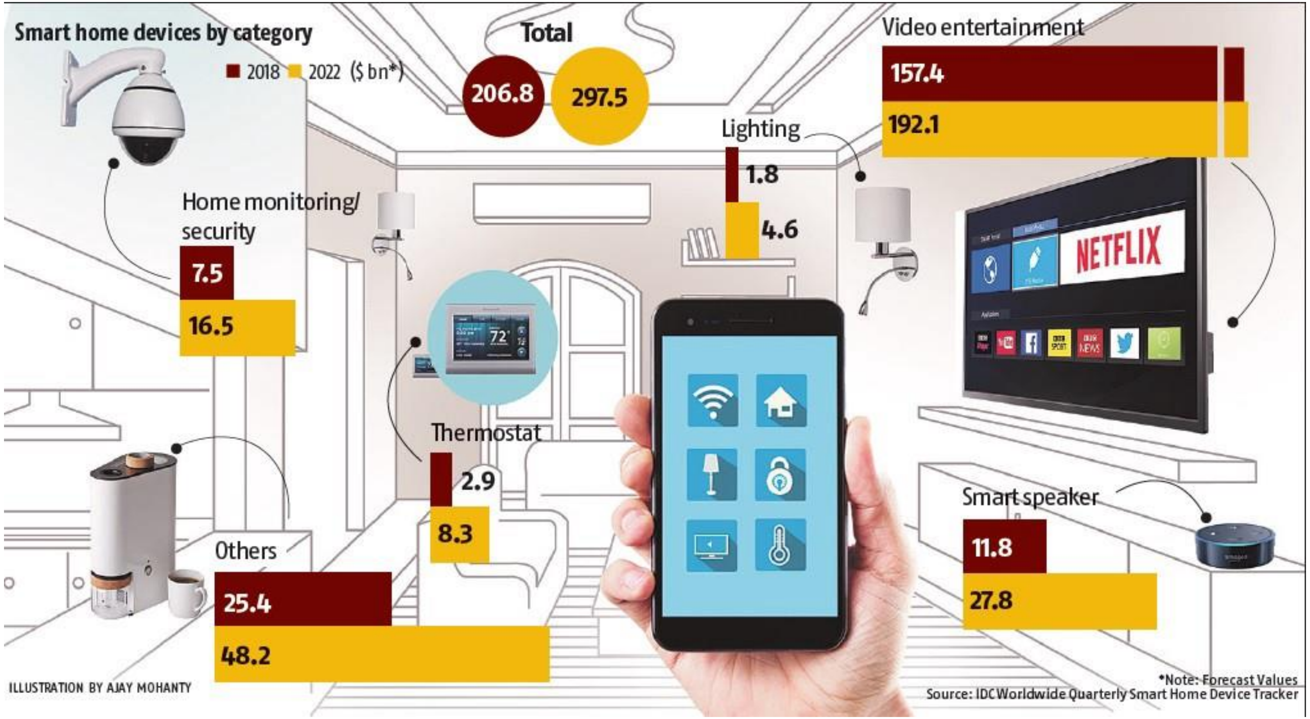
Consumer IoT Protocols

- one
- two
- three



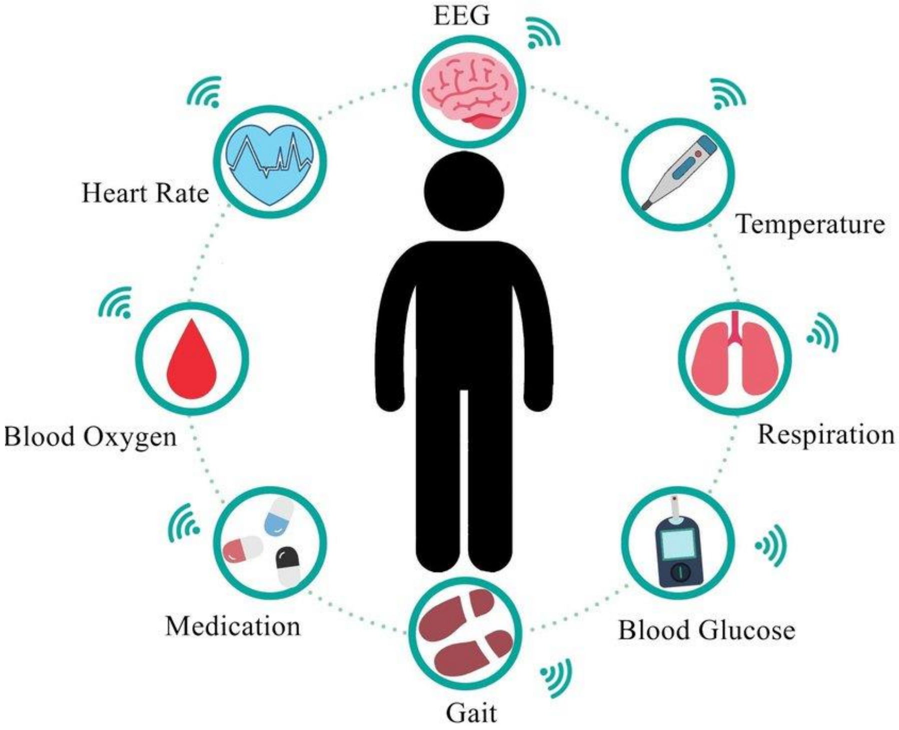
https://www.ubuntupit.com/top-15-standard-iot-protocols-that-you-must-know-about/

Consumer IoT Data



https://towardsdatascience.com/tagged/smart-home

Consumer IoT Data



Linkous, Zohrabi, Abdelwahed (2019, p.30)

IoT Physical Attacks

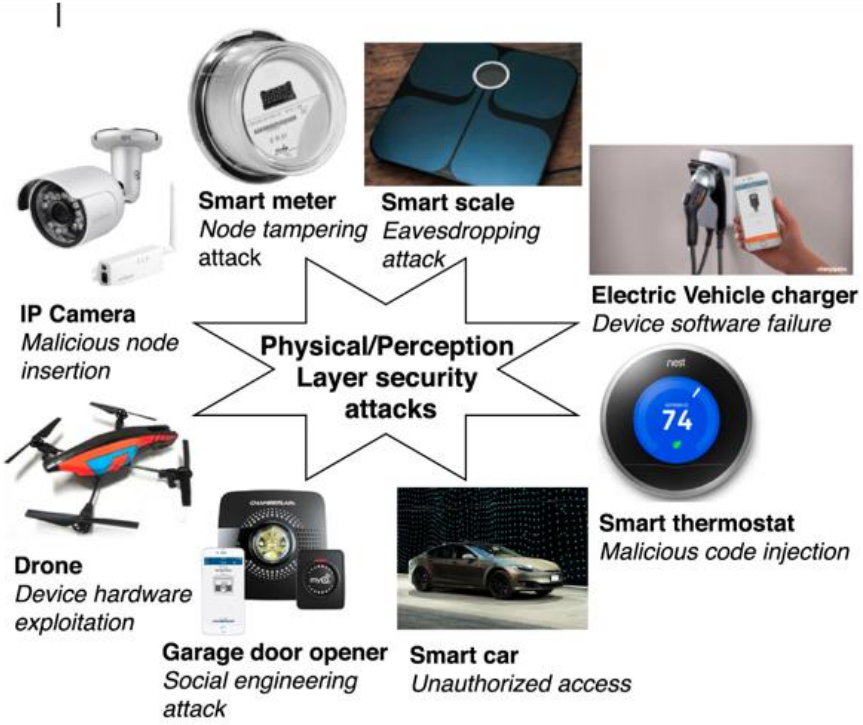


Figure 1. Eight common security attacks on the physical IoT layer with their relevant case studies.

Alladi et al (2020, p.18)

Device Failure

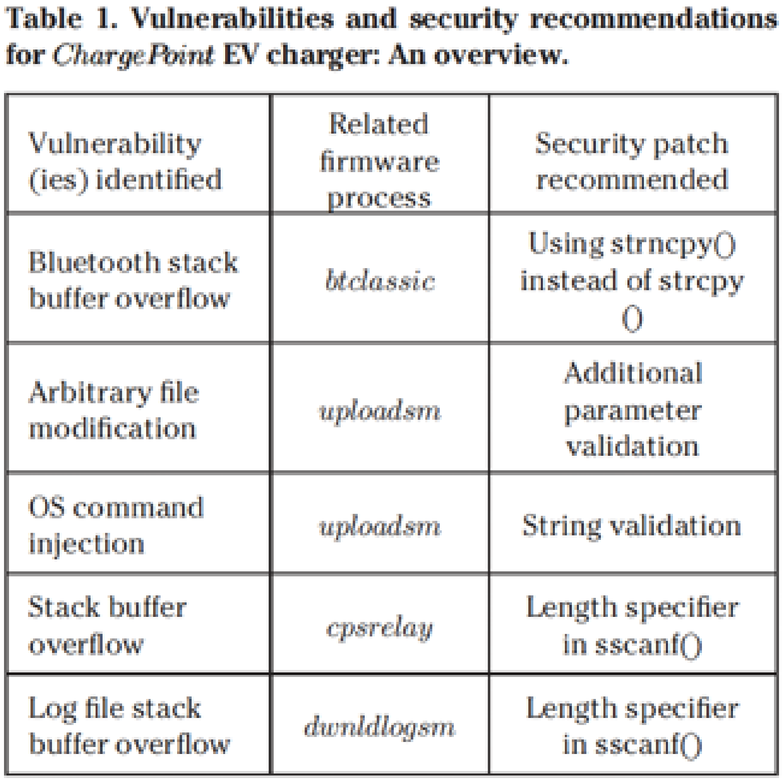
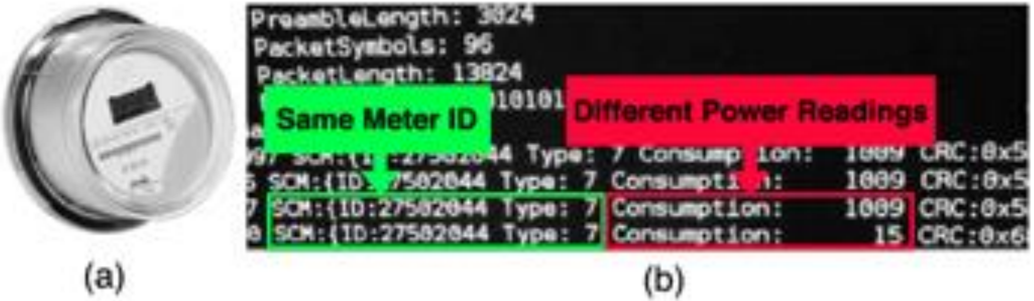


Table 1. Vulnerabilities and security recommendations for *ChargePoint* EV charger: An overview.

Vulnerability (ies) identified	Related firmware process	Security patch recommended
Bluetooth stack buffer overflow	*btclassic*	Using strncpy() instead of strcpy ()
Arbitrary file modification	*uploadsm*	Additional parameter validation
OS command injection	*uploadsm*	String validation
Stack buffer overflow	*cpsrelay*	Length specifier in sscanf()
Log file stack buffer overflow	*dwnldlogsm*	Length specifier in sscanf()

Alladi et al (2020, p.19)

Node Tempering

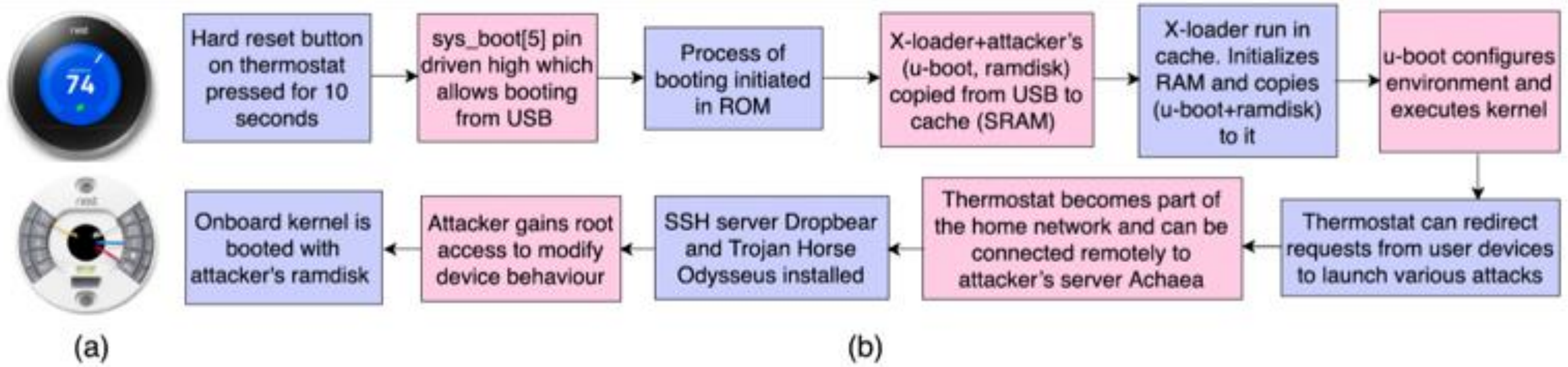


```
PreambleLength: 3024
PacketSymbols: 96
PacketLength: 13824
                  )10101
e
97 SCM:{I  :27502044 Type: 7 Consump  ion:    1009 CRC:0x5
5 SCM:{ID  7502044 Type: 7 Consumpti  n:      1009 CRC:0x5
7 SCM:{ID:27502044 Type: 7 Consumption:     1009 CRC:0x5
0 SCM:{ID:27502044 Type: 7 Consumption:       15 CRC:0x6
```

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

Alladi et al (2020, p.19)

Malicious Code Injection



Hard reset button on thermostat pressed for 10 seconds

sys_boot[5] pin driven high which allows booting from USB

Process of booting initiated in ROM

X-loader+attacker's (u-boot, ramdisk) copied from USB to cache (SRAM)

X-loader run in cache. Initializes RAM and copies (u-boot+ramdisk) to it

u-boot configures environment and executes kernel

Thermostat can redirect requests from user devices to launch various attacks

Thermostat becomes part of the home network and can be connected remotely to attacker's server Achaea

SSH server Dropbear and Trojan Horse Odysseus installed

Attacker gains root access to modify device behaviour

Onboard kernel is booted with attacker's ramdisk

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

Alladi et al (2020, p.20)

Unauthorized Access

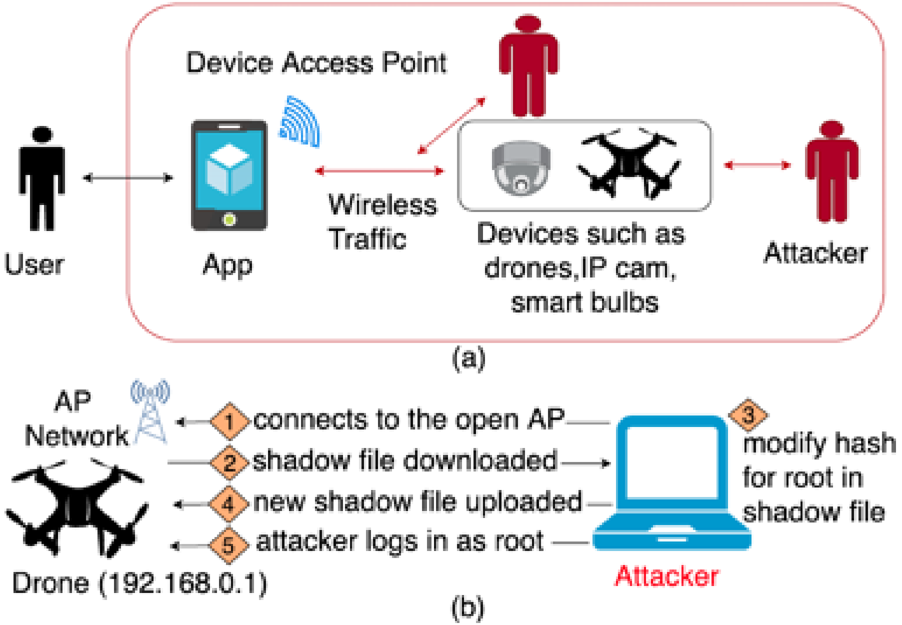

Device Access Point
User
App
Wireless Traffic
Devices such as drones,IP cam, smart bulbs
Attacker
(a)
AP Network
1 connects to the open AP
2 shadow file downloaded
3 modify hash for root in shadow file
4 new shadow file uploaded
5 attacker logs in as root
Drone (192.168.0.1)
Attacker
(b)

Figure 5. (a) Attack on the network (by eavesdropping the traffic) or on the drone (via insecure network services like FTP). (b) Attacker gains root access to the device via telnet using anonymous FTP login as a backdoor.

Alladi et al (2020, p.22)

Other Countermeasures and Challenges

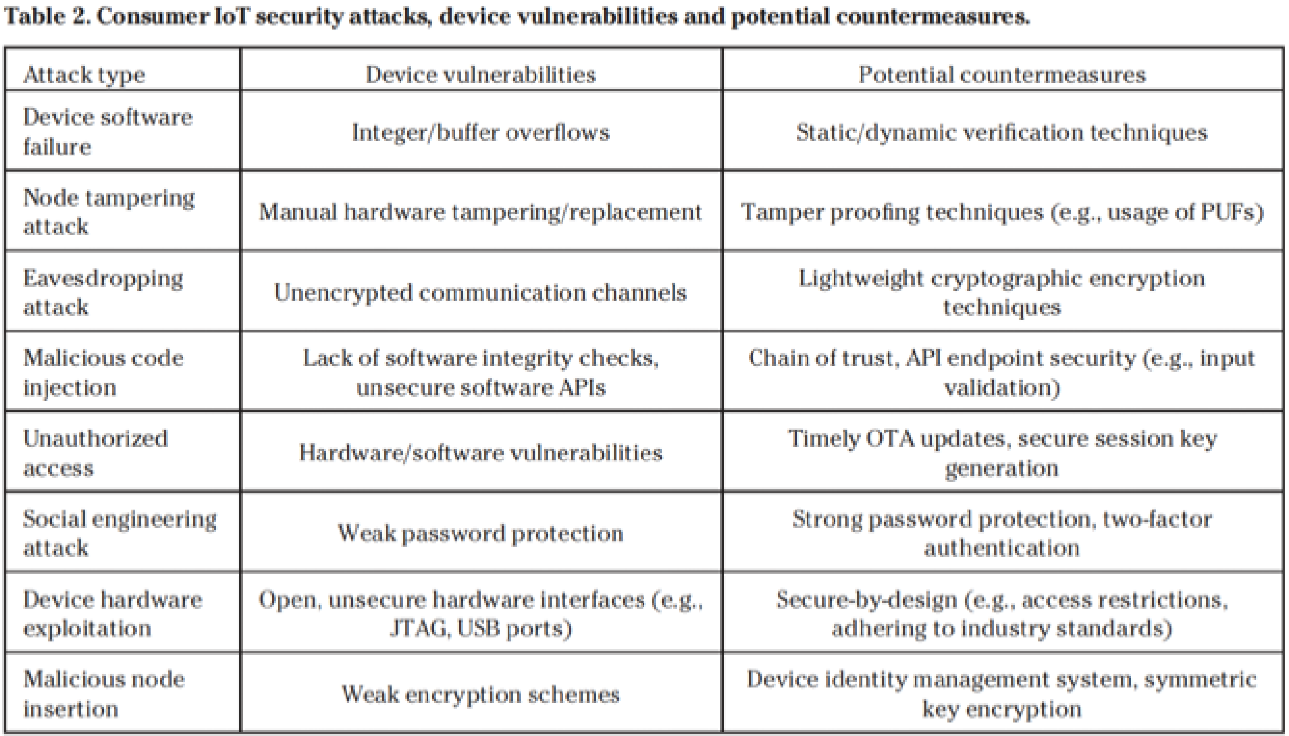


Table 2. Consumer IoT security attacks, device vulnerabilities and potential countermeasures.

Attack type	Device vulnerabilities	Potential countermeasures
Device software failure	Integer/buffer overflows	Static/dynamic verification techniques
Node tampering attack	Manual hardware tampering/replacement	Tamper proofing techniques (e.g., usage of PUFs)
Eavesdropping attack	Unencrypted communication channels	Lightweight cryptographic encryption techniques
Malicious code injection	Lack of software integrity checks, unsecure software APIs	Chain of trust, API endpoint security (e.g., input validation)
Unauthorized access	Hardware/software vulnerabilities	Timely OTA updates, secure session key generation
Social engineering attack	Weak password protection	Strong password protection, two-factor authentication
Device hardware exploitation	Open, unsecure hardware interfaces (e.g., JTAG, USB ports)	Secure-by-design (e.g., access restrictions, adhering to industry standards)
Malicious node insertion	Weak encryption schemes	Device identity management system, symmetric key encryption

Alladi et al (2020, p.24)