10-Mar-2020

IoT Security:

Exploring Risks, Attacks, and Challenges in Securing IoT

Joseph Bugeja

MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE RESEARCH CENTER

KK-stiftelsen

SUMMARY OF IOT SECURITY THREATS

IoT Services

IoT Network

IoT Devices

Threat	Against
Hardware Trojans	All
Side-channel attacks	C,AU,NR,P
DoS	A,AC,AU,NR,P
Physical attacks	All
Node replication attacks	All
Camouflage	All
Corrupted node	All
Tracking	P, NR
Inventorying	P, NR
Tag cloning	All
Counterfeiting	All
Eavesdropping	C,NR,P
Injecting fraudulent packets	P,I,AU,TW,NR
Routing attacks	C,I,AC,NR,P
Unauthorized conversation	All
Malicious injection	All
Integrity attacks against learning	C,I
Non-standard frameworks and inadequate testing	All
Insufficient/Inessential logging	C,AC,NR,P

DOS AS AN EXAMPLE OF AN ATTACK ON DEVICES

IoT Devices

Example of an attack:

> *Denial-of-service*

- ✓ ***Battery draining*:** By depleting the battery of a connected device, e.g., a smoke detector, an attacker will be able to disable a fire detection system
- ✓ ***Sleep deprivation*:** An attacker may attempt to send an undesired set of requests that seem to be legitimate but are not
- ✓ ***Outage attacks*:** Devices may stop functioning as a result of an unintended error in the manufacturing process, battery draining, sleep deprivation, etc.

DEVICE HARDWARE EXPLOITATION

Parrot AR Drone 2.0 Quadcopter

DEVICE HARDWARE EXPLOITATION

- ✓ Open ports in the quadcopter system (e.g., port 21-File Transfer Protocol (FTP) and port 23-Telnet) were discovered through NMAP
- ✓ Using a compatible mobile app, one can connect to the target device through its open access point (AP)
- ✓ Via FTP, malicious files can then be loaded into its file system or a harmful firmware update can be performed
- ✓ An attacker can remotely power off and bring down a flying drone

ROUTING AS AN EXAMPLE OF A NETWORK ATTACK

IoT Network

Example of an attack:

> *Routing*

- ✓ ***Black hole*:** This attack is launched by using a malicious node, which attracts all the traffic in the network by advertising that it has the shortest path to the destination in the network
- ✓ ***Gray hole:*** This attack is a variation of Black Hole attack in which the nodes selectively drop some packets
- ✓ ***Worm hole*:** In this attack, the attacker first records packets at one location in the network and then tunnels them to a different location
- ✓ ***Others*:** HELLO floods, Sybil, bogus routing information, etc.

MALICIOUS NODE INSERTION

Edimax IP Cameras

MALICIOUS NODE INSERTION

- ✓ The attack begins from a public IoT device infected by a malware acting as a software bot
- ✓ The bot sends TCP SYN probes to random IPv4 addresses in the network guessing their 12-character MAC addresses
- ✓ Once, an acknowledgment for one of them is received that confirms a valid MAC address
- ✓ The software bot now binds and registers with the registration server following the same steps the camera would, using the MAC address of that camera
- ✓ It then sends a TCP request to the command relay server, which in turn responds with the authentication information (for the original camera) to the software bot
- ✓ The attacker can now very easily extract the password from this information and the IP camera is in full control of the attacker

INJECTION AS AN EXAMPLE OF A SERVICE ATTACK

IoT Services

Example of an attack:

> Malicious injection

- ✓ Insufficient validation of the input may enable malicious input injection
- ✓ An attacker could inject a malicious input that causes the service providers to perform operations on behalf of the attacker
- ✓ For example, an attacker may add an unauthorized component that is capable of injecting malicious inputs into the servers. Afterwards, the attacker might be able to steal data, compromise database integrity, or bypass authentication
- ✓ Standard database error messages returned by a database may also assist the attacker

UNAUTHORIZED ACCESS

Tesla Model S

UNAUTHORIZED ACCESS

- ✓ Tesla service centers and charging stations are equipped with *TeslaService* WiFi SSID
- ✓ The credentials to access them are stored in *QtCarBrowser* (Tesla's web browser) as part of the auto-connect feature
- ✓ By faking this SSID, the attackers redirected the traffic from the browser to their domain
- ✓ Attackers exploited software bugs in QWebKit/2.2x (Tesla's browser engine) allowing them to read/write arbitrary memory addresses and finally obtaining root access