Lecture 8

Tuesday, 6 December 2022 13:28

data comes from 'sensors'

UPnP 'leaks' quite a bit of data ⇒ allows gathering information about devices
↓
can use profile to investigate which vulnerabilities might play a role

largest customer has 1 million devices

honeypot: simulates existence of devices to find out what attackers are doing

feed generation
threat investigation
threat attribution
mitigation

intelligence factory → reports, feeds, intel

knowledge is shared openly, partially because of openness requirements from governments

getting access to actually used devices is sometimes difficult

e.g. actual PLC is probably not on Amazon

manufacturers make devices easy to install → everything enabled by default

many languages on team → threats come from many different backgrounds/countries

IT information technology — routers, servers, computer, iPhone, ...

OT operational technology

first: focus on this ↓ then: Stuxnet ⟹ OT security became important

critical infrastructure — differs per country

initial mindset: 'it has to work' → security more like an availability thread

IoT internet of things → consumer IoT; → enterprise/industrial IoT

IoMT internet of medical things

eventually: internet of everything

all things are connected

OTA: over the air update

IoT devices usually aren't
- agentable — cannot install antivirus, management software, intelligence gathering
- manageable — difficult to retrieve information, apply changes, monitor state + compliance

IP phones are common in companies

UPS = uninterruptible power supply

OT/IoT → legacy, critical infrastructure, lack of authentication
more and more interconnected

kill chain → phases such as reconnaissance, initial entry, lateral movement

Stuxnet	Industroyer 1	Triton	Industroyer 2	ransomware spills to OT
Iran, highly targeted & sophisticated	Ukraine, multistage automated	highly targeted; Saudi Arabia safety system	Ukraine less sophisticated, less targeted	e.g. Colonial Pipeline

nation states ⟶ criminals

key trends:
1. device landscape is changing
2. IoT devices used as entry point for attack
3. attackers want easy money

relevant threat actors depend on the target

activist groups have very specific goals

most commonly targeted sectors
1. telecom
2. utilities
3. several
4. manufacturing

most common targeted devices
1. SCADA
2. PLC/controllers
3. VoIP
4. router
5. UPS

Criminal software as a service
ransomware as a service

default/weak credentials are still often used to get in

infosec is often not involved when IoT/OT devices are purchased

ransomware 4 IoT

one-way, two-way, three-way } extortion
→ can also be: shut down production

→ exploits IoT ⟶ encrypts IT ⟶ disrupts OT

1. exploit for initial access & persistence
2. Windows 10 host discovery, RDP credentials
3. SSH tunneling
4. drop & execute, discover exploit dump
6. exfiltrate & encrypt
8. network scan & DoS

published report → later: similar attacks reviewed in practice

2023 predictions:
- hacking groups
- state-sponsored actors
- critical infrastructure

observations:
1. attacks are not immediate and fully automated
2. cybercrime-as-a-service means that hundreds of very similar attacks are happening
3. most tools & techniques are well known

NIST cybersecurity framework functions
- identify
- protect
- detect
- respond
- recover