Lecture 3

Tuesday, 22 November 2022 12:30

targeted attacks on critical infrastructure

SCADA → supervisory control and data acquisition → sends control commands to PLC

PLC → programmable logic controller

many communication protocol

level 4

level 3

SCADA level 2 supervisory computers

PLC level 1 direct control

level 0 plant

SCADA systems were designed (20 years ago) in isolated situations, with no security in mind, for local access

today: connected throughout backoffice, allow remote control

lots of proprietary protocols, very hard to patch

very few attacks e.g. due to lack of monetary gain, lack of standardization in systems

supply chain attack: infect (USB of) maintenance supplier

Stuxnet phases

1. worm with update — Windows (4 zero-day vulnerabilities, rootkit (→ modifies interface/API of OS to hide itself), checks which AV is used, select target based on that
2. infects PLC, modifies programming — find PLC-related software, attack even via USB-sticks, hook into software DLL to replace code, includes rootkit
3. attack if in correct environment — change frequency if certain (very specific) hardware was used

Havex:

spread through email, watering hole

gather information + gain persistent attacks

enumeration and qualification of network hosts

OPC servers + VPN connections to PLCs

initially targeted aviation & defense then US/EU

from compile time, can be derived as most likely Eastern European

Blackenergy 3

ICS (industrial control system) / OT (operational technology) network

limited number of hosts

same operations repeat over and over

changes are less frequent

IT system

most important: integrity

↑

confidentiality

↑

least important: availability

OT system

availability + integrity

↑

confidentiality

ICS is different from IT

expensive to get inside

difficult to replace/attack as-is

defender has no idea what happens inside

Types of attackers:

Criminals

hacktivists

nation states