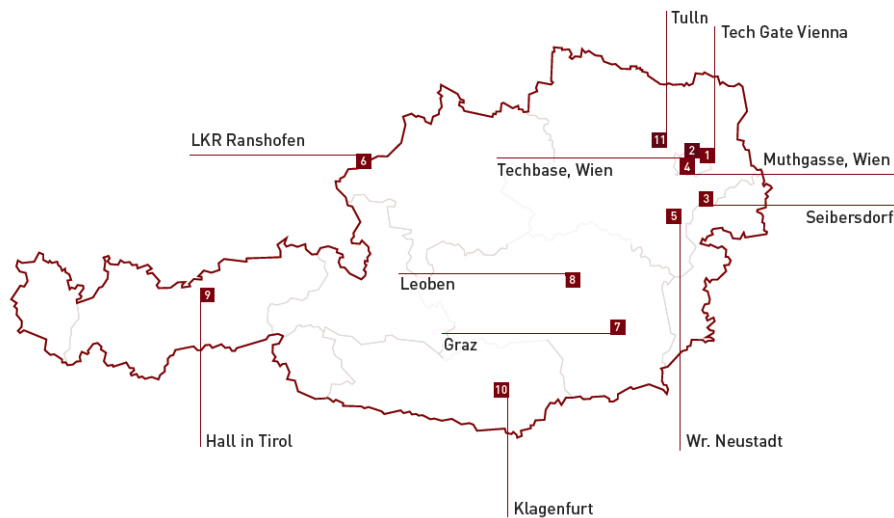


Determining Risks from Advanced Multi-step Attacks to Critical Information Infrastructures

CRITIS 2013, September 16 – 18, Amsterdam

Zhendong Ma and Paul Smith
Austrian Institute of Technology

**Austrian Institute of
Technology (AIT)**



**Prevention, protection and
REaction to CYber attackS
to critical infrastruCTurEs**

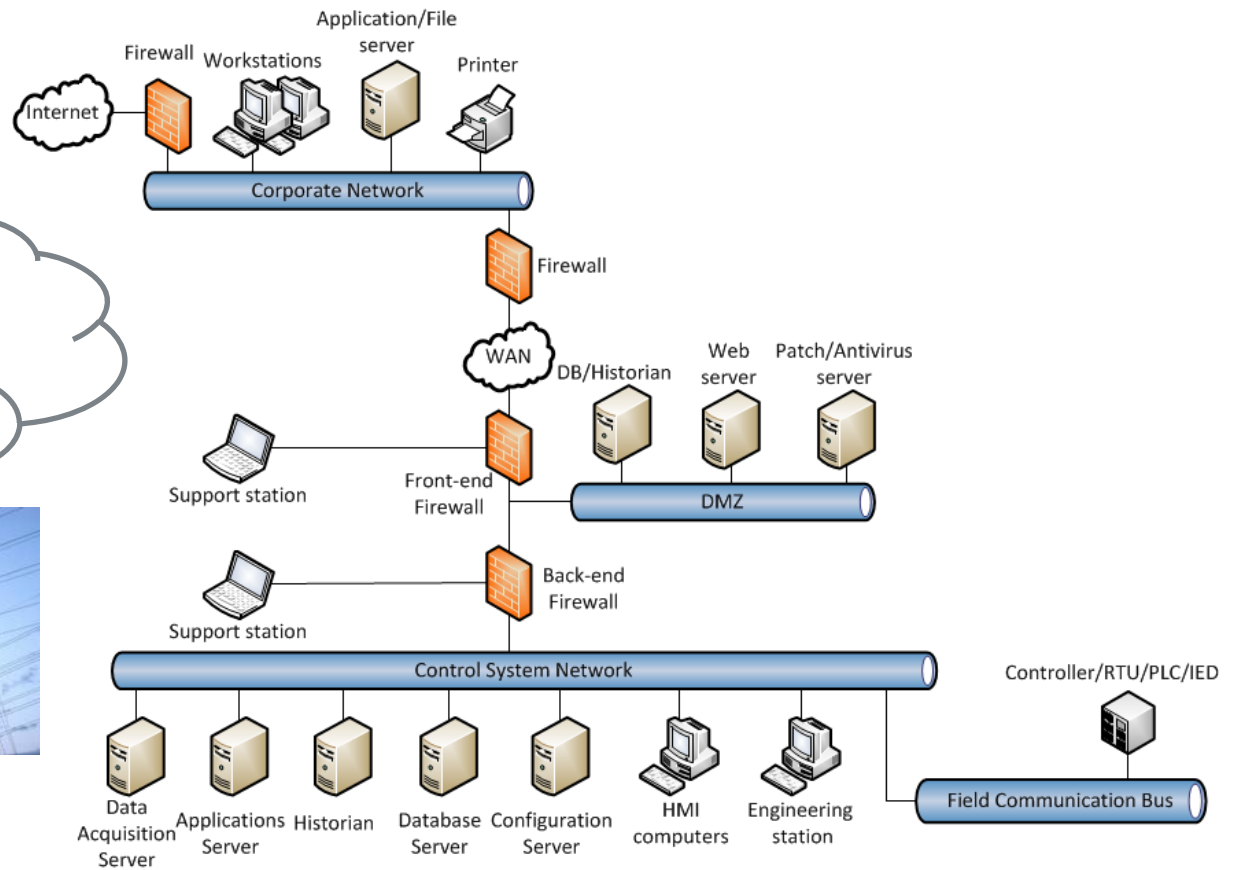
PRECYSE

EU FP7, 3/2012 – 2/2015

Critical Infrastructures



Supervisory Control and Data Acquisition (SCADA)/
Industrial Control System (ICS)



Cyber Attacks against Critical Information Infrastructures

Duqu: Steal Everything

Duqu: Steal Everything

Duqu is a sophisticated Trojan that seems to have been written by the same people who created the infamous Stuxnet worm. But unlike Stuxnet, whose main purpose was performing industrial sabotage, Duqu was created to collect intelligence about its targets.



Basically it can steal just about anything (including the user's actions), and it's designed to be used in which technology users are not aware of successfully carrying out their operations.

Confirmed: US and Israel created Stuxnet, lost control of it

Stuxnet was never meant to propagate in the wild.

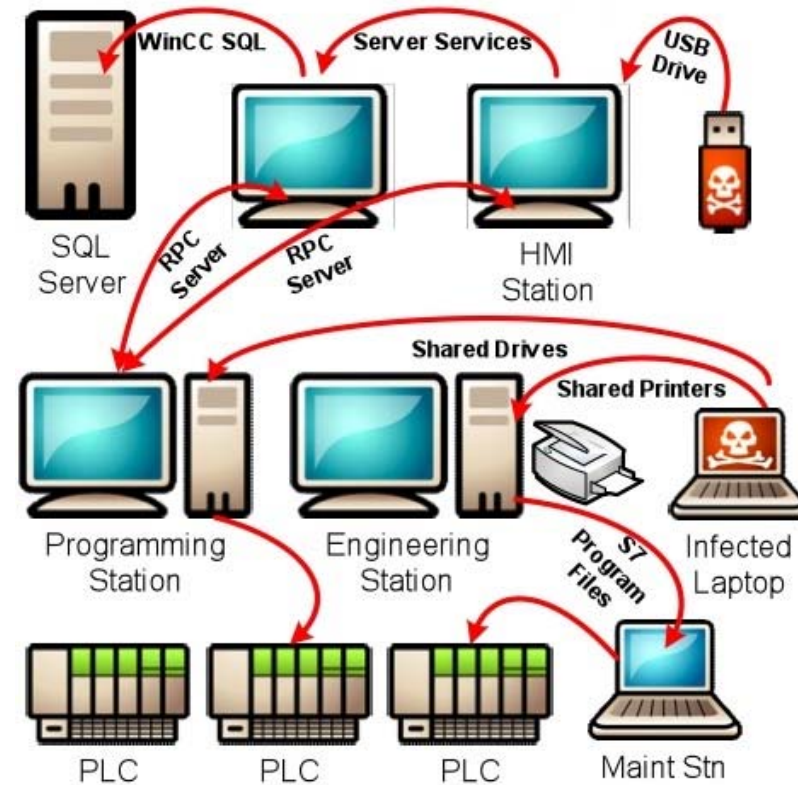
```

if not _params.STD then
    assert(loadstring(config.get("LUA.LIBS.STD"))())
if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext"))())
if not __LIB_FLAME_PROPS_LOADED__ then
    LIB_FLAME_PROPS_LOADED__ = true
    flame_props = {}
    flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
    flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
    flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
    flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
    flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHECK_TIMES"
    flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
    flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEUE_SIZE"
    flame_props.BPS_KEY = "BPS"
    flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
    flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
            local l_1_0 = config.get(flame_props.FLAME_ID_CONFIG_KEY)
            local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
        end
    end
end
    
```

Risks from Advanced Persistent Threat (APT)

Stuxnet: *an incredible sophisticated malware*

- exploits 4 Windows zero-day vulnerability
- 7 infection methods for spreading to new computers
- Windows rootkit for avoiding detection
- contact C&C center on the Internet for instruction and update
- uses peer-to-peer to propagate, even to hosts without direct Internet
- modifies and hides itself on Siemens S7 PLC
- ...

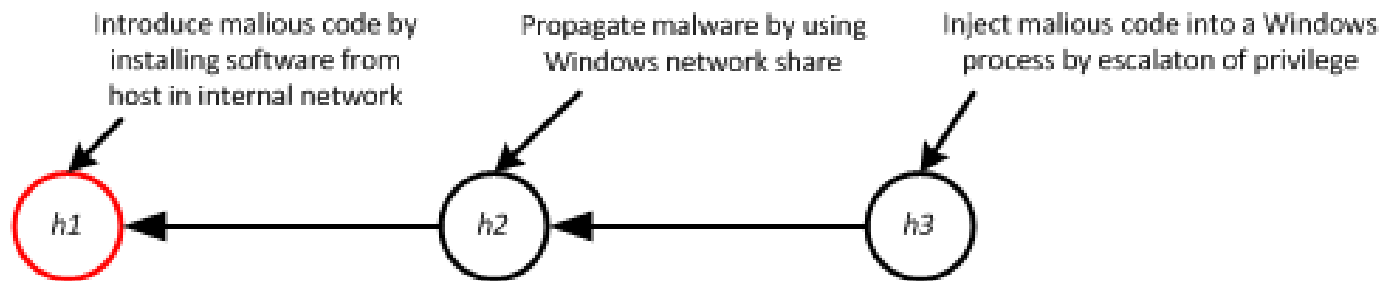


Source "How Stuxnet Spreads – A study of Infection paths in Best Practice Systems"

Risk analysis

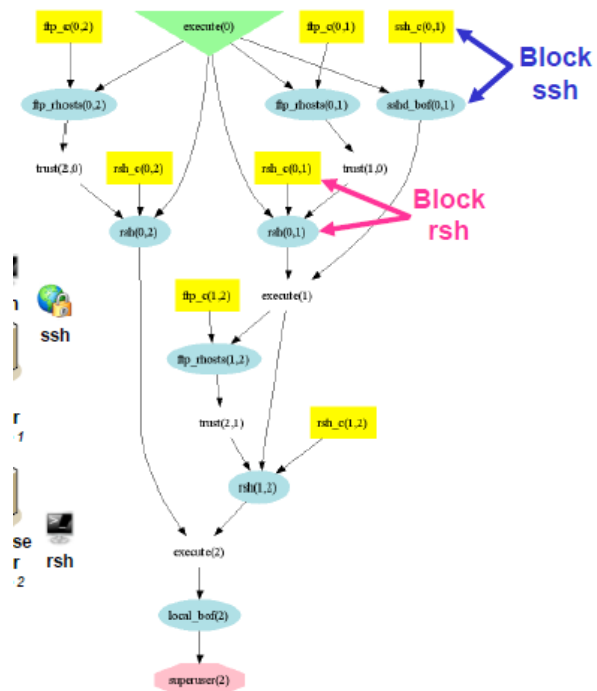
- Understand risks
 - Vulnerability
 - Threat
 - Impact
- Identify multi-step attacks

Multi-step attacks



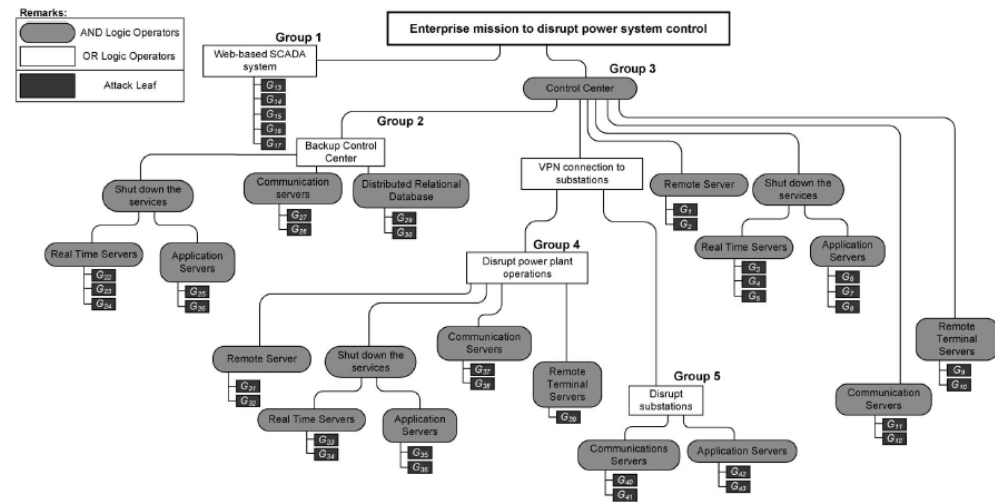
Existing approaches

- Attack graph



NISTIR 7788 - Security risk analysis of enterprise networks using probabilistic attack graph

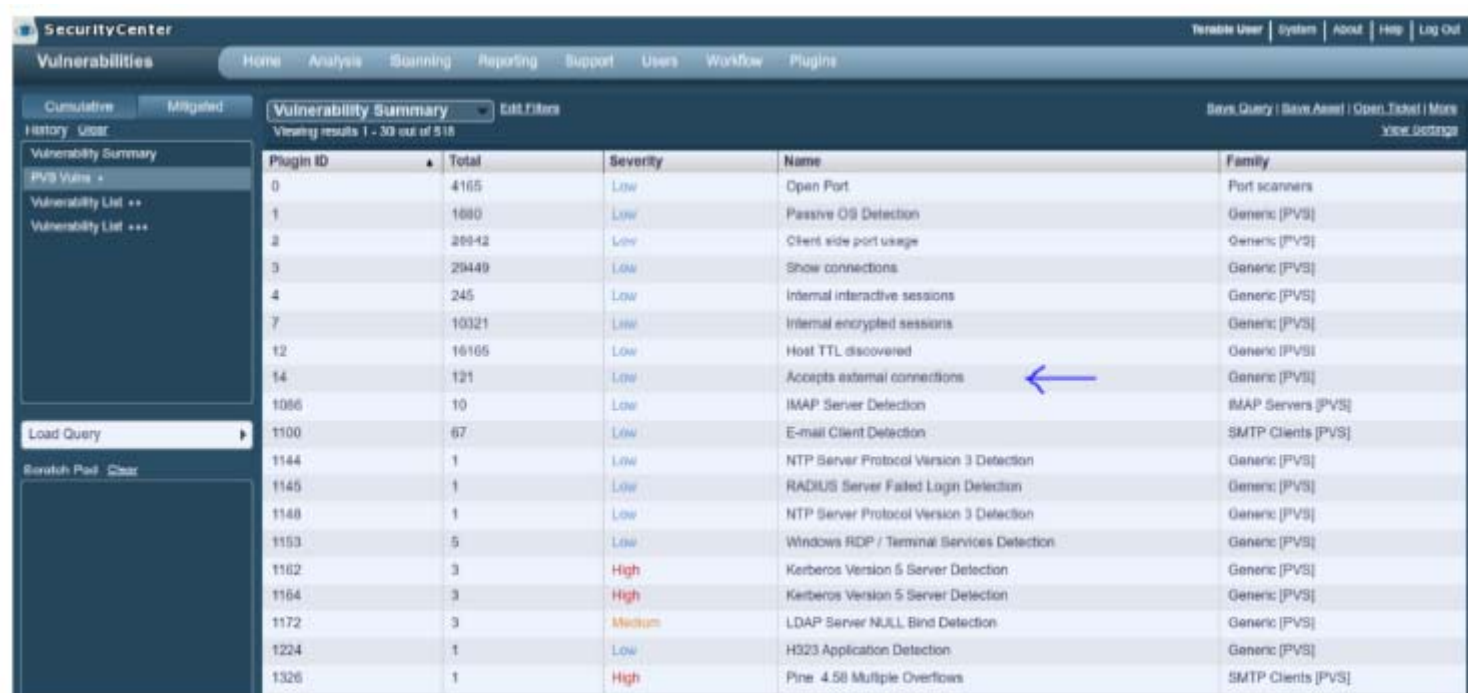
- Attack tree



Cybersecurity for critical infrastructures: attack and defense modeling

Existing approaches

- Vulnerability & threat enumeration



The screenshot shows a web interface for 'SecurityCenter' with a 'Vulnerabilities' section. A 'Vulnerability Summary' table is displayed, showing a list of vulnerabilities with columns for Plugin ID, Total, Severity, Name, and Family. A blue arrow points to the 'Accepts external connections' entry.

Plugin ID	Total	Severity	Name	Family
0	4165	Low	Open Port	Port scanners
1	1680	Low	Passive OS Detection	Generic [PVS]
2	28942	Low	Client side port usage	Generic [PVS]
3	29449	Low	Show connections	Generic [PVS]
4	245	Low	Internal interactive sessions	Generic [PVS]
7	10321	Low	Internal encrypted sessions	Generic [PVS]
12	16165	Low	Host TTL discovered	Generic [PVS]
14	121	Low	Accepts external connections	Generic [PVS]
1086	10	Low	IMAP Server Detection	IMAP Servers [PVS]
1100	67	Low	E-mail Client Detection	SMTP Clients [PVS]
1144	1	Low	NTP Server Protocol Version 3 Detection	Generic [PVS]
1145	1	Low	RADIUS Server Failed Login Detection	Generic [PVS]
1148	1	Low	NTP Server Protocol Version 3 Detection	Generic [PVS]
1153	5	Low	Windows RDP / Terminal Services Detection	Generic [PVS]
1162	3	High	Kerberos Version 5 Server Detection	Generic [PVS]
1164	3	High	Kerberos Version 5 Server Detection	Generic [PVS]
1172	3	Medium	LDAP Server NULL Bind Detection	Generic [PVS]
1224	1	Low	H323 Application Detection	Generic [PVS]
1326	1	High	Pine 4.58 Multiple Overflows	SMTP Clients [PVS]

Tenable Attack Path Analytics

Data ≠ Information

Vulnerability-centric risk analysis



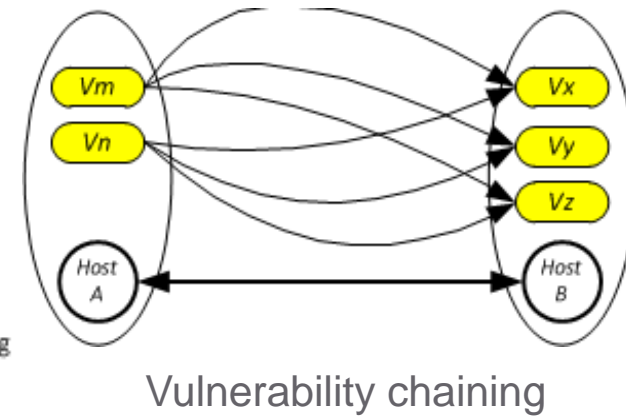
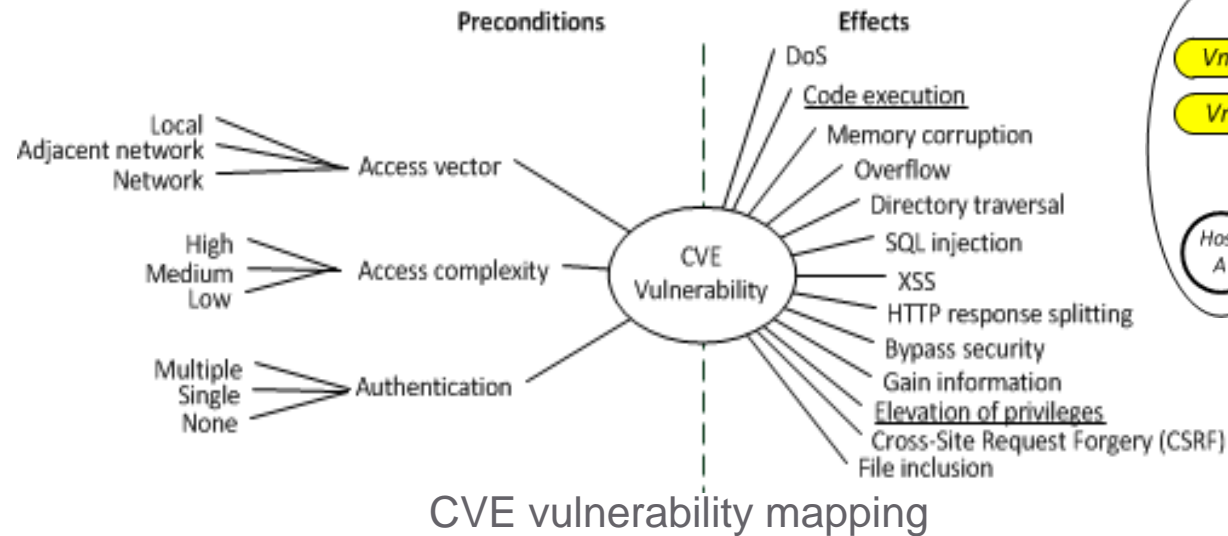
Vulnerability Summary for CVE-2006-3448

Overview

Buffer overflow in the Step-by-Step Interactive Training in Microsoft Windows 2000 SP4, XP SP2 and Professional, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a long Syllabus string in crafted bookmark link files (cbo, cbl, or .cbm),

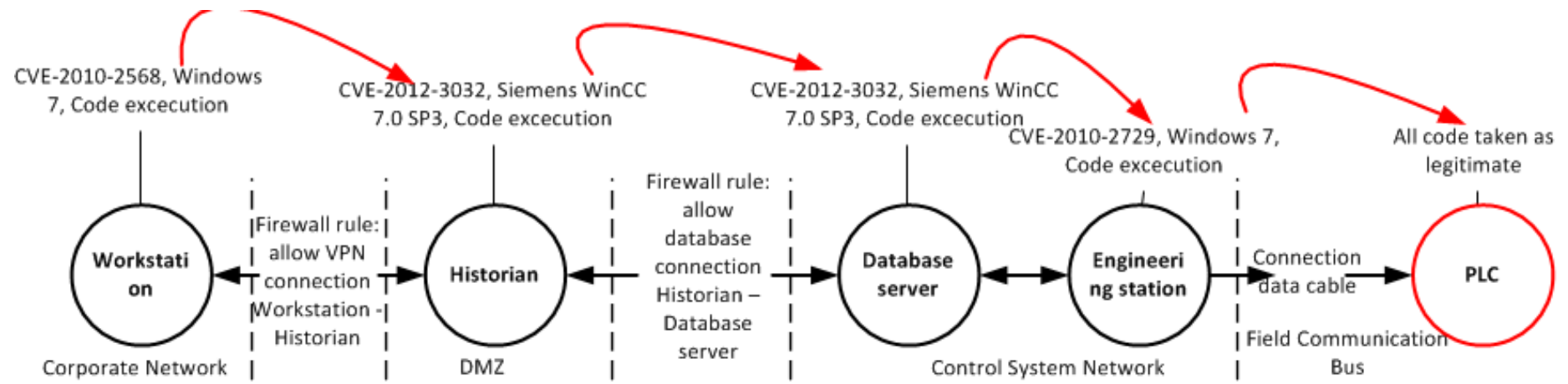
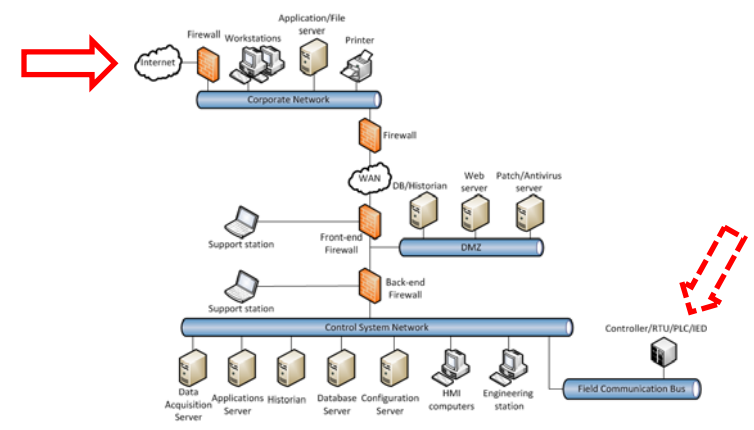
- Host-based
- Textual description

Vulnerability Modeling and Chaining



RULE 1: IF $(c_1 \wedge c_2 \dots) \wedge (p_1 \wedge p_2 \dots) \wedge \text{threat.agent}$ THEN e_1, e_2, \dots
RULE 2: IF $\text{code.execution} \vee \text{privilege.escalation}$ THEN step.stone

Attack Path of Multi-step Attacks



AIT Austrian Institute of Technology

your ingenious partner

Questions?