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

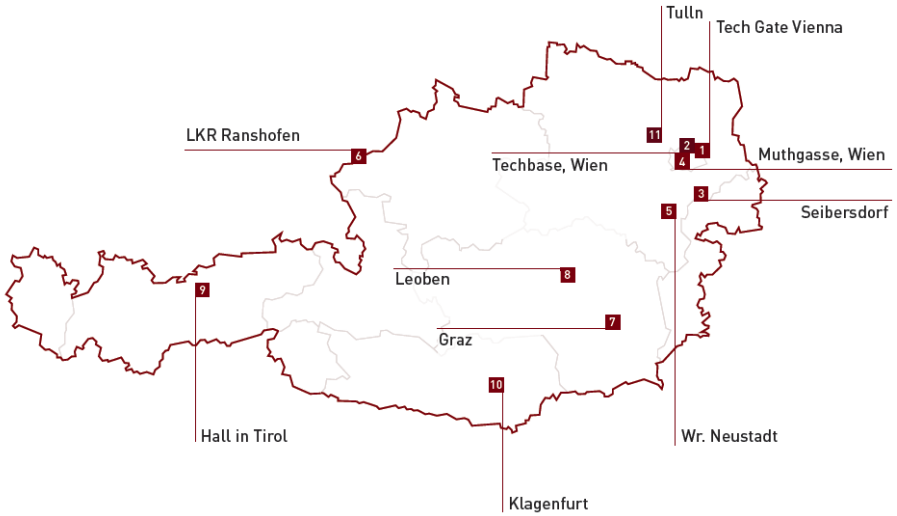
CRITIS 2013, September 16 – 18, Amsterdam

Zhendong Ma and Paul Smith
Austrian Institute of Technology

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

bmvit iv INDUSTRIELLEN VEREINIGUNG

Austrian Institute of Technology (AIT)



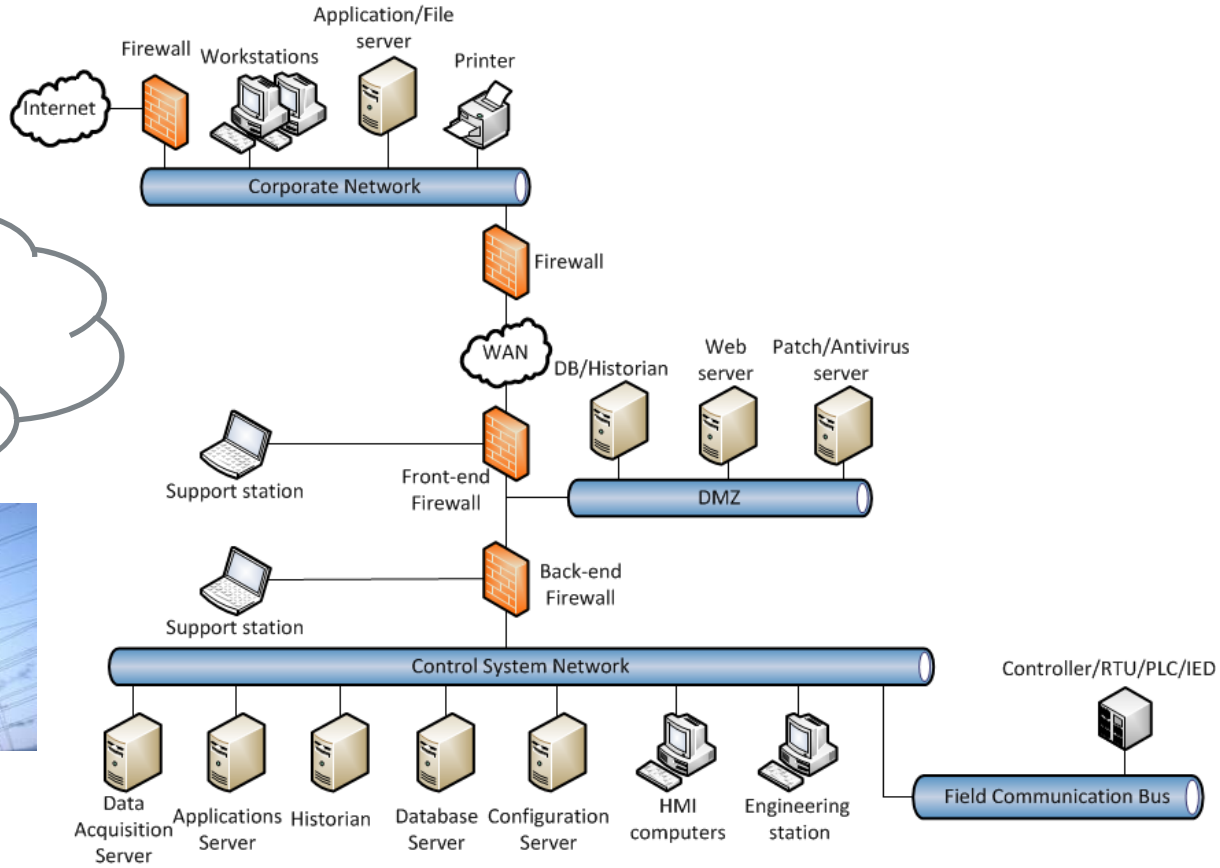
Prevention, protection and REaction to CYber attackS to critical infrastructurEs

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 jus
attackers were particula
on the user's actions), a
in which technology use
of successfully carrying

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

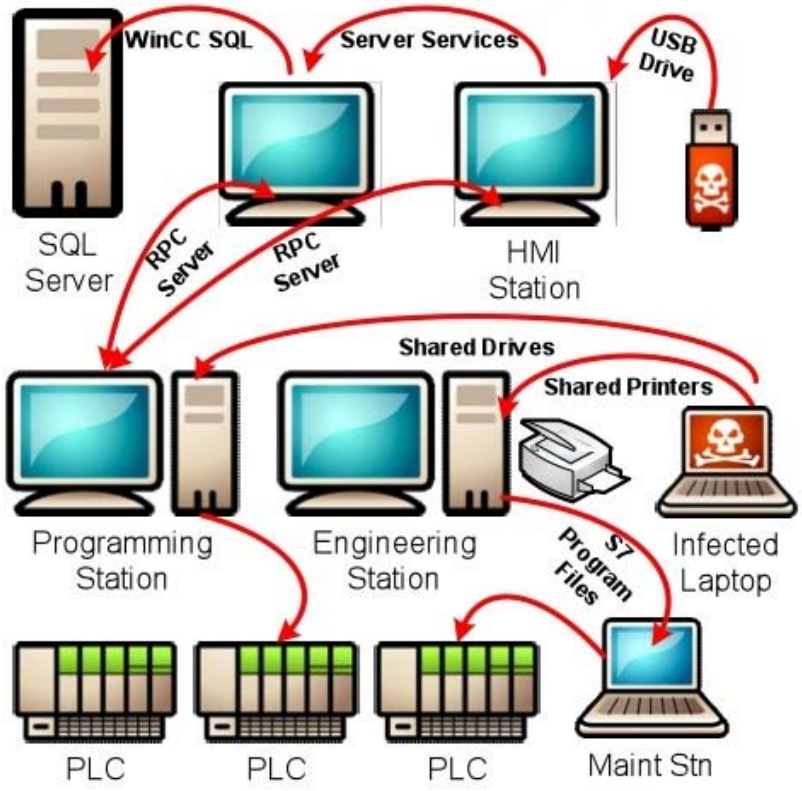
Stuxnet was never meant to propagate in the wild.

```
if not _params.STD
  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_CHE
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEU
      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
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
```

Risks from Advanced Persistent Threat (APT)

Stuxnet: ***an incredible sophisticated malware***

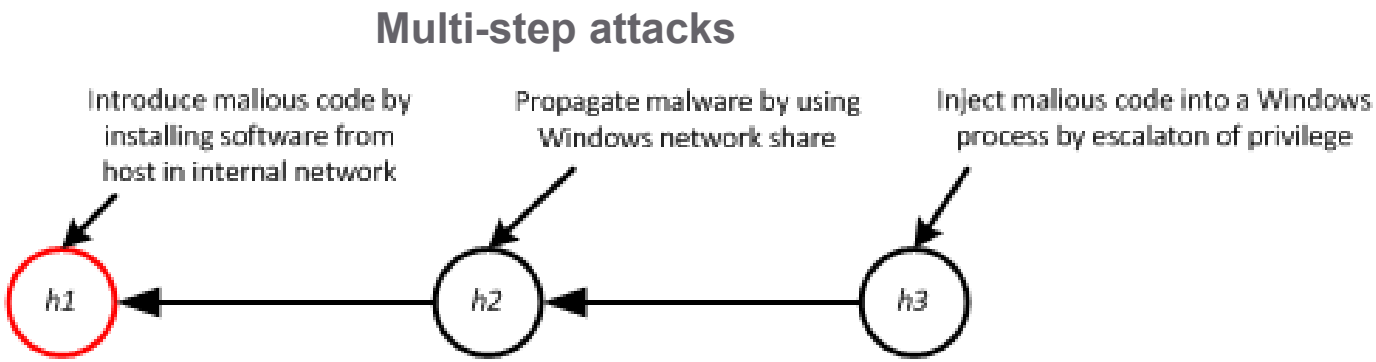
- exploits 4 Windows zero-day vulnerability
- 7 infection methods for spreading to new computers
- Windows rootkit for avoiding detection
- contact C&C center on the Internet for instruction and update
- uses peer-to-peer to propagate, even to hosts without direct Internet
- modifies and hides itself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



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

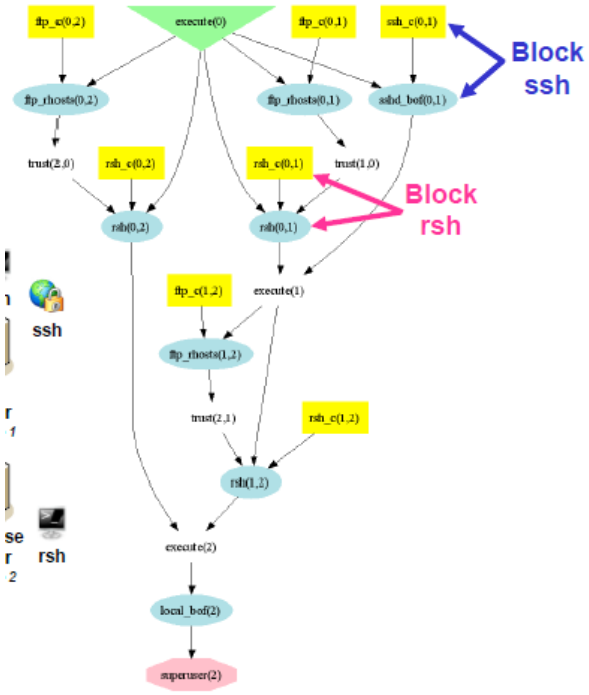
Risk analysis

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



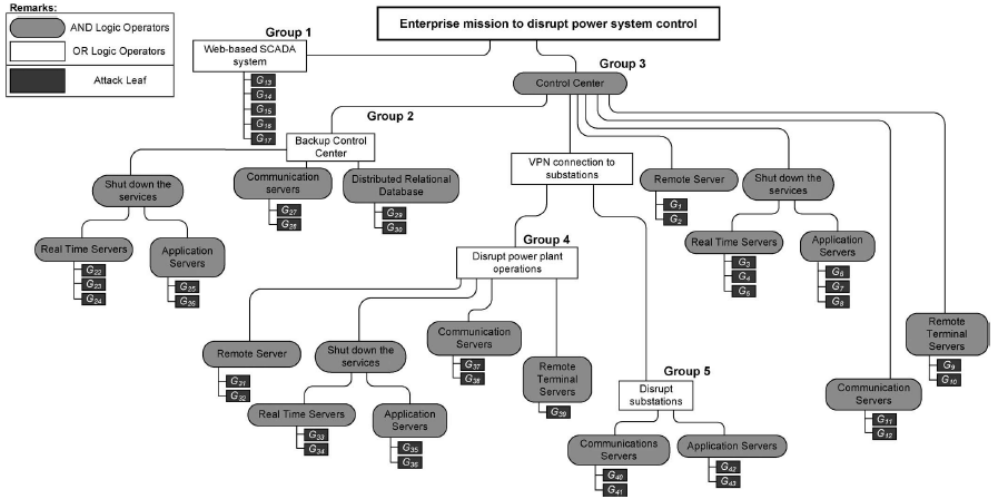
Existing approaches

- Attack graph



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

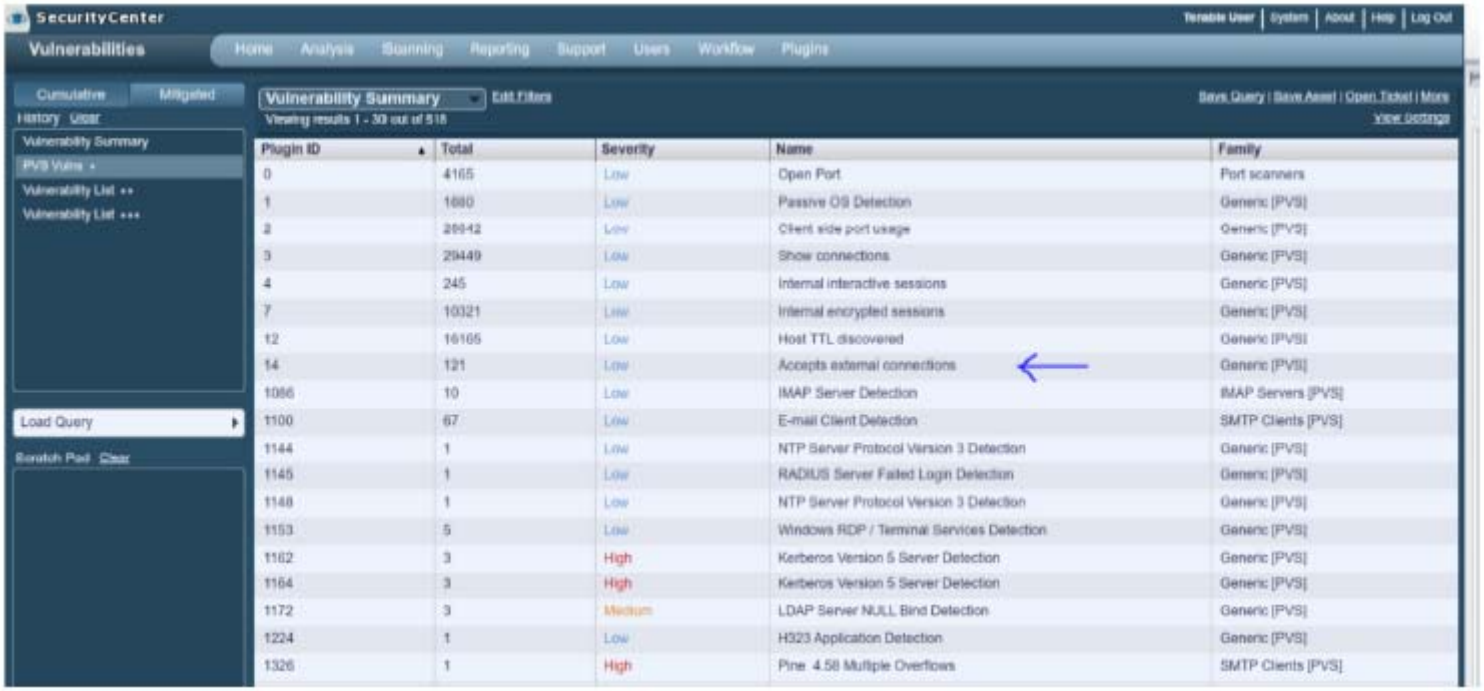
- Attack tree



Cybersecurity for critical infrastructures: attack and defense modeling

Existing approaches

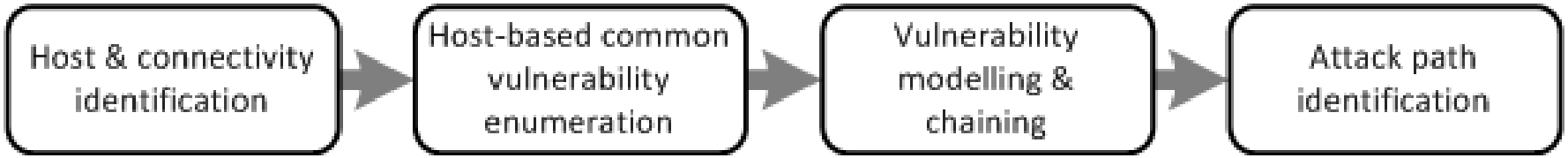
- Vulnerability & threat enumeration

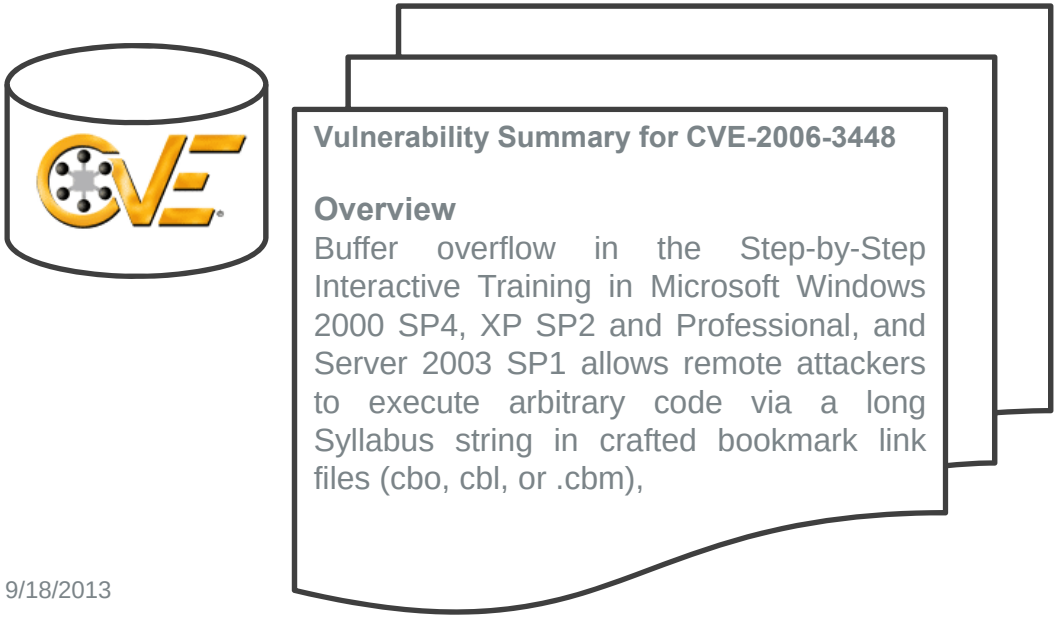


Tenable Attack Path Analytics

Data ≠ Information

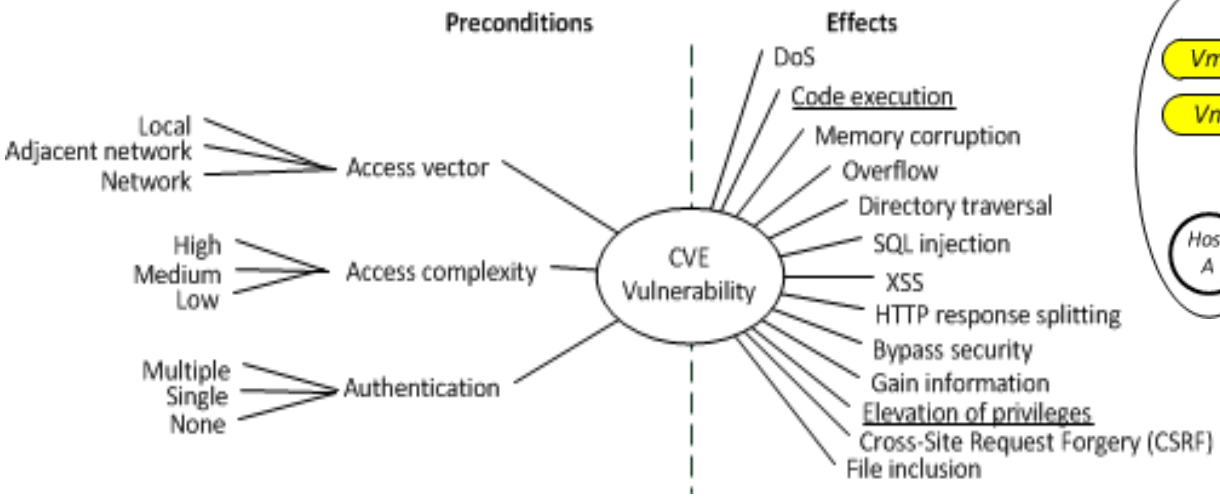
Vulnerability-centric risk analysis



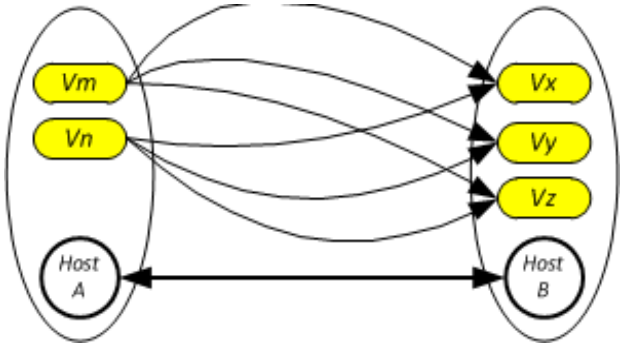


- Host-based
- Textual description

Vulnerability Modeling and Chaining



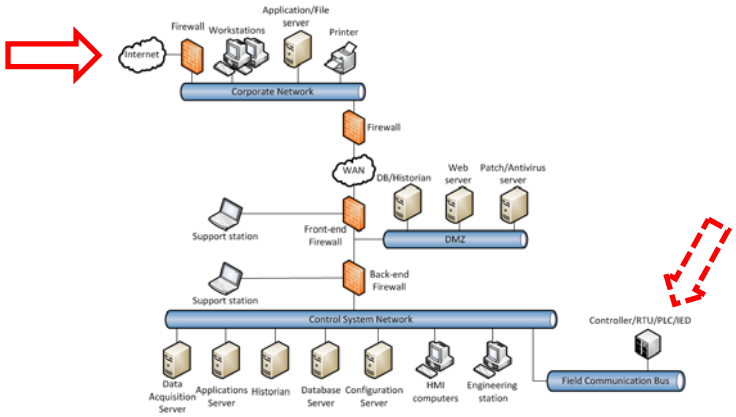
CVE vulnerability mapping

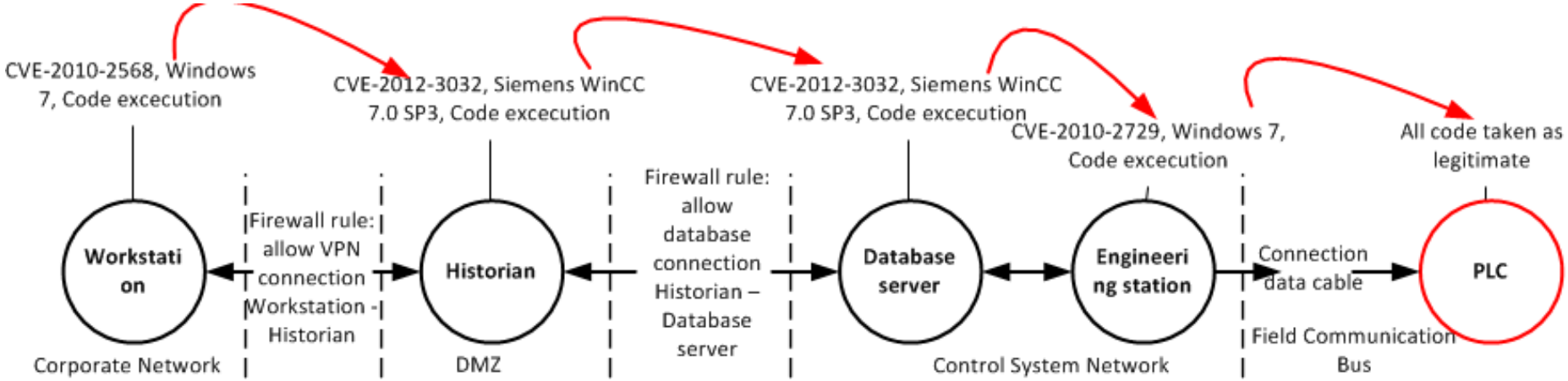


Vulnerability chaining

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

Attack Path of Multi-step Attacks





AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AIT Austrian Institute of Technology

your ingenious partner

Questions?

Partially supported by PRECYSE