SMART GRID PROTECTION AGAINST CYBER ATTACKS

Intrusion Detection in Smart Grid

Symposium on Innovative Smart Grid Cybersecurity Solutions

Vienna, 13th March, 2017

BooJoong Kang

Centre for Secure Information Technologies (CSIT) @QUB

EU FP7 Programme Contract No. 608224

Outline

- Recent Cyber-attacks
- Advanced Persistent Threat
- Countermeasures
- Intrusion Detection

EU FP7 Programme Contract No. 608224

Recent Cyber-attacks

- "Black Energy" (2011…2014)
  - Malware discovered on internet-connected HMIs
  - Targeting HMI products from three vendors: GE, Siemens, BroadWin
- "Havex" Remote Access Trojan (2014)
  - Targeting OPC communications
  - Client/server technology widely used in process control systems
- German Steel Plant (2014)
  - 'Spear phishing' emails and social engineering techniques
  - Blast furnace could not shut down as normal and caused "massive damage"
- Ukraine Electric Grid Attack (2015)
  - Sophisticated attacks: malware, a denial of service and "final component"
  - Undesirable state changes lead to the outage

Advanced Persistent Threat (APT)

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- Becoming more sophisticated
  - multiple stages and multiple options for each stage

Phishing email & social engineering	Install Remote Access Trojan (RAT) in office PC	Network mapping & lateral movement	Exploit vulnerability & pivot to SCADA network	Deploy SCADA attack payload	Attack physical system functions
• Waterhole attacks • Infected software • Stolen/insecure username and password credentials • Compromise from the internet	• Office PC • Third party remote maintenance • Engineer's laptop • BYOD	• Well known tools like nmap • Havex, Stuxnet sniffed traffic • RAT can keylog credentials	• Vulnerable operating system • Vulnerable services on SCADA server, data historian, etc. • Vulnerable network devices	• Variety of known and unknown vulnerabilities in SCADA devices and software – CVEs • e.g. GE, Siemens, BroadWin	• Inherently vulnerable SCADA protocols • Devices vulnerable to freeze, shutdown, etc.

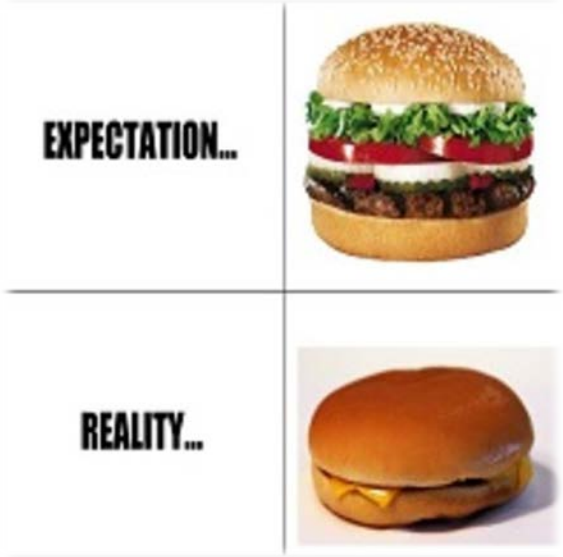
Can we prevent/detect all of them?
Should we? Really?

EU FP7 Programme Contract No. 608224

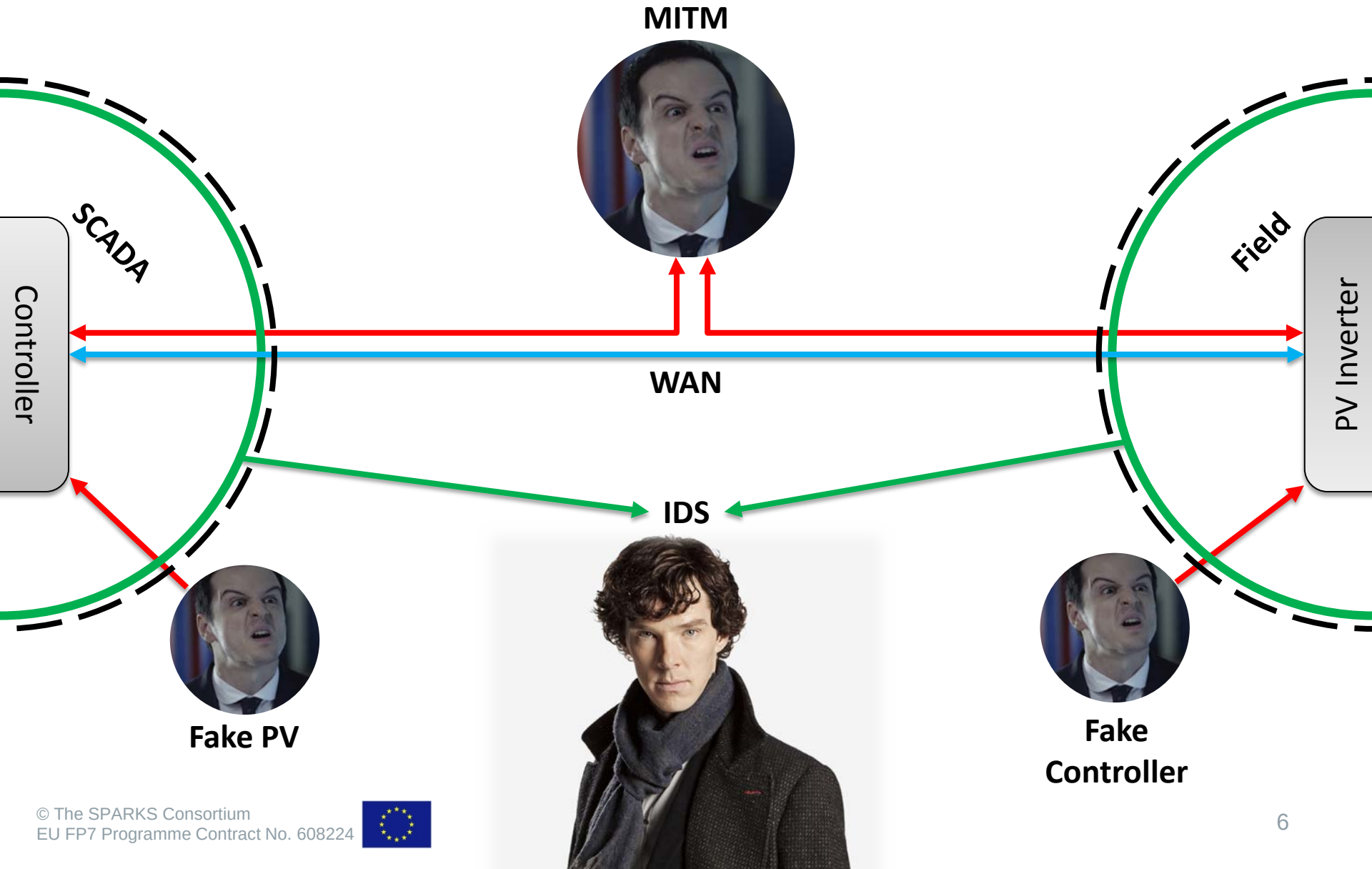
Countermeasures

- Security Recommendation/Enhancement
  - authentication, access control, encryption, …
  - IEC 62351 recommends the use of TLS and X.509 certificates

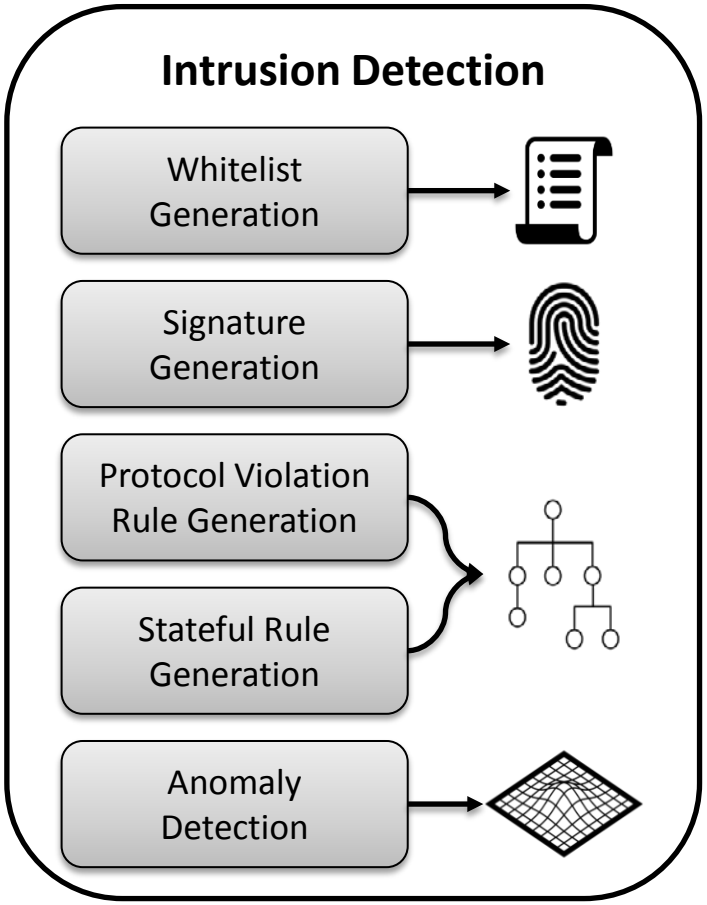
Always…

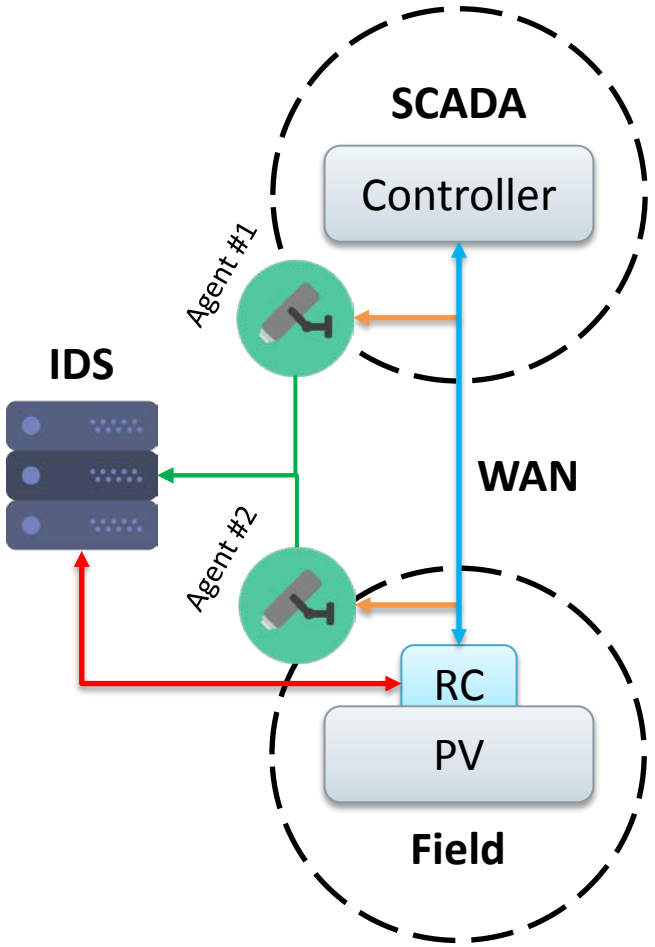


Intrusion Detection



Intrusion Detection





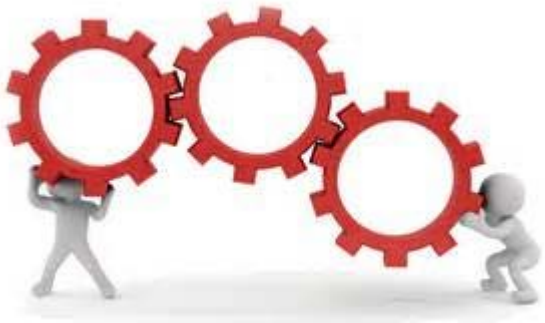
mirrored traffic

local information and alerts

global information and alerts & device information from RC

Alerts

- Alerts to other countermeasures
  - attack
    - illegal connection
    - abnormal traffic
    - man-in-the-middle
      - eavesdrop, manipulation, injection and drop
  - suspicious source/path
  - original data
  - other compromised device information
  - …



Visualization

- Elasticsearch + Logstash + Kibana (ELK)