Security of Cyber-Physical Systems

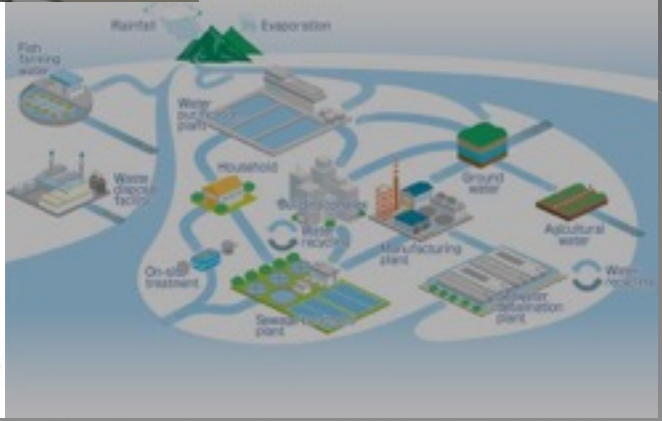
By Priya Mishra, Randy Halim, and Kristen McIntosh

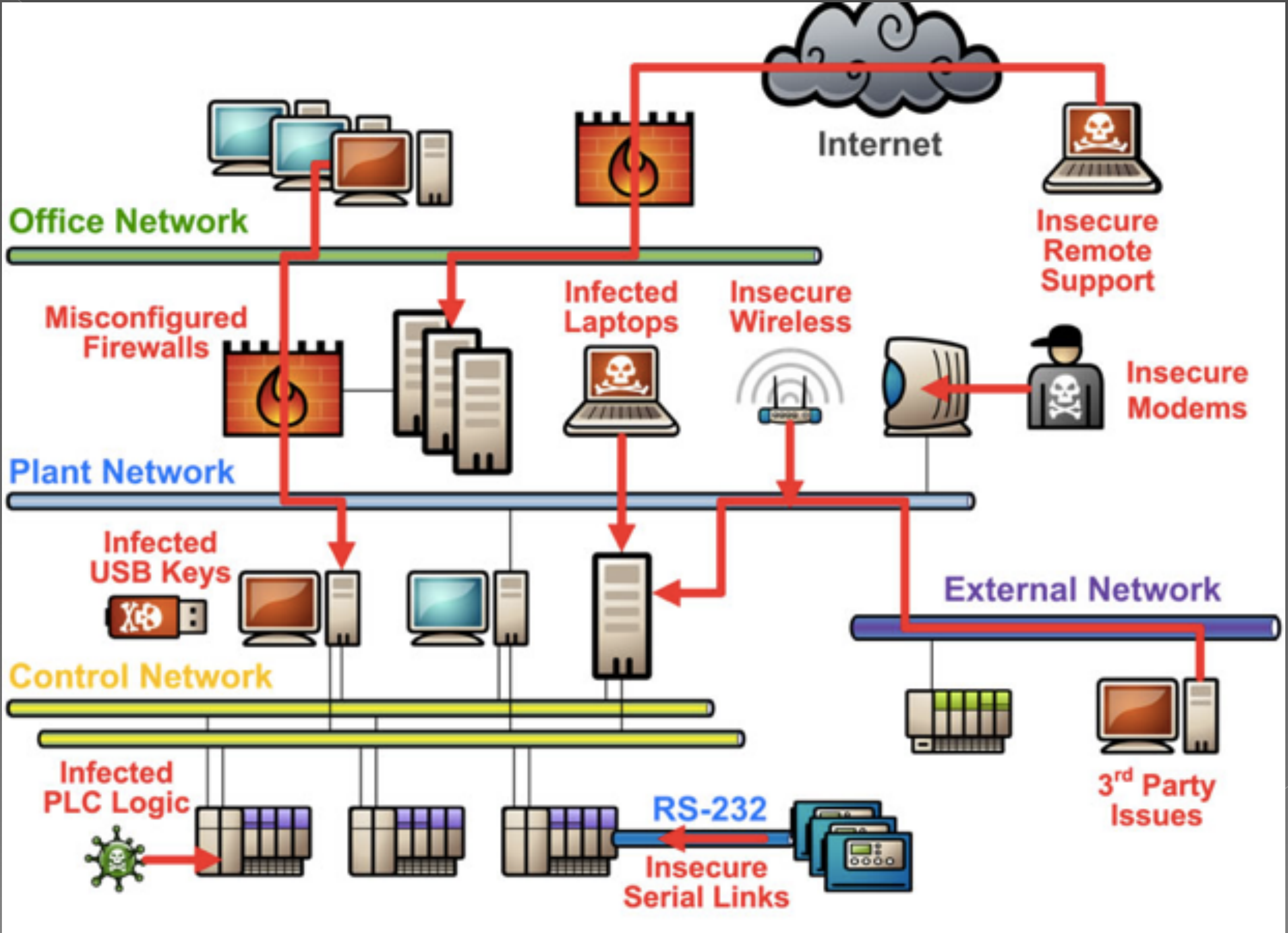
What is a cyber-physical system?

integration of physical processes, computational resources, and communication capabilities

What is a cyber-physical system?

Types of Infrastructures




Internet
Office Network
Insecure
Remote
Support
Misconfigured
Firewalls
Infected
Laptops
Insecure
Wireless
Insecure
Modems
Plant Network
Infected
USB Keys
External Network
Control Network
Infected
PLC Logic
RS-232
Insecure
Serial Links
3rd Party
Issues

Ignalina nuclear power plant (1992)

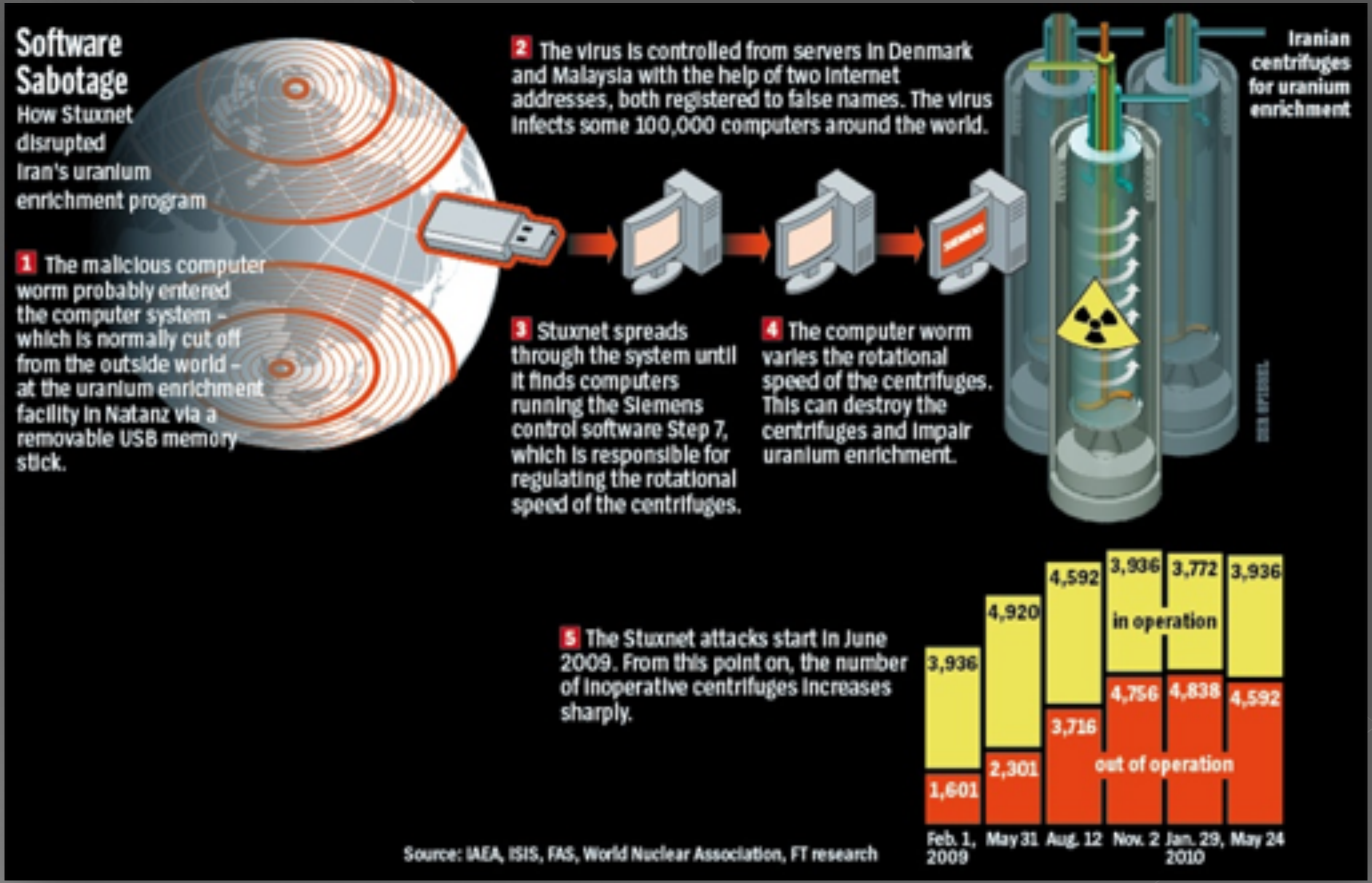
- Lithuania
- technician intentionally introduced a virus
- little harm caused
- illustrates dangers of insider attacks

Stuxnet

- A computer worm
- Exposed in 2010
- Attacked:
  - Natanz Nuclear facility
  - Bushehr Nuclear power plant

Stuxnet

- How?



Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.

Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

Korea Hydro and Nuclear Power Co.

- Phishing emails to employees
  - Clicking on the links caused malware to be installed
- Hackers stole data such as blueprints and manuals
- Extortion attempt

How can CPS attacks be prevented?

- Address the following potential issues:
  - Vulnerabilities
  - Government
  - Employees

Vulnerabilities

➢Threats to security systems have been changing and evolving more rapidly than expected. The current “signature based” approach that relies on known malicious threats is no more to be relied on.

➢Corporations need cyber-defenses that provide real time updates and make use of models that can detect suspicious activities in no time and respond to potential attacks automatically after detecting.

➢Since the infrastructures rely on the security systems on a daily basis, the security updates are being avoided in order to avoid disruptions caused by security updates.

➢Many or most companies avoid replacing old security systems with new ones as they are not cost effective. However, this is not a good approach as security is being compromised big time in order to save a few bucks and some time! The companies need to understand the threats and the risks of sticking to old security systems which are not effective enough anymore.

Corporations & Government

- cooperation of government and industry on cybersecurity.
- It is not easy for the companies to share cyber-attack information openly with the government. Nor can the government access attacks and provide assistance to companies easily.
- According to Kate (Forbes Staff), we need clear legislative guidelines for sharing cybersecurity information between the government and the private sector, and liability protection for companies that do so.

Employees

- One of the priorities must be well training and education of employees so that when charged with protecting corporate and/or government networks, they're well prepared.
- Employees must not have access to all the information ahead of need. Trusting employees is necessary but security must be a priority. There must also be security against employees. "Many of the organizations that are so fixated on perimeter security give implicit trust to anyone who walks through their doors" says Chriss Stoneff in one of his articles.
- Background check of employees! Employees (or former employees) could have unknown and wrong intentions or can be manipulated by an outside attacker to get access to inside systems. This is one thing that companies cannot well avoid but the best they can do is again, focus on tight security systems not making it easy for an attacker to succeed.

Questions

1. What are the main components/criteria of CPS?
2. What exactly did Student do to sabotage nuclear facilities in Iran?
3. What is the greatest help to attackers of CPS? How can this threat be reduced?

Questions

1. What are the main components/criteria of CPS?
2. What exactly did Student do to sabotage nuclear facilities in Iran?
3. What is the greatest help to attackers of CPS? How can this threat be reduced?

1. physical processes, computational resources, communication capabilities
2. Caused centrifuges to spin too fast and break apart thus impairing the uranium enrichment process
3. Employees. Ensure that they are adequately trained & do background checks

The End!

https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf

http://arxiv.org/pdf/1202.6144.pdf

http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5724910&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5724910