Industrial Automation
(Automação de Processos Industriais)

PLC Network Security

http://users.isr.ist.utl.pt/~jag/courses/api1819/api1819.html

Prof. José Gaspar, rev. 2018/2019

Some pointers to PLC security

Bibliography:

- **On PLC network security**
  Asem Ghaleb, Sami Zhioua, and Ahmad Almulhem
  International Journal of Critical Infrastructure Protection 22, 2018

- **The real story of Stuxnet**
  D. Kushner
  IEEE Spectrum, 3(50), pp.48-53, 2013.

Online Videos:

STUXNET: The Virus that Almost Started WW3 - YouTube (~3min)
https://www.youtube.com/watch?v=7g0pi4J8auQ

American Blackout - National Geographic (Full Movie) Cyber Attack
https://www.youtube.com/watch?v=zNfJkMPTtWQ
YouTube (~1h30min)

*Cloud **cyber-physical systems** are the natural evolution of **embedded systems** based on trends which may be observed in various domains [Jirkovsky18].*

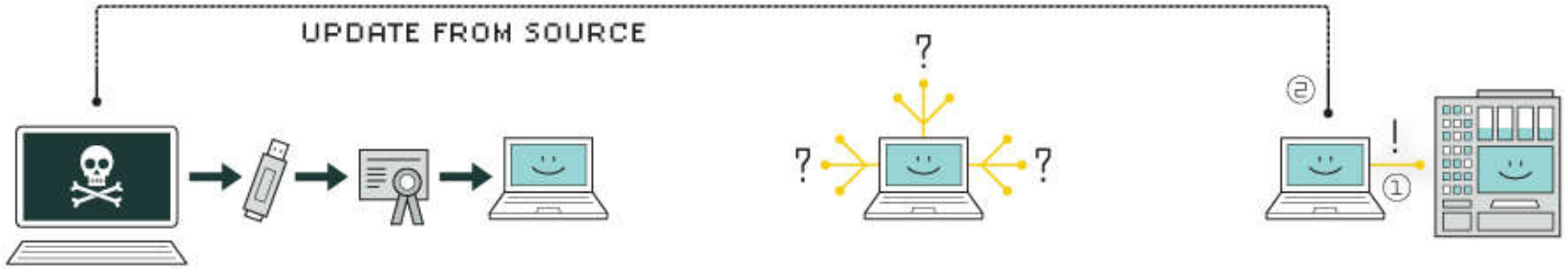
2010 - The **Stuxnet worm is detected**. It is the first worm known to attack SCADA (supervisory control and data acquisition) systems [Kushner18].

2011 - The Duqu worm is discovered. Unlike Stuxnet, to which it seems to be related, it was designed to **gather information** rather than to interfere with industrial operations.

[Jirkovsky18] OPC UA Realization Of Cloud Cyber-Physical System, V. Jirkovský, P. Kadera and M. Obitko, IEEE Int. Conf. on Industrial Informatics (INDIN) 2018

[Kushner18] The real story of Stuxnet, D. Kushner, IEEE Spectrum, 3(50), pp.48-53, 2013.

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

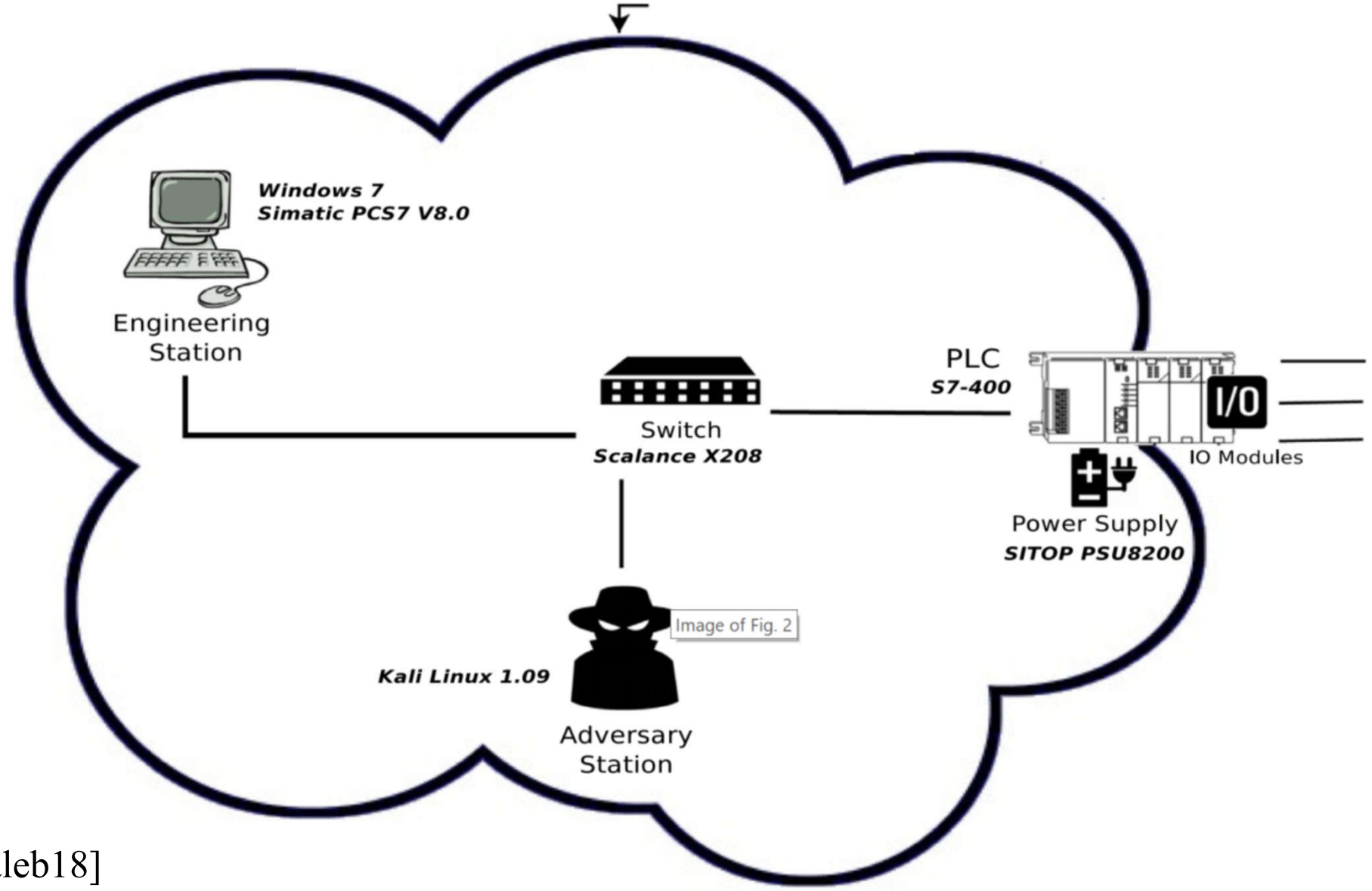
4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

https://spectrum.ieee.org/image/MjIyMTQzMg.jpeg

PLC Network Security



[Ghaleb18]

PLC Network Security

Examples of attacks:

- **Replay attack** – three steps (i) make the engineering station send one command (start, stop, etc) to the PLC, (ii) capture the packets, (iii) replay the captured packets at a later time.

- **Man in the middle attack** – Insert an attacker in between the engineering station and the PLC. Address Resolution Protocol (ARP) poisoned.

- **Stealth command modification attack** – Combination of the previous two methods. Interfering with sent commands by replaying other commands in a stealth way.

[Ghaleb18]

PLC Network Security – Challenges & Solutions

Industry 4.0 / Cyber Physical Systems protection

- **Firewalls** – Avoid field-buses direct access. Run traditional **field-buses just at the factory** floor. PLC programming (LD / IL / ST / SFC) **still to run as learned** in this course.

- **Hardware low level protection** – Separate local area networks (LANs) from the wide (global) area network (WAN). Use **dedicated hardware** and software to bridge the WAN to the LANs.

- **Industrial secure protocols** – Use knowledge, HW and SW from the telecommunications global market. **Open Platform Communications** (OPC), formerly OLE for Process Control (Object Linking and Embedding for …) already contains security features. OPC Unified Architecture (OPC UA), *extended to the field level may end the fieldbus wars [www19]*.

[www19] https://drivesncontrols.com/news/fullstory.php/aid/5851/Extending_OPC_UA_to_the_field_level__91will_end_fieldbus_wars_92.html (accessed Mar2019)