Cyber Threats, the World is no Longer what we Knew…

Presented by S. Perez

Commissariat à l’Energie Atomique et aux Energies Alternatives,
CEA/DIF, Bruyères le Châtel, 91297, Arpajon, France

Email: stephane.perez@cea.fr
Help, We’ve been Hacked…!
ICS Cyber Threats

Office Report Level

Enterprise Network (Level 3)

Internet Remote Access

Supervisory System

PLC Network (Level 1)

SCADA Network (Level 2)

SCADA Server

PLC Level

RS-485 Bus (Level 0)
ICS Cyber Threats

Internet Remote Access

Supervisory System

Office Report Level

WiFi Remote Access

PLC Level

Remote Access

Enterprise Network (Level 3)

SCADA Network (Level 2)

PLC Network (Level 1)

RS-485 Bus (Level 0)
ICS Cyber Threats

- Compromised Office Desktop
- Bad Fire Wall Rules

Non Secure WiFi AP
Infected Prog

Non Protected Remote Working

Compromised Remote Access
Infected USB Key
Infected Maintenance PC
ICS Vulnerabilities Stats...

Top Level: SCADA & PLCs

Vulnerabilities in various ICS components

Number of vulnerabilities in ICS components (by vendor)

Total number of vulnerabilities discovered in ICS components

2008: Attack on the BP Baku-Tbilisi-Ceyhan Turkish Pipeline

- Combined physical and cyber attack
- Attack through the wireless network
- Security alarms disconnection
- Survey cameras disconnection

→ Equipment destruction (20 days of indisponibility)
→ More than $1 Million loss

- Defense in Depth
  - Physical access improvement
  - Use of network layers
  - Securing wireless and camera networks
2008 : Emergency Stop in a Nuclear Plant (Hatch Georgia)

- Computer update
- System restart
- Plant connection, synchronization
- Control system’s data set to zero for a brief moment…

→ plant’s Unit 2 set into automatic shutdown for 48 hours

- Setup of updates protocols
- Network separation between critical systems and Data Servers
- Strong partnership with software providers on updates consequences
- Updates tests protocols

Unintended consequence of a contractor update
Hackers took control of the Payment App.
Manipulation of the SCADA with no Knowledge of the System

→ Hackers manipulated the PLC’s that managed the amount of chemicals used to treat the water to make it safe to drink

- SQL injection and phishing
- Login credentials stored on the frontend Web server
- Unpatched Web vulnerabilities exploitation
- Same computer managed SCADA and Web Services

→ Network separation between SCADA and payment apps
- Strong authentication
- Regular analysis of Web exposed apps
2013 : Target → 40 Million Credit Cards Stolen

- Trojan Horse (BlackPos) delivered in an email
- Attack through a small heating and air conditioning firm in Pennsylvania
- Direct communication with the point of sale servers through the core network

→ 40 Million Credit cards sold on the black market
→ $200 Million refund from Banks
→ High-ranking employees lost their jobs including the CEO

- Efficient protection belong the Payment Card Industry Cert.
- Strong authentication for the distant access
- Network separation
- Use of a Security Operation Center (SOC) for alarms detection and analysis

Source : Case Study: Critical Controls that Could Have Prevented Target Breach, SANS Institute
Target invests $5 million in cybersecurity coalition

February 18, 2014 In an open letter published in newspapers across the country in January, Gregg Steinhafel, chairman, president and chief executive officer, announced a new coalition to help educate the public on the dangers of scams.

A group of nationally recognized, respected cybersecurity organizations in cybersecurity and consumer protection will launch a campaign to educate consumers about cybersecurity and the dangers of phishing scams. Target will invest $5 million in a multi-year campaign for this effort.
States and Labs are Concerned…

If you are not a lab employee, complete the following training within 30 days of being given your computing account:

- **Course CS100: Cyber Security for Laboratory Users Training**

This course must be taken every year to keep the account active.

SLAC employees should take Course CS200.

**SLAC Cyber Security Training is required** to maintain a SLAC computer account. If you do not complete the training within 31 days of its due date, access to your SLAC computer account will be blocked. You will not be able to log in again until after you complete the required training.

How to Complete SLAC Cyber Security Awareness Training:

If you are using a computer issued by SLAC Computing or are using VPN, you can click the blue Launch Web Course button on this page: [https://www-internal.slac.stanford.edu/esh-db/training/alconly/bin/catalog_item.asp?course=CS100](https://www-internal.slac.stanford.edu/esh-db/training/alconly/bin/catalog_item.asp?course=CS100)

---

**Overview**

At CERN, due to its unique academic environment and the associated academic freedom, computer security has been delegated to CERN's users:

**At CERN, the individual users are in first instance responsible for securing their computers, networks, data, systems & services.**

The Computer Security Team and the IT department are ready to help users assuming this responsibility assist you in this. On this Web site, you can find:

- The CERN Computing Rules, i.e. the "Dos" and "Don'ts" for using CERN's computing facilities;
- Recommendations, i.e. tips, hints & best practices intended to helping you to properly assume this responsibility;
- Training courses and material for starters & experts;
- Security Services provided for you by the Computer Security Team; and
- Reports & Presentations featuring monthly reports, theses, reports from conferences, dedicated presentations & much more.

© Copyright 2017 CERN Computer Security Team

Please use the following PGP key to encrypt messages sent to CERN Computer Security Team: <Cryptographer, Security@cern.ch>

+49228 8264 8088 8088 D632W 86432 W3A1 8234 6426 8254
States and Labs are very Concerned…

Complete required training

Once you guest appointment has been approved, you must complete the online training modules before experiments may begin. The general User training modules described in this section should be completed online prior to arrival at BNL. Please complete the following training courses:

- General Employee Radiation Training*
- NSLS-II Safety Module
- Cyber Security Training
- Guest Site Orientation

*If you have completed BNL GERT training in the past, then you may take the GERT Challenge Exam to renew your GERT training.

LIGO implemented a cybersecurity plan in 2004
- General level of security awareness within Laboratory has increased

Fermilab’s Computing Policy is a set of mandated user and system behaviors designed to:

- operate an effective and efficient computing and networking environment;
- maintain an open environment supporting global collaboration and innovation and free exchange of scientific information;
- guard the laboratory’s reputation and protect its computing systems, data, and operations against attacks and unauthorized use;
- ensure compliance with all applicable mandates, directives and legal requirements for computing.
How to deal with security?

- Defense in Depth
- USB Key handling
- Outsourcing Management
Defense in Depth

SCADA Network

Intrusion Prevention
Defense in Depth

SCADA Network

Critical Assets

Intrusion Prevention
Defense in Depth

- Firewall
- SCADA Network
- Critical Assets
- Intrusion Prevention
The Brand New USB Killer

Killer USB
Drive that can explode your Computer
The Brand New USB Killer

Killer USB
Drive that can explode your Computer

200v 5v

USB KILLER V3
49.95 €

USB KILLER V3: 1.5x Power, 2x Faster Surges, 2x Stable
Choose your edition:
© Anonymus Edition: No brand, no text, 100% discrete, or
© Standard Edition: White Case, USB Kill Logo + Text
GO PRO, SAVE BIG: Get the USB Kill Professional Kit (USB Killer, Test Shield & Adaptor Kit)
and get a 20% instant discount and free worldwide shipping! (Applied at checkout)

Stéphane PEREZ| ICALEPCS October 2017 | PAGE 23
How Does People React?

Nearly 300 Flash Drives Test Dropped in a Large University Campus*…

(a) Unlabeled drive  (b) Drive with keys  (c) Drive with return label  (d) Confidential drive  (e) Exam solutions drive

<table>
<thead>
<tr>
<th>Drive Type</th>
<th>Opened</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential</td>
<td>29/58</td>
<td>(50%)</td>
</tr>
<tr>
<td>Exams</td>
<td>29/60</td>
<td>(48%)</td>
</tr>
<tr>
<td>Keys</td>
<td>29/60</td>
<td>(48%)</td>
</tr>
<tr>
<td>Return Label</td>
<td>14/59</td>
<td>(24%)</td>
</tr>
<tr>
<td>None</td>
<td>27/60</td>
<td>(45%)</td>
</tr>
</tbody>
</table>

Users Really Do Plug in USB Drives They Find

Mathew Tischer†  Zakir Durumeric‡  Sam Foster†  Sunny Duan†
Alec Mori†  Elie Bursztein§  Michael Bailey†

† University of Illinois, Urbana Champaign  ‡ University of Michigan  § Google, Inc.

†tischer1, sfoster3, yduan2, ajmor2, mdbailley@illinois.edu
‡zaki@umich.edu  elieb@google.com

*University of Illinois, Urbana-Champaign campus, 2015
A simple $35 USB Test…

Files Transfer
.pdf
.pptx
.docx
.xlsx
...

Trusted USB Key

Raspberry or Portable Device

6.2.1 USAGE OF USB STICKS

The usage of USB sticks being connected to devices on the TN/EN must be avoided by any means and alternative methods for file transfer like AFs, DFS, SAMBA, NFS must be used whenever possible. Failure to adhere to this rule will be considered as professional fault putting a risk to the TN/EN. If there are no alternatives to using USB sticks, users must:

- Use a dedicated USB stick and not reuse USB sticks which have already been used outside CERN (e.g. at an Internet café);
- Scan the USB stick on a PC solely connected to the GPN with up-to-date antivirus software and up-to-date virus signatures. Any indication of malware prohibits the further usage of that USB stick.
SOC and Data Analysis for What?

Log Survey for
- Realtime mapping
- Non authorized computer detection
- Account profiling
- IP spoofing and analysis
- Incident reports
- Protocol analysis
(in French): IVRE, il scanne Internet.
(in English): Know the networks, get DRUNK!
Why are Attacks so Successfull

- Password Policies are too weak
- Systems and Apps are not regularly Updated
- Weak balance between regular users and Admin accounts
- Balance between Money and Security → Money often wins…
- There is no separations between networks
- No access restrictions (devices)
- Outsourcing is not controlled
- Remote working is not controlled, including wifi
- Many recommendations but not enough users training
- No SOC
Do Not...

...Modify Procedures

...Use Non Tested or Appropriate Patch...

...Use bad Configuration for your Firewall
**ANSSI, 9 points Guide¹ (...and 40 more detailed rules**

1: Education

2: Knowledge of the System and Users

3: Authentication and Access Control

4: Secure Configurations for Terminal Devices

5: Secure Configurations for Network Devices

6: Secure Configurations for Administration

7: Remote Access Management

8: System Update Management

9: Survey, Monitor, React

**The 20 Critical Controls²**

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software


4: Continuous Vulnerability Assessment and Remediation

5: Malware Defenses

6: Application Software Security

7: Wireless Access Control

8: Data Recovery Capability

9: Security Skills Assessment and Appropriate Training to Fill Gaps

10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

11: Limitation and Control of Network Ports, Protocols, and Services

12: Controlled Use of Administrative Privileges

13: Boundary Defense

14: Maintenance, Monitoring, and Analysis of Audit Logs

15: Controlled Access Based on the Need to Know

16: Account Monitoring and Control

17: Data Protection

18: Incident Response and Management

19: Secure Network Engineering

20: Penetration Tests and Red Team Exercises

1 : Guide d’Hygiène Informatique, ANSSI, 2017

2 : SANS Institute 2014c
Recommendations

- Use National and Labs Standards for ICS and Cybersecurity (NIST, SANS, ANSSI, CERN CNIC Security Policy for Controls…)
- Be careful with non trusted USB Keys
- Be aware of contractors and sub contractors computers
- Use a SOC for ICS Supervising
- Write and maintain Security Systems Reports
The question is not to know IF but WHEN you’ll be hacked…