DE LA RECHERCHE À L'INDUSTRIE

cea

www.cea.fr

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

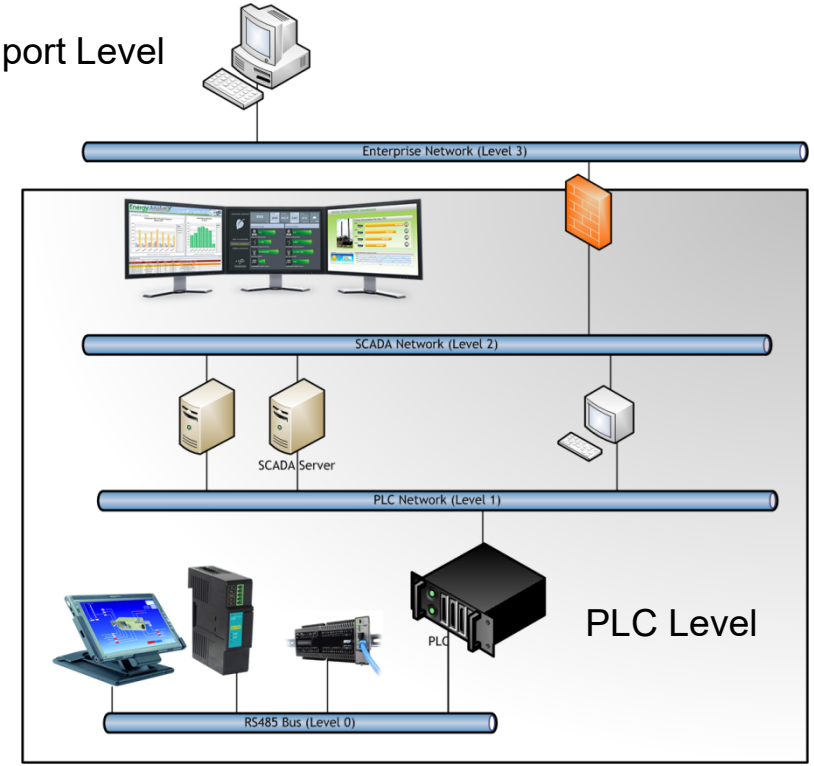
Presented by S. Perez

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

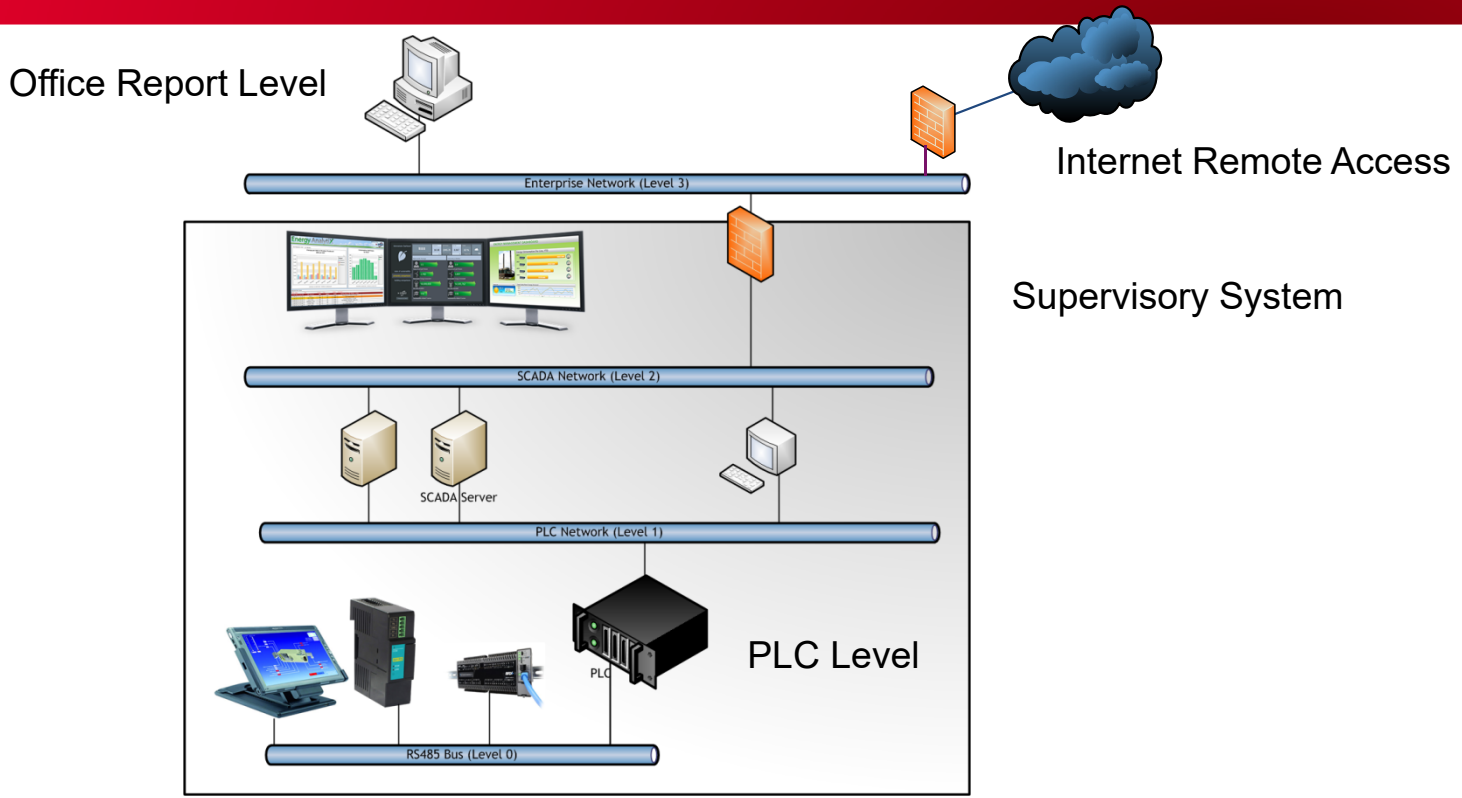
Email: stephane.perez@cea.fr

Help, We've been Hacked…!

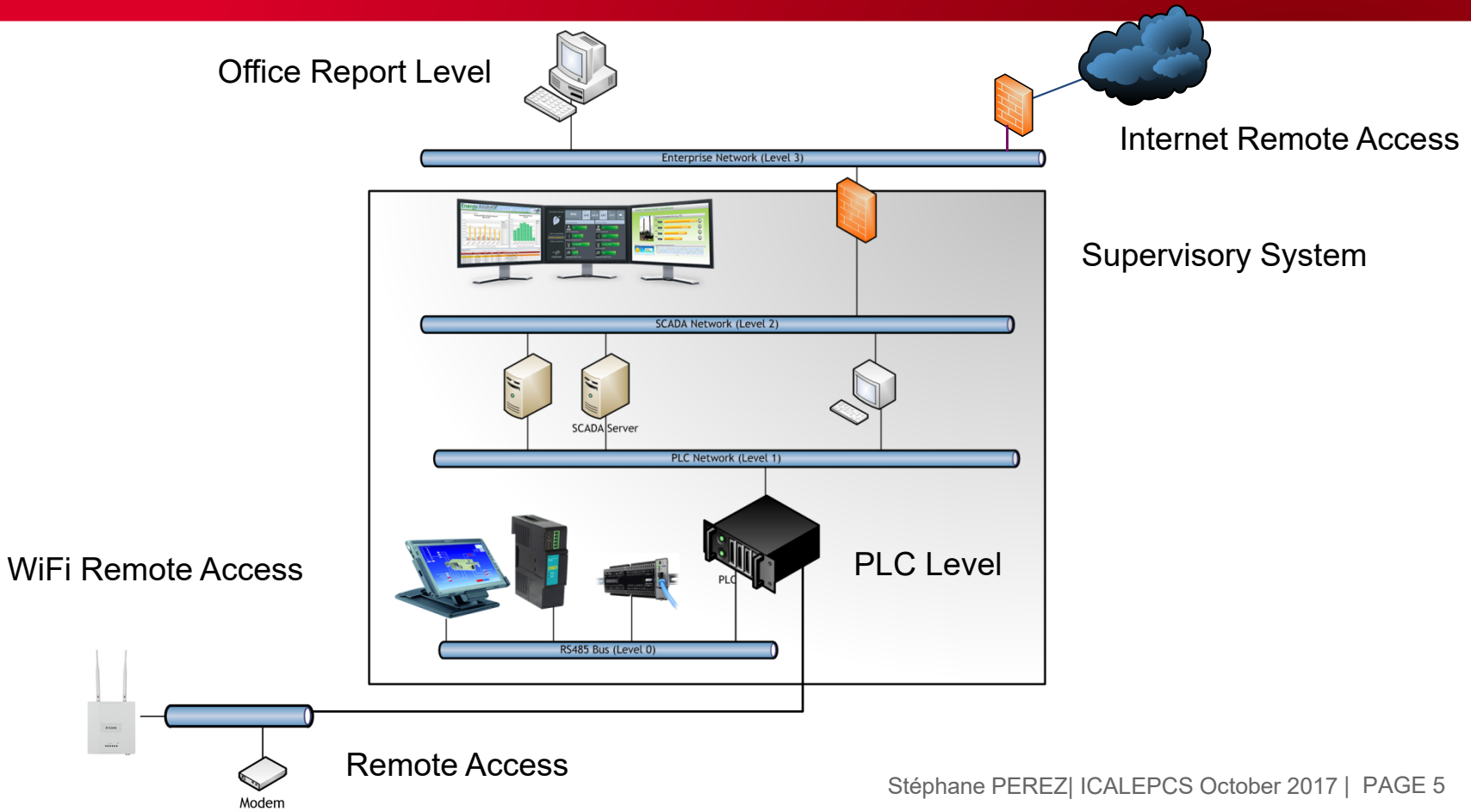
ICS Cyber Threats



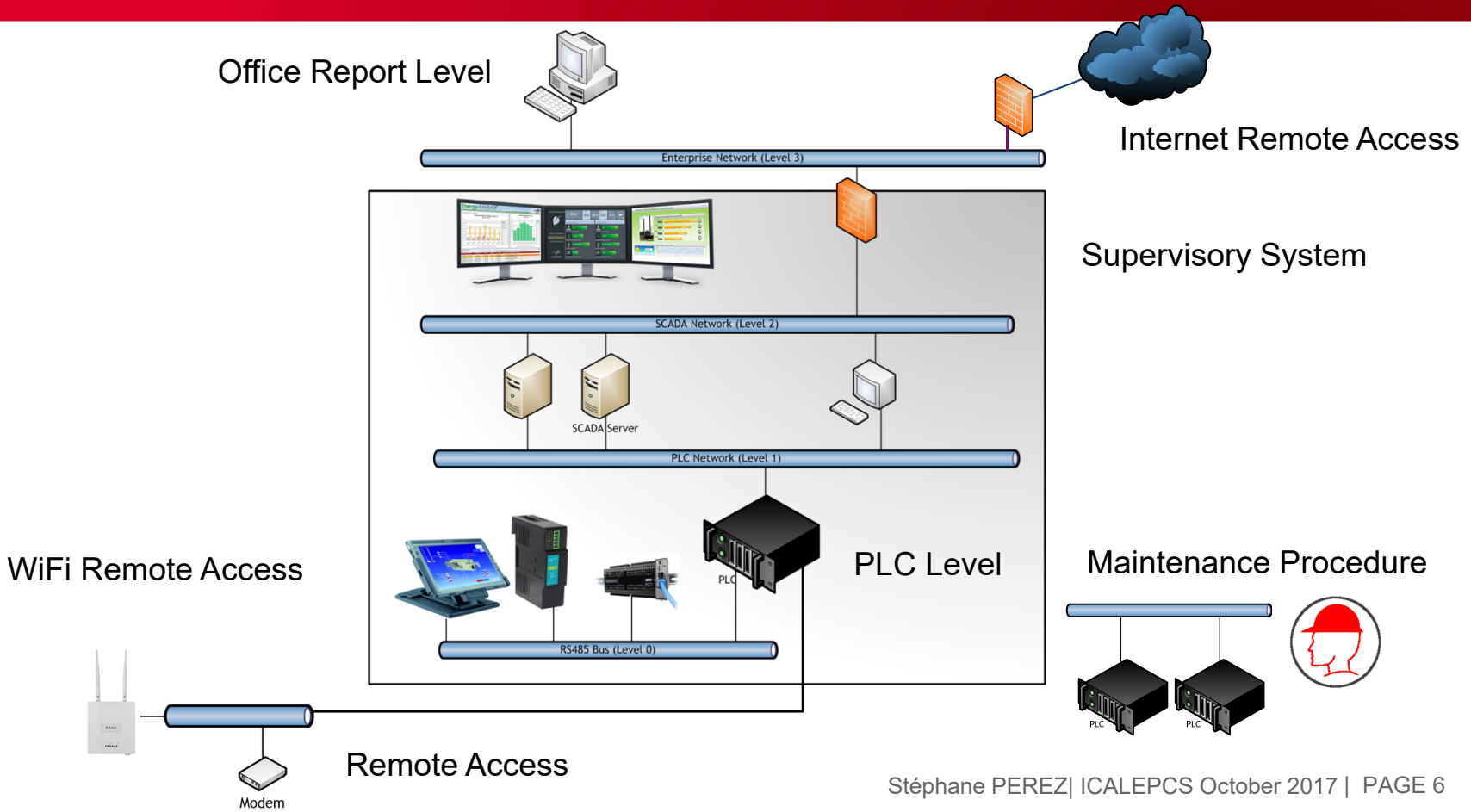
ICS Cyber Threats



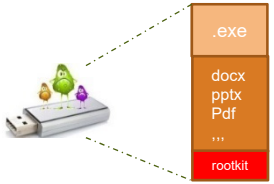
ICS Cyber Threats



ICS Cyber Threats



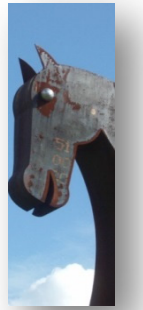
ICS Cyber Threats



Compromised Office Desktop

Bad Fire Wall Rules

Compromised Remote Access



Enterprise Network (Level 3)

Bad Fire Wall Rules

SCADA Network (Level 2)

SCADA Server

Infected USB Key

Non Secure WiFi AP

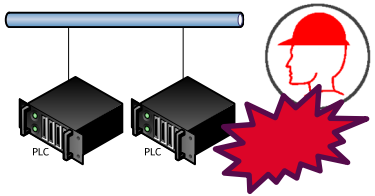
PLC Network (Level 1)

PLC Trapped

Infected Prog

RS485 Bus (Level 0)

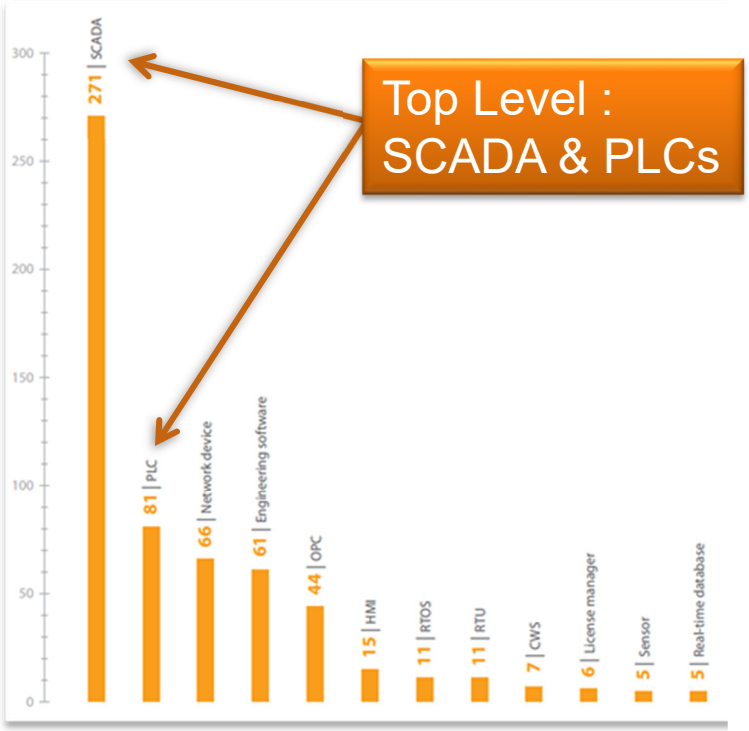
Infected Maintenance PC



Modem

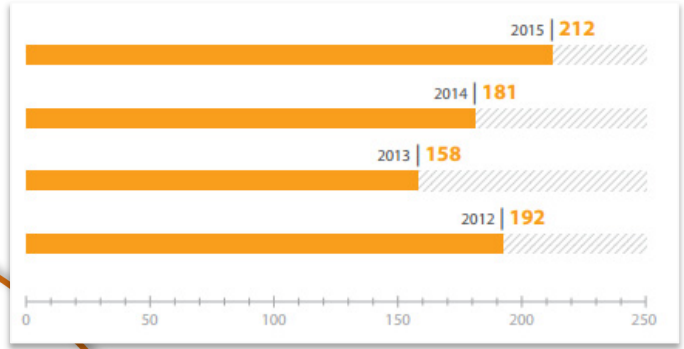
Non Protected Remote Working

ICS Vulnerabilities Stats…



Vulnerabilities in various ICS components

Total number of vulnerabilities discovered in ICS components



Number of vulnerabilities in ICS components (by vendor)

Source : Security Trends & Vulnerabilities Review – ICS - 2016

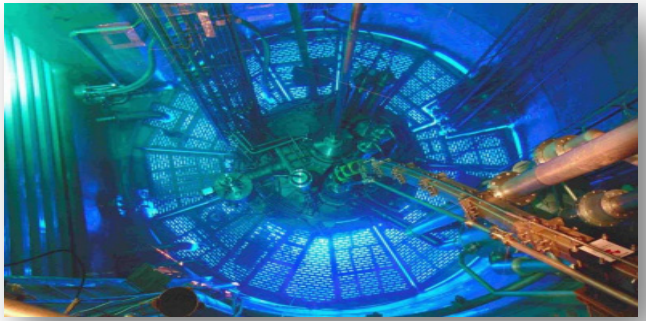
2008 : Attack on the BP Baku-Tbilisi-Ceyhan Turkish Pipeline

- 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

Unintended consequence of a contractor update

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

2015 : Chemical Settings Change at Water Treatment plant

- Hackers took control of the Payment App.
- Manipulation of the SCADA with no Knowledge of the System

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

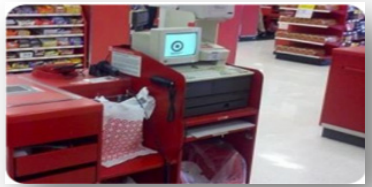
→ Hackers manipulated the PLC's that managed the amount of chemicals used to treat the water to make it safe to drink

- 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 Hack Consequences

Cyber Security Jobs →

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.

results for cyber security

Lead Engineer - Cyber Security
Brooklyn Park, Minnesota
07/20/2017

Lead Analyst - Enterprise Incident Management
Brooklyn Park, Minnesota
05/23/2017

Lead Engineer - Product Security (Application Security)
Brooklyn Park, Minnesota
05/31/2017

Sr Target Security Specialist
Minneapolis, Minnesota
06/29/2017

Target Security Specialist
Perth Amboy, New Jersey
07/13/2017

Sr Corporate Security Tech
Minneapolis, Minnesota
07/05/2017

Target Security Specialist
Woodbury, Minnesota
07/21/2017

Lead Analyst - Vendor Security
Brooklyn Park, Minnesota
06/27/2017

Sr. Analyst - Vendor Security
Brooklyn Park, Minnesota
02/02/2017

Sr Engineer - Cloud Security
Brooklyn Park, Minnesota
04/03/2017

Lead Engineer - Product Security

States and Labs are Concerned…

How Do I…?

- Protect Myself from Cyber Attacks
- Report Cyber Incidents
- Prepare My Family for a Disaster
- Report Suspicious Activity
- Find Overseas Travel Alerts
- Get a Homeland Security Job
- Do Business with DHS
- Verify Employment Eligibility (E-Verify)
- Find Student Resources
- Get a Green Card
- Check the National Terrorism Advisory System (NTAS)
- Find Training Opportunities
- File a Travel Complaint (DHS TRIP)

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/slaconly/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 practises 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.

ity@cern.ch

rded instructions.)

Please use the following PGP key to encrypt messages sent to CERN Computer Security Team <**Computer.Security@cern.ch**>
429D 6046 0EBE 8006 B04C DF02 954C E234 B4C6 ED84

States and Labs are very Concerned…

BROOKHAVEN NATIONAL LABORATORY
BROOKHAVEN SCIENCE ASSOCIATES

2 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*
- Cyber Security Training
- NSLS-II Safety Module
- 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.

Cyber Security Program
Office of the CIO

Policy 2329/4329 v3.3
June 2012

Proper Use of LLNL Computers

Statement of Policy
The following rules apply to all users of LLNL classified and unclassified computers; individual organizations may apply additional rules to the use of their resources, provided these additional rules are not in conflict with this policy. Questions concerning organization-specific rules should be addressed to your supervisor, manager, Information System Security Officer (ISSO), or Organizational Information System Security Officer (OISSO).

LIGO

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

Fermilab

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.

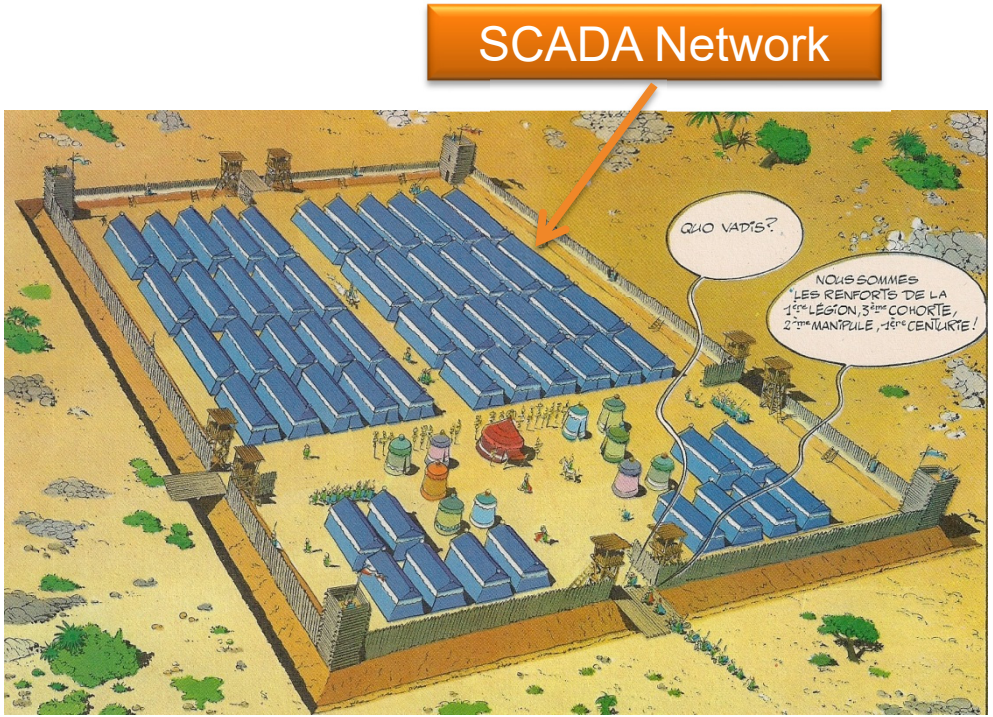
How to deal with security ?

- Defense in Depth

- USB Key handling

- Outsourcing Management

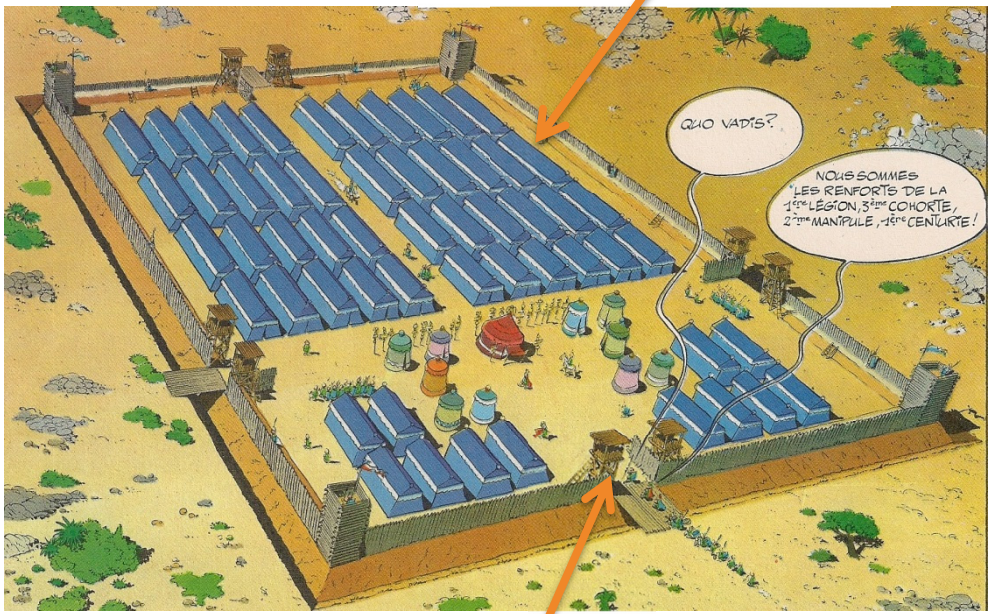
Defense in Depth



Astérix légionnaire, pl-32, 1ère édition Pilote, 1966, © 2015 Les Editions Albert René / Goscinny-Uderzo

Defense in Depth

SCADA Network

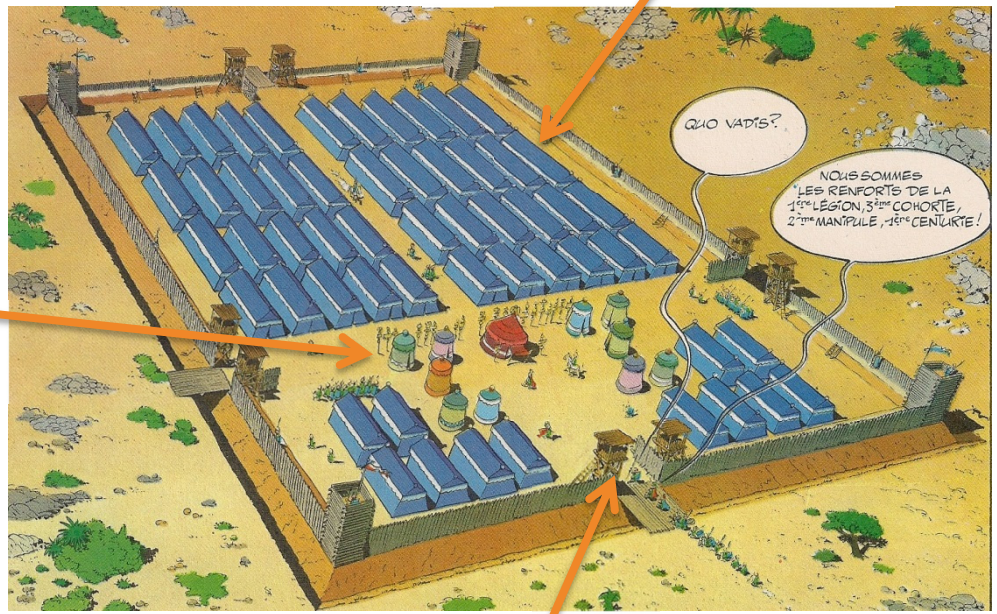


Intrusion Prevention

Astérix légionnaire, pl-32, 1ère édition Pilote, 1966, © 2015 Les Editions Albert René / Goscinny-Uderzo

Defense in Depth

SCADA Network



Critical Assets

Intrusion Prevention

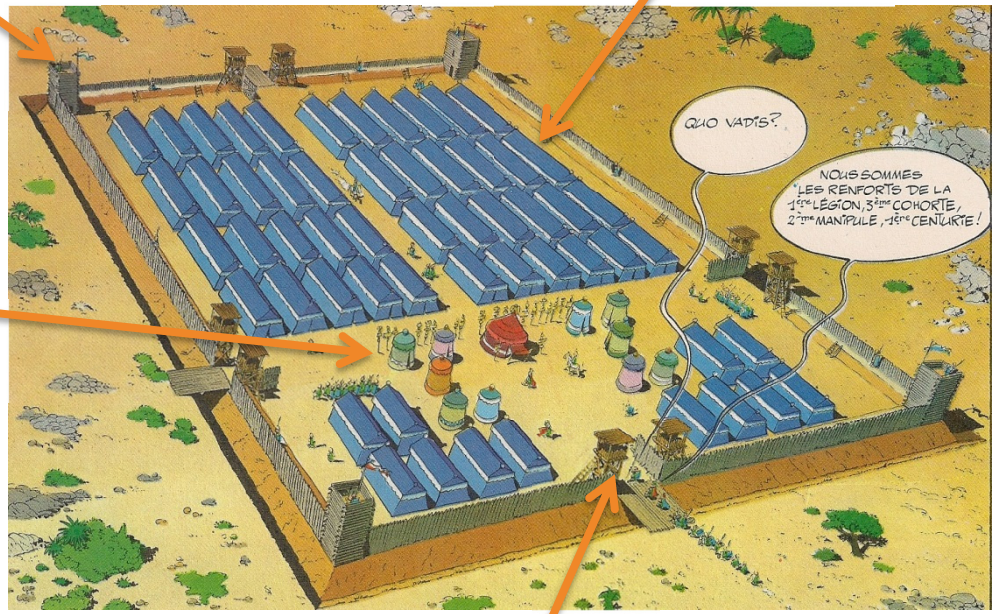
Astérix légionnaire, pl-32, 1ère édition Pilote, 1966, © 2015 Les Editions Albert René / Goscinny-Uderzo

Defense in Depth

Firewall

SCADA Network

Critical Assets



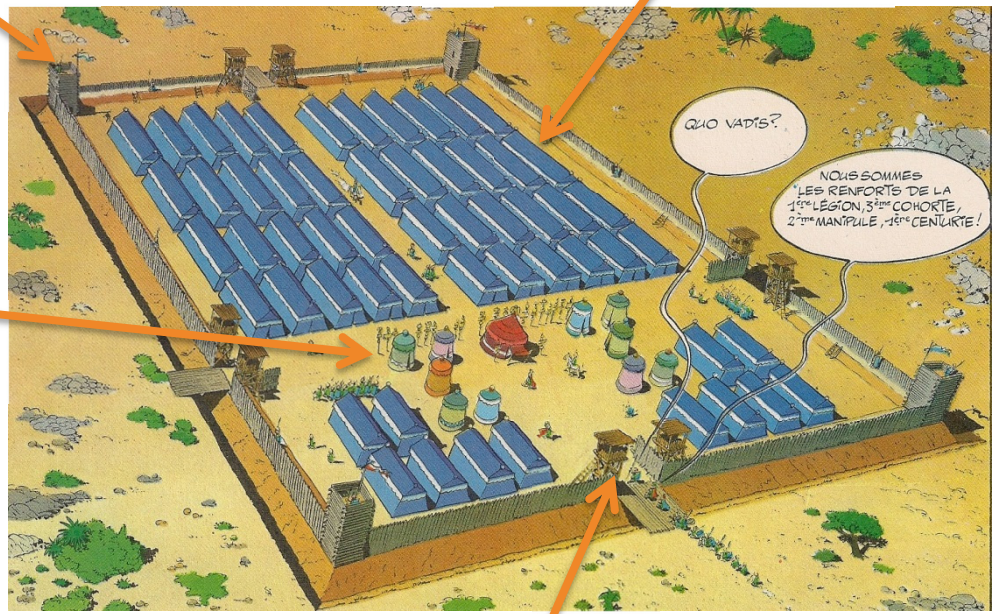
Intrusion Prevention

Astérix légionnaire, pl-32, 1ère édition Pilote, 1966, © 2015 Les Editions Albert René / Goscinny-Uderzo

Defense in Depth

Firewall

SCADA Network



Critical Assets

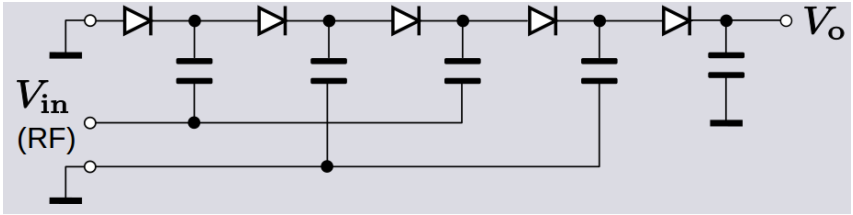
Credential Authority

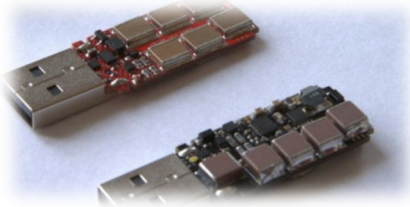
Intrusion Prevention

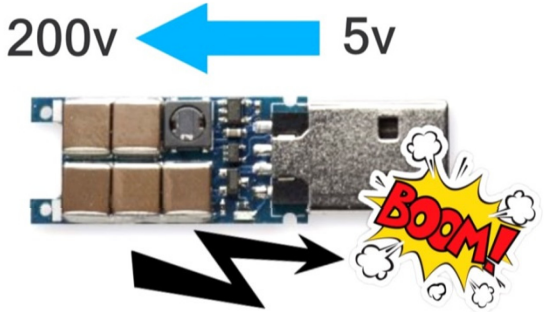
Astérix légionnaire, pl-32, 1ère édition Pilote, 1966, © 2015 Les Editions Albert René / Goscinny-Uderzo

The Brand New USB Killer

The Brand New USB Killer







USB KILLER V3

49,95 €

USB KILLLER V3: 1.5x Power, 2x Faster Surges, 2x Stable

Chose your edition:
Anonymous 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)*

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

Drive Type	Opened	
Confidential	29/58	(50%)
Exams	29/60	(48%)
Keys	29/60	(48%)
Return Label	14/59	(24%)
None	27/60	(45%)

Users Really Do Plug in USB Drives They Find

Matthew Tischer[†] Zakir Durumeric[‡†] Sam Foster[†] Sunny Duan[†]
Alec Mori[†] Elie Bursztein[◇] Michael Bailey[†]

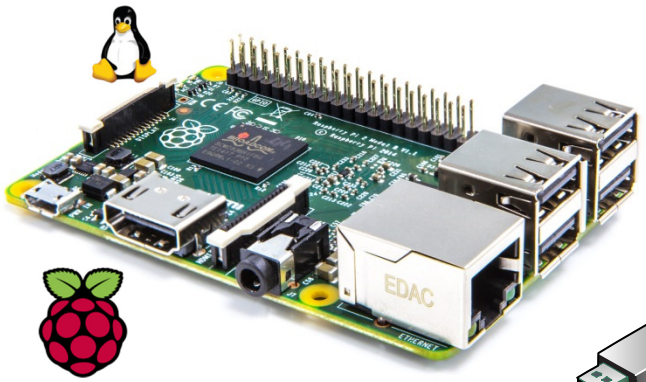
[†] University of Illinois, Urbana Champaign [‡] University of Michigan [◇] Google, Inc.
{tischer1, sfoster3, syduan2, ajmori2, mdbailey}@illinois.edu
zakir@umich.edu elieb@google.com

*University of Illinois, Urbana-Champaign campus, 2015

A simple $35 USB Test…

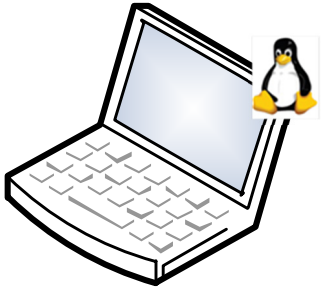
Files Transfer

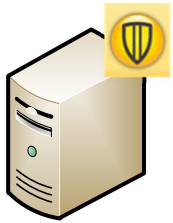
.pdf
.pptx
.docx
.xlsx
…



Raspberry or Portable Device

Trusted USB Key





CERN

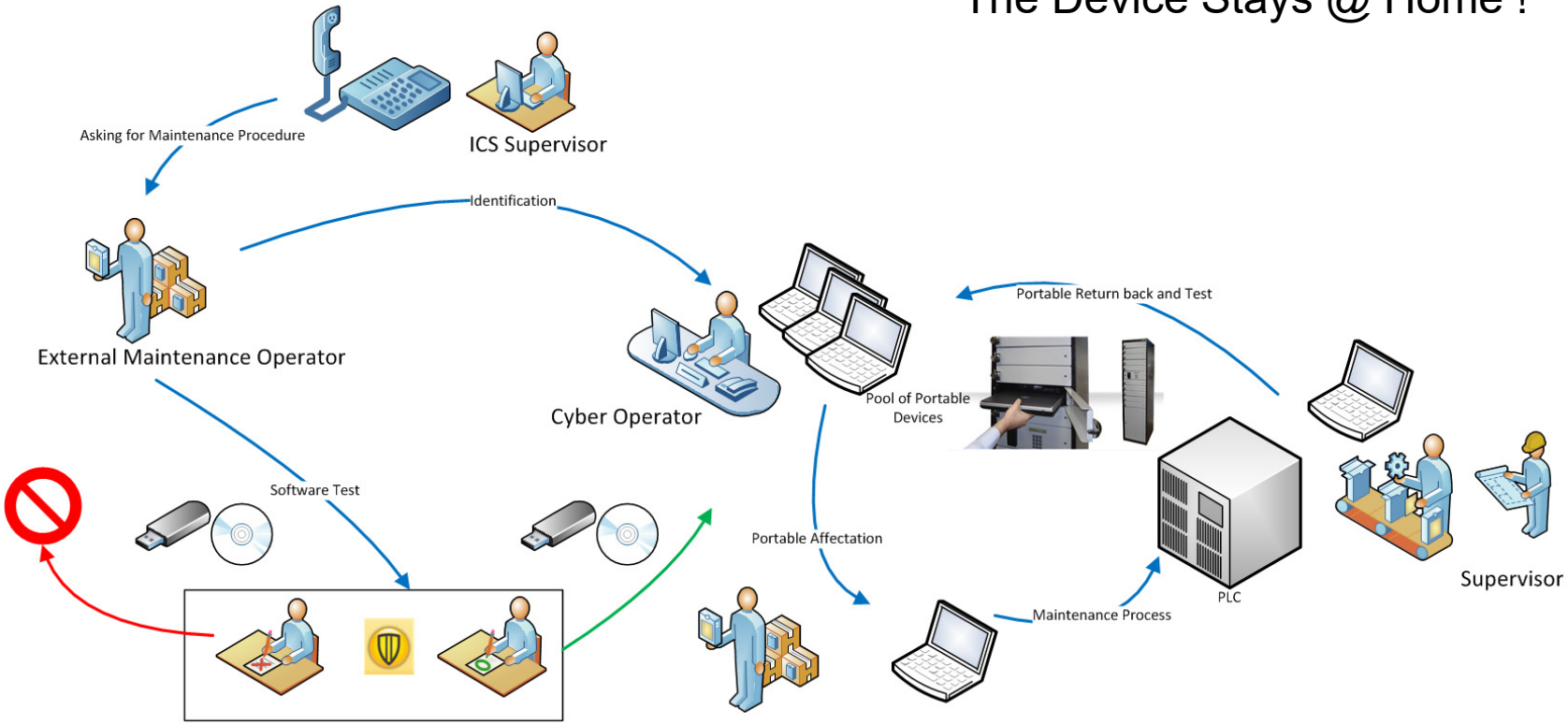
6.2.1 USAGE OF USB STICKS

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.

Managing Third Party Portable Devices

The Device Stays @ Home !



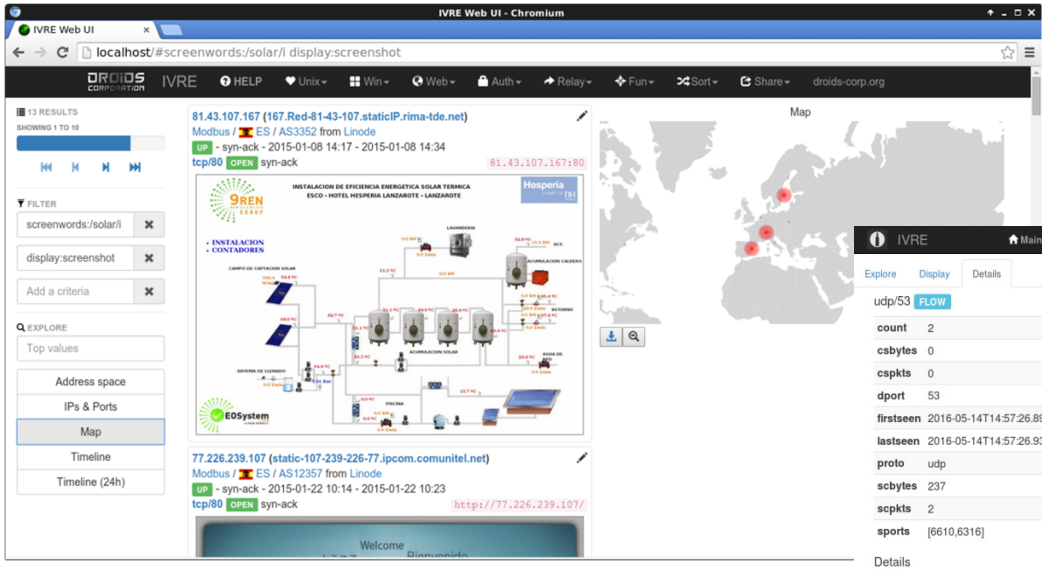
SOC and Data Analysis for What ?

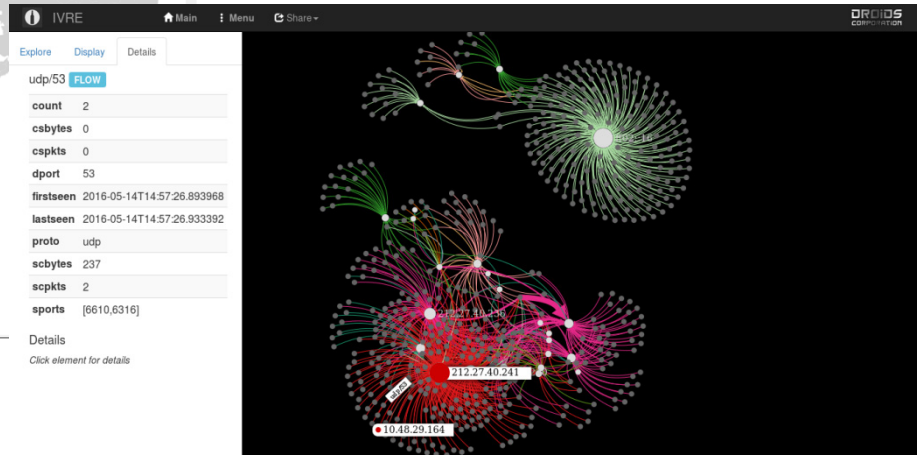
Log Survey for

- Realtime mapping
- Non authorized computer detection
- Account profiling
- IP spooffing and analysis
- Incident reports
- Protocol analysis

CEA IVRE Analysis Toolkit

(in French): IVRE, il scanne Internet.
(in English): Know the networks, get DRUNK!





About IVRE

IVRE is an open-source framework for network recon. It relies on open-source well-known tools (Nmap, Zmap, Masscan, Bro and p0f) to gather data (*network intelligence*), stores it in a database (MongoDB), and provides tools to analyze it.

It includes a Web interface aimed at analyzing Nmap scan results (since it relies on a database, it can be much more efficient with huge scans than a tool like Zenmap, the Nmap GUI, for example).

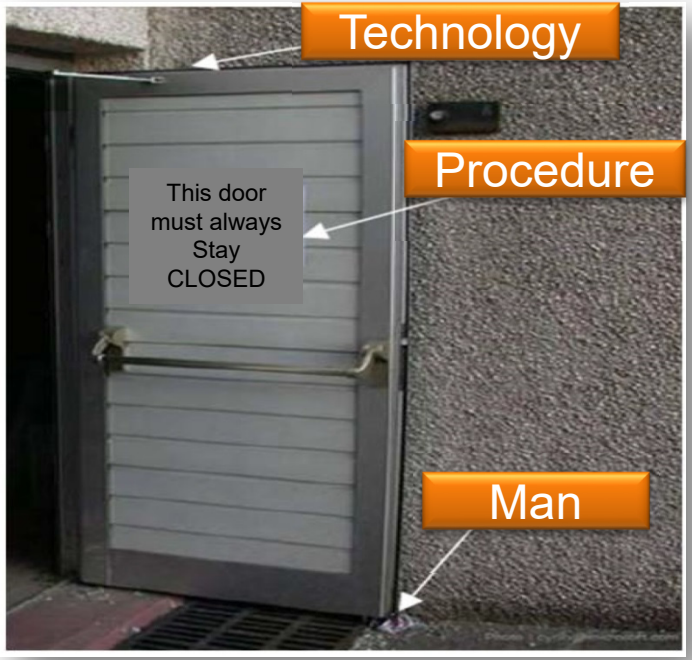
IVRE means *Instrument de veille sur les réseaux extérieurs*, and is French for DRUNK, *Dynamic Recon of Unknown NetworKs*.

It's free software, and it's on GitHub!

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

Read…

ANSSI, 9 points Guide[1] (…and 40 more detailled 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 Controls[2]
1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hard and Soft on Mobile Devices, Laptops, WS, and Servers
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 carefull 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

Hackers Through the Ages

The question is not to know **IF** but **WHEN** you'll be hacked…