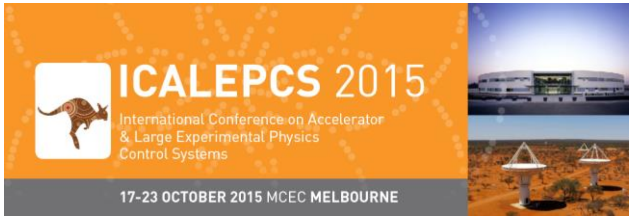
Finding Our Skeletons: Information Security Assessment of CERN Access and Safety Systems

Timo Hakulinen,
Pascal Oser, Xurxo Breogan Costa Lopez, Pierre Ninin
CERN

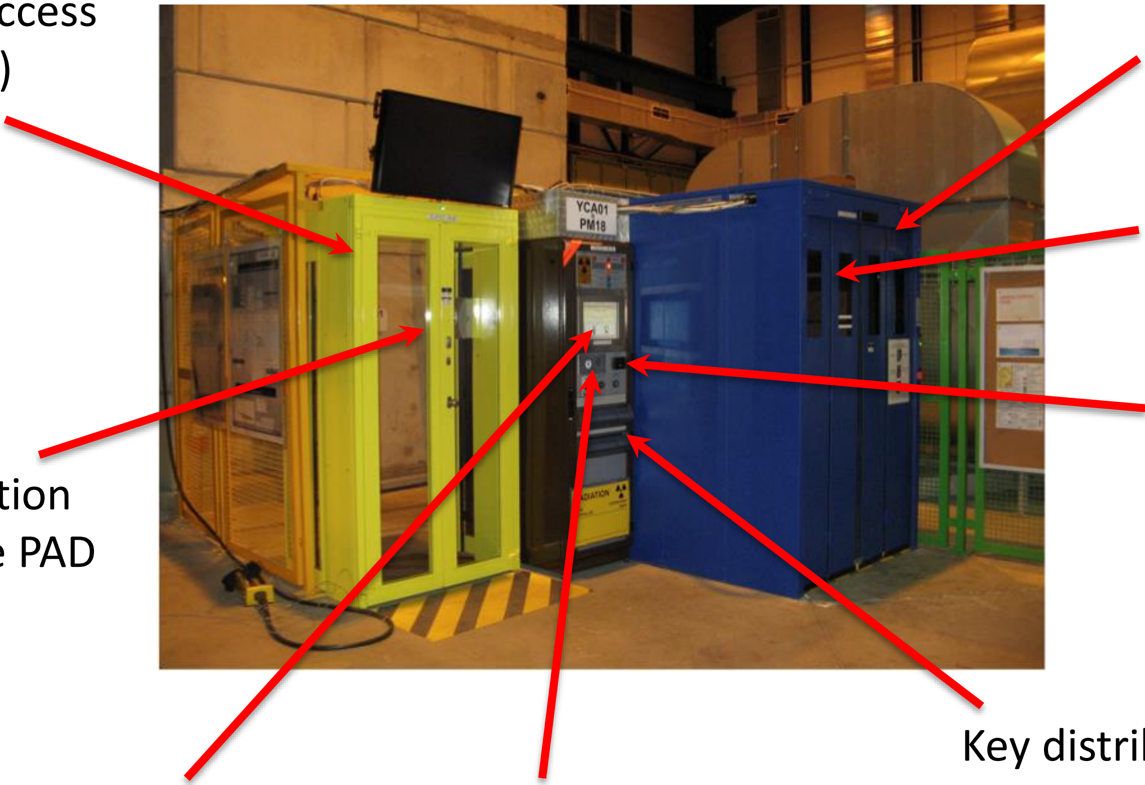
5th Control System Cyber-Security Workshop (CS)2/HEP
18.10.2015


ICALEPCS 2015
International Conference on Accelerator
& Large Experimental Physics
Control Systems
17-23 OCTOBER 2015 MCEC MELBOURNE

CERN Personnel Protection Systems (PPS)

- **PPS** = Access Control System + Access Safety System
- **Access Control Systems** (LACS, PACS, SPS PPS)
  - Access points (PAD, MAD, info panel, badge reader, iris scanner, interphone, video surveillance)
  - Doors (sector, end-of-zone, ventilation, trapdoors, moving walls)
  - Interacts with CERN systems (ADaMS, HR, AIS, …)
- **Access Safety Systems** (LASS, PASS, SPS PPS, SSA)
  - Zone envelope (door contacts)
  - Personnel elements (safety tokens / key distributors, patrol boxes, veto reset boxes)
  - Beam elements (beam stoppers/dumps, power converters, injection/extraction septa, separation dipoles, access safety blocks)
  - Machine elements (electron stoppers, RF cavities)
  - Two separate and diverse safety chains: PLC and hardwired
  - Isolated environment / network
  - Subject to inspection / approval by host state authorities (INB)

Access point components



Personnel Access Device (PAD)

Biometry detection (iris scan) inside PAD

Touch screen panel-PC

Interphone

Key distributors (safety token, part of the access safety system)

Material Access Device (MAD)

Person detection inside MAD

Badge reader

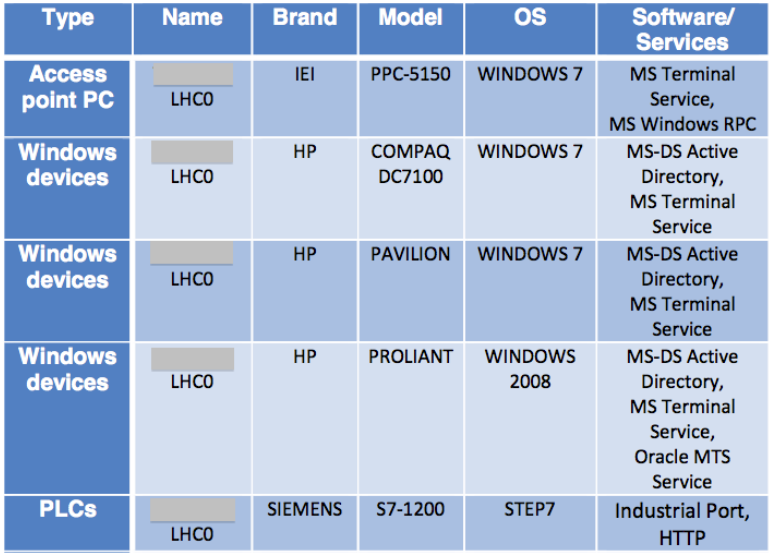
Why information security?

- Personnel protection systems are **control systems**:
  - Automation with PLCs and industrial controllers
  - Communication via field buses (Profibus / Profinet) and Ethernet
  - Sensors (door contacts, special safety devices)
  - Actuators (relays, contacts, electric motors)
  - SCADA systems (servers, databases, operator posts, local interface screens)
  - Running commodity and proprietary software (Windows, Linux, etc.)
  - Interface with other CERN systems (personnel databases, monitoring and surveillance, public information systems)
- Access and safety systems are **critical** to personnel safety and accelerator operations
- As **network connected** systems, they are subject to the full panoply of potential hazards related to information security today

Information security assessment

- Mission: evaluate the current access and safety systems for their level of information security today
- We chose two main ones for closer scrutiny: PS and LHC access and safety systems – they have comprehensive test bench installations
- Order of business:
  1. **Inventory:** what devices, networks, software?
  2. **Pre-testing:** selection of methodology and tools
  3. **Testing:** penetration, vulnerability checks, usual goofs
  4. **Evaluation of results:** classification, best practices
  5. **Other findings:** any surprises out there?

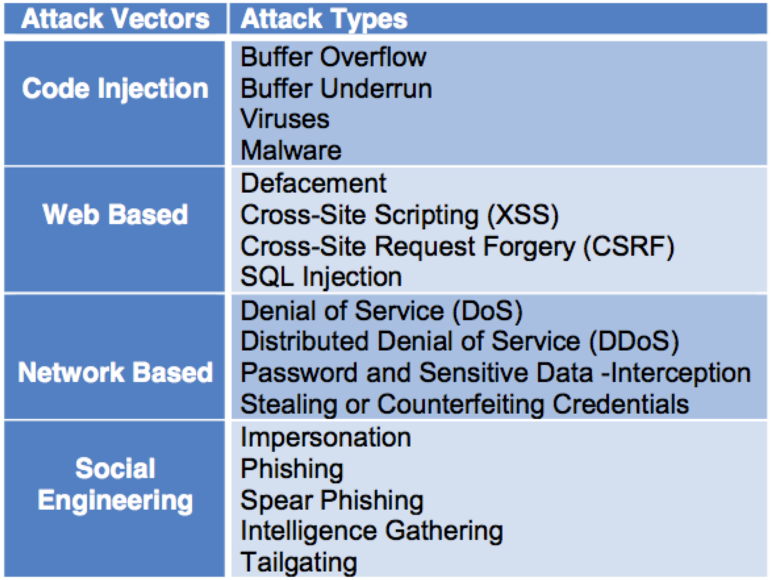
Inventory and threat assessment



Type	Name	Brand	Model	OS	Software/ Services
Access point PC	[redacted] LHC0	IEI	PPC-5150	WINDOWS 7	MS Terminal Service, MS Windows RPC
Windows devices	[redacted] LHC0	HP	COMPAQ DC7100	WINDOWS 7	MS-DS Active Directory, MS Terminal Service
Windows devices	[redacted] LHC0	HP	PAVILION	WINDOWS 7	MS-DS Active Directory, MS Terminal Service
Windows devices	[redacted] LHC0	HP	PROLIANT	WINDOWS 2008	MS-DS Active Directory, MS Terminal Service, Oracle MTS Service
PLCs	[redacted] LHC0	SIEMENS	S7-1200	STEP7	Industrial Port, HTTP

List basic parameters of every device in the system

List the known threats: will affect the methodology and tools to be chosen



Attack Vectors	Attack Types
Code Injection	Buffer Overflow Buffer Underrun Viruses Malware
Web Based	Defacement Cross-Site Scripting (XSS) Cross-Site Request Forgery (CSRF) SQL Injection
Network Based	Denial of Service (DoS) Distributed Denial of Service (DDoS) Password and Sensitive Data -Interception Stealing or Counterfeiting Credentials
Social Engineering	Impersonation Phishing Spear Phishing Intelligence Gathering Tailgating

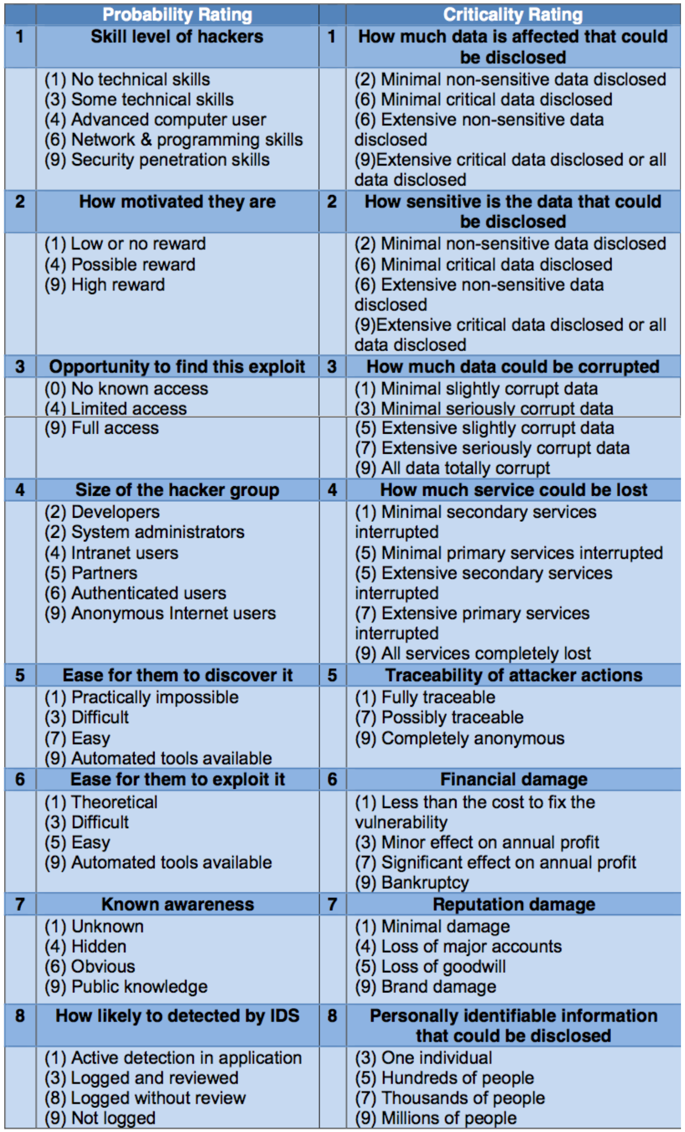
Methodology and tools

- Deterministic pen-testing vs. fuzzing
  - Exploiting known vulnerabilities is deterministic
  - Throwing stuff at the device to see if it breaks is fuzzy
- Many tools out there. These were chosen:
  - **Metasploit Framework:** penetration-testing software
  - **Armitage:** GUI for Metasploit
  - **nMap:** network mapping tool
  - **Wireshark:** protocol analysis tool
  - **Backfuzz:** multi-protocol fuzzing toolkit
  - **W3af:** open source tool for finding vulnerabilities in web-applications
  - **Nikto:** web scanner for detecting vulnerabilities
  - **BeEF:** penetration-testing tool for exploiting web browsers
  - **THC Hydra:** dictionary-based password-cracking tool
  - **THC flood_router26:** script for flooding the network with router advertisements
  - **THC smurf6:** IPv6 tool for DDoS (Distributed Denial-of-Service) attacks
- The whole circus runs on a security-testing-oriented **Kali Linux** platform

Some findings

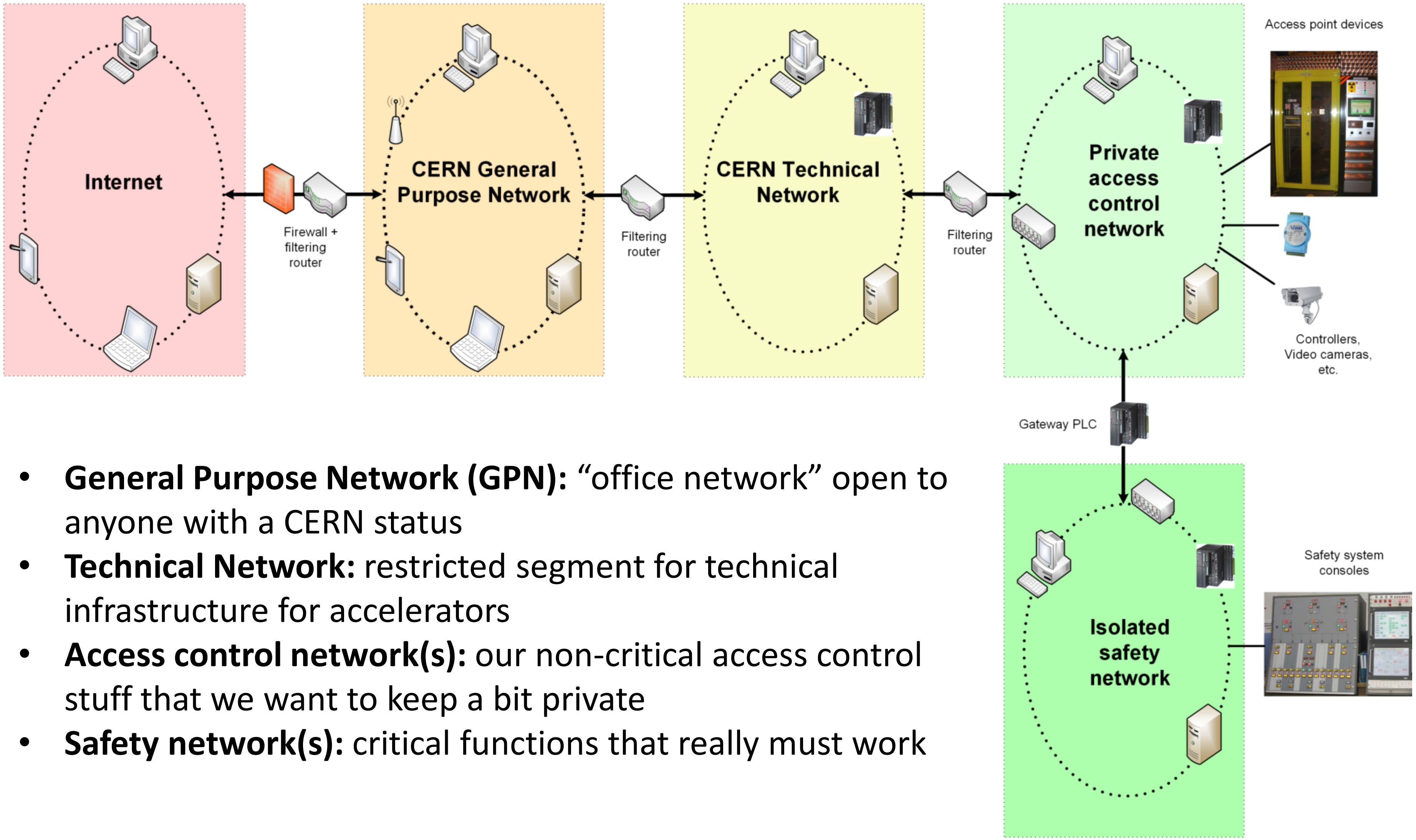
- Classification according to OWASP criteria
- A good number of usual suspects:
  - Missing or default passwords on embedded devices
  - Configuration issues: unnecessary services, protocols, etc.
  - Missing patches
  - Test benches sometimes lagging in security behind production systems
  - Fresh vulnerabilities: Heartbleed etc.
- Each issue was inspected and classified, and mitigation measures were proposed and put in place when possible
- During the assessment a number of new findings were discovered

Reminder: a big part of the study was to see what else is out there



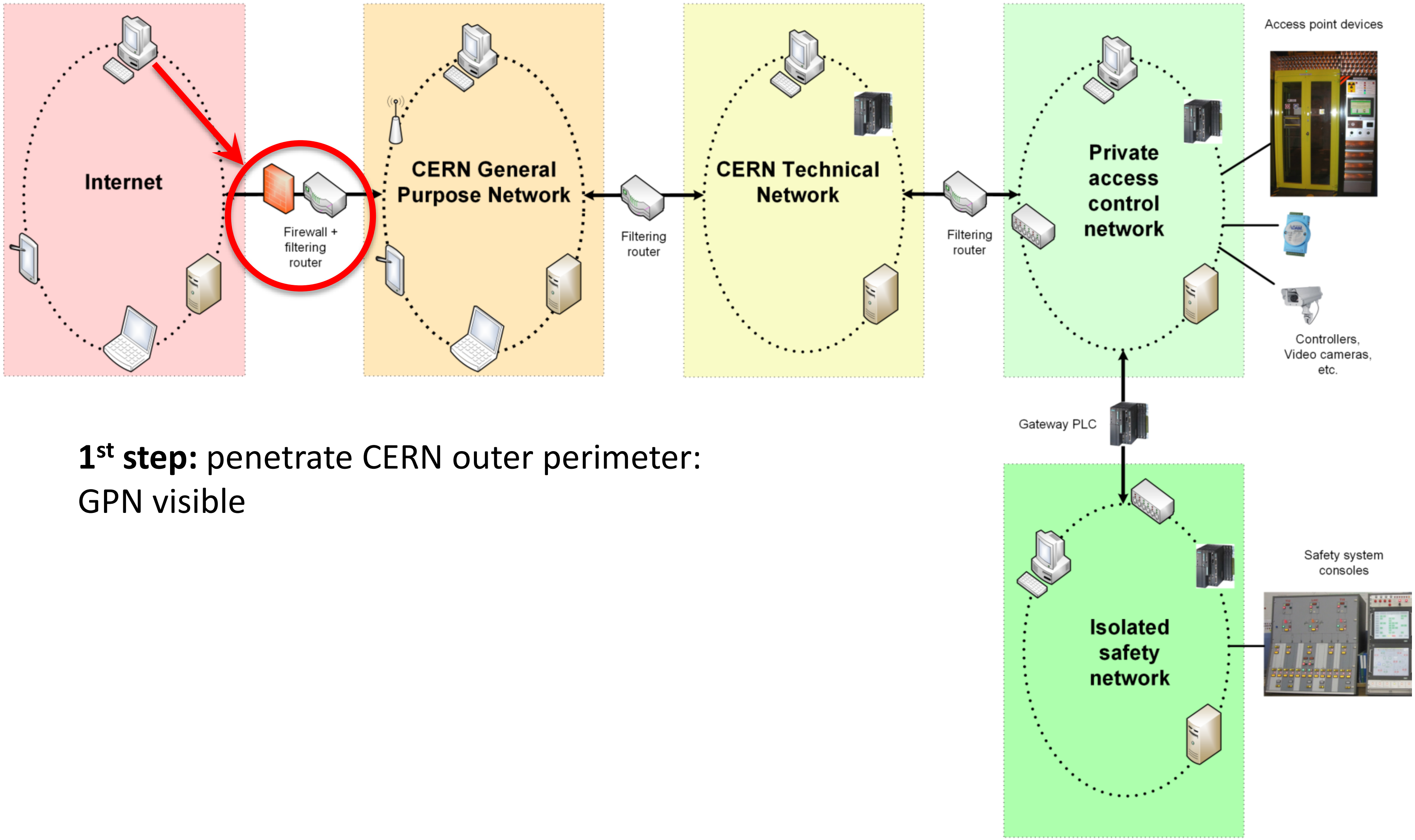
	Probability Rating		Criticality Rating
1	**Skill level of hackers**	1	**How much data is affected that could be disclosed**
	(1) No technical skills (3) Some technical skills (4) Advanced computer user (6) Network & programming skills (9) Security penetration skills		(2) Minimal non-sensitive data disclosed (6) Minimal critical data disclosed (6) Extensive non-sensitive data disclosed (9)Extensive critical data disclosed or all data disclosed
2	**How motivated they are**	2	**How sensitive is the data that could be disclosed**
	(1) Low or no reward (4) Possible reward (9) High reward		(2) Minimal non-sensitive data disclosed (6) Minimal critical data disclosed (6) Extensive non-sensitive data disclosed (9)Extensive critical data disclosed or all data disclosed
3	**Opportunity to find this exploit**	3	**How much data could be corrupted**
	(0) No known access (4) Limited access (9) Full access		(1) Minimal slightly corrupt data (3) Minimal seriously corrupt data (5) Extensive slightly corrupt data (7) Extensive seriously corrupt data (9) All data totally corrupt
4	**Size of the hacker group**	4	**How much service could be lost**
	(2) Developers (2) System administrators (4) Intranet users (5) Partners (6) Authenticated users (9) Anonymous Internet users		(1) Minimal secondary services interrupted (5) Minimal primary services interrupted (5) Extensive secondary services interrupted (7) Extensive primary services interrupted (9) All services completely lost
5	**Ease for them to discover it**	5	**Traceability of attacker actions**
	(1) Practically impossible (3) Difficult (7) Easy (9) Automated tools available		(1) Fully traceable (7) Possibly traceable (9) Completely anonymous
6	**Ease for them to exploit it**	6	**Financial damage**
	(1) Theoretical (3) Difficult (5) Easy (9) Automated tools available		(1) Less than the cost to fix the vulnerability (3) Minor effect on annual profit (7) Significant effect on annual profit (9) Bankruptcy
7	**Known awareness**	7	**Reputation damage**
	(1) Unknown (4) Hidden (6) Obvious (9) Public knowledge		(1) Minimal damage (4) Loss of major accounts (5) Loss of goodwill (9) Brand damage
8	**How likely to detected by IDS**	8	**Personally identifiable information that could be disclosed**
	(1) Active detection in application (3) Logged and reviewed (8) Logged without review (9) Not logged		(3) One individual (5) Hundreds of people (7) Thousands of people (9) Millions of people

CERN networks (that we care about)



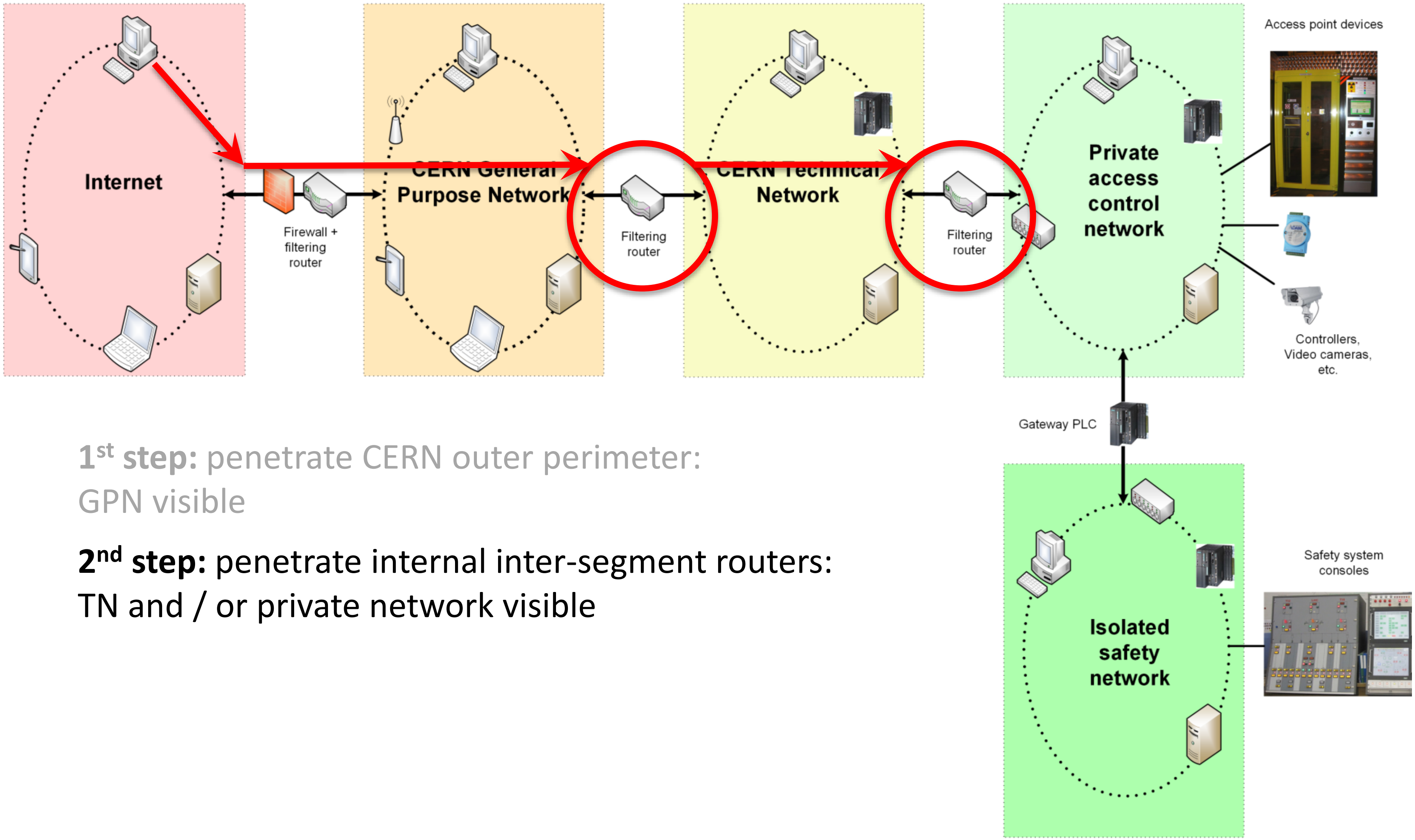
- **General Purpose Network (GPN):** “office network” open to anyone with a CERN status
- **Technical Network:** restricted segment for technical infrastructure for accelerators
- **Access control network(s):** our non-critical access control stuff that we want to keep a bit private
- **Safety network(s):** critical functions that really must work

Intrusion: the procedure



1st step: penetrate CERN outer perimeter: GPN visible

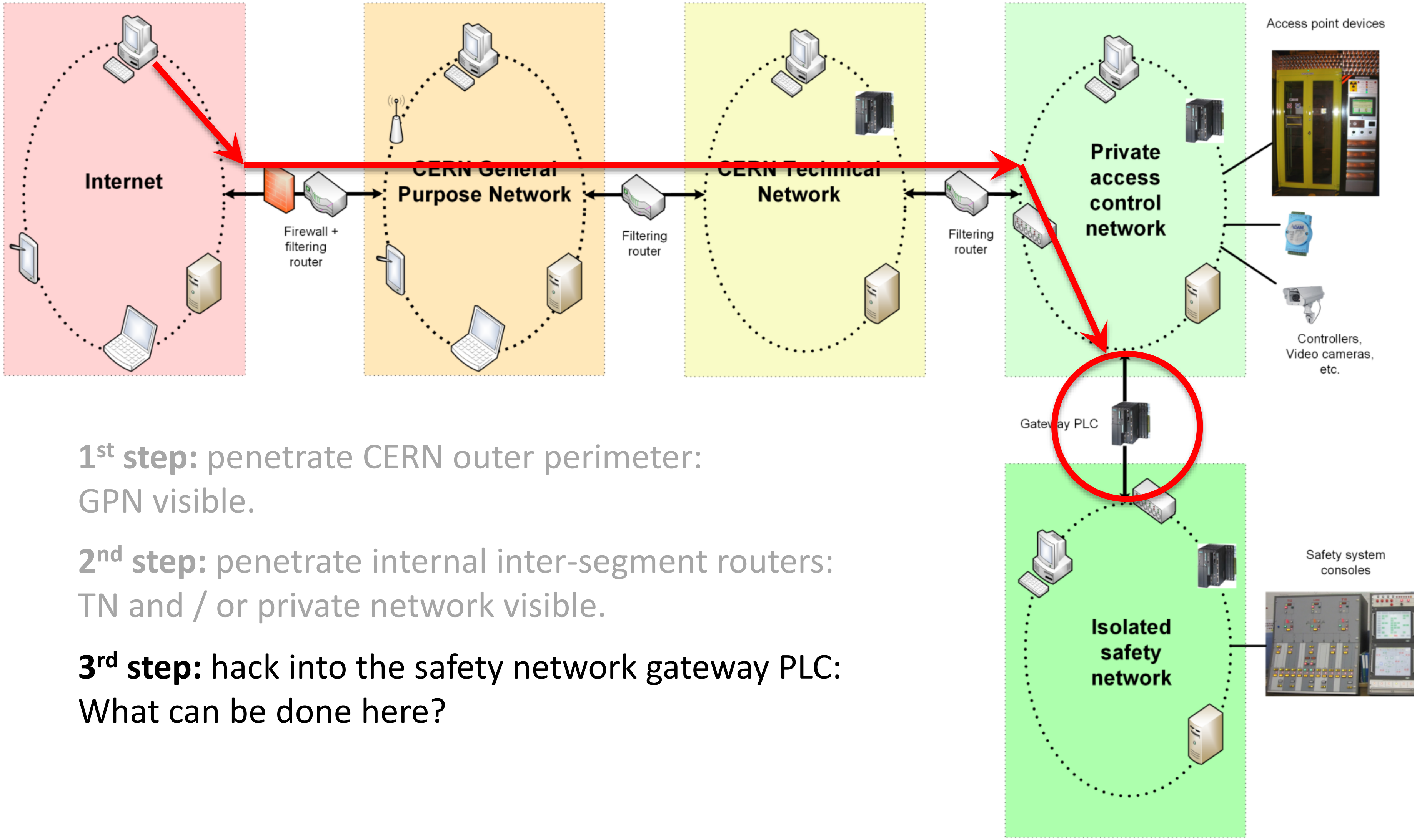
Intrusion: the procedure



1st step: penetrate CERN outer perimeter: GPN visible

2nd step: penetrate internal inter-segment routers: TN and / or private network visible

Intrusion: the procedure

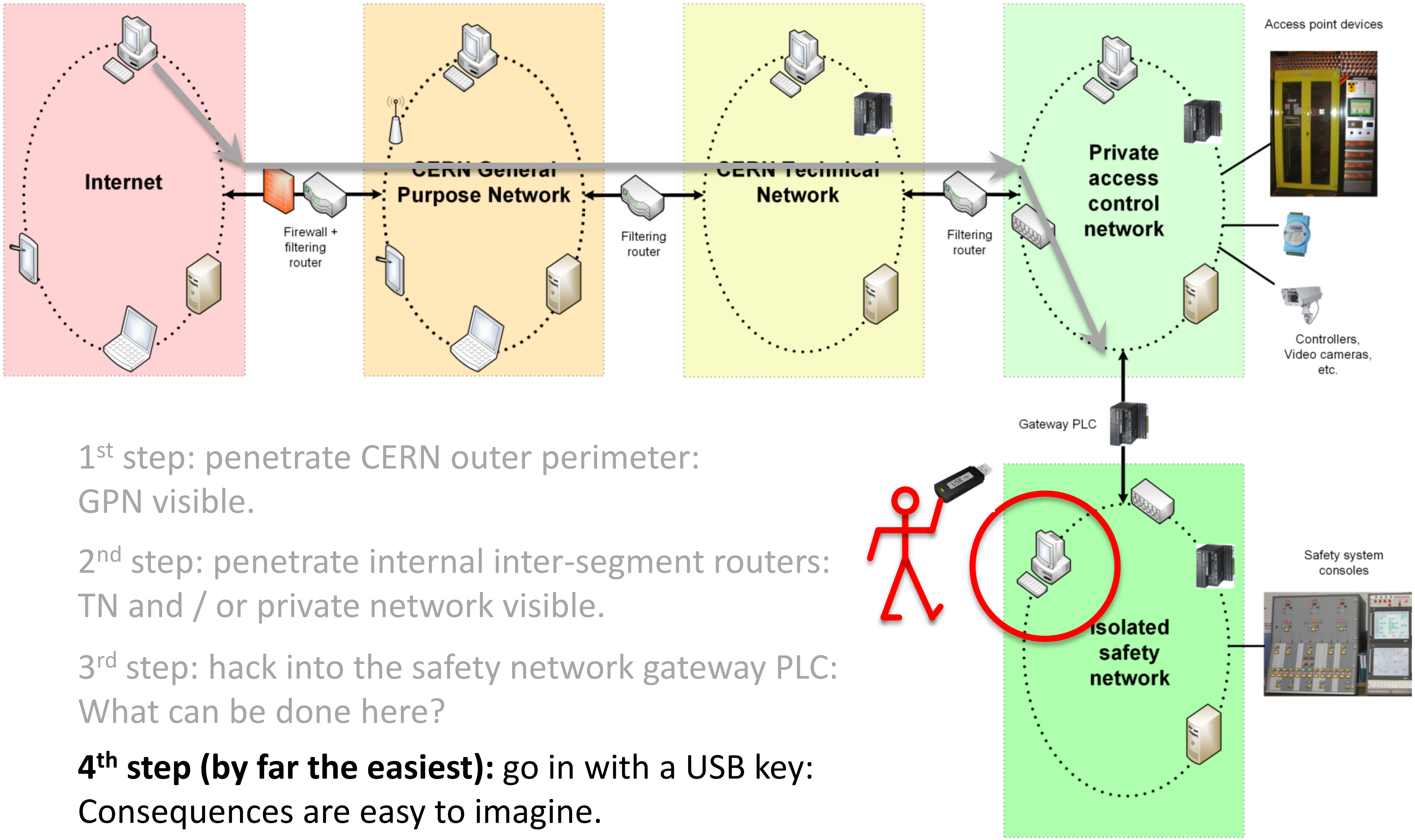


1st step: penetrate CERN outer perimeter: GPN visible.

2nd step: penetrate internal inter-segment routers: TN and / or private network visible.

3rd step: hack into the safety network gateway PLC: What can be done here?

Intrusion: the procedure



1st step: penetrate CERN outer perimeter: GPN visible.

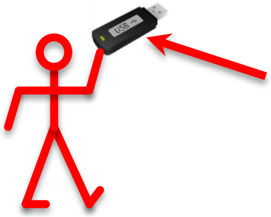
2nd step: penetrate internal inter-segment routers: TN and / or private network visible.

3rd step: hack into the safety network gateway PLC: What can be done here?

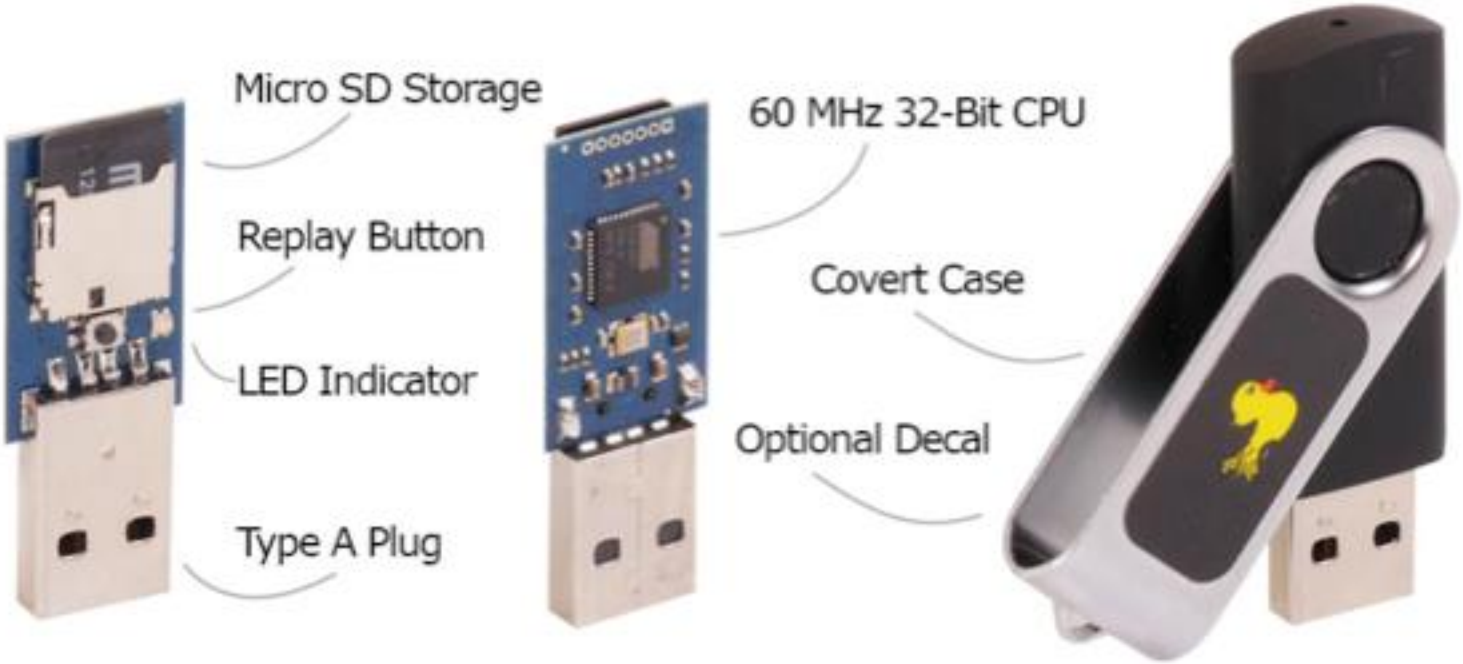
4th step (by far the easiest): go in with a USB key: Consequences are easy to imagine.

Q: How fast can you infect a machine?

A: With a *USB keyboard injector* pretty damn fast…



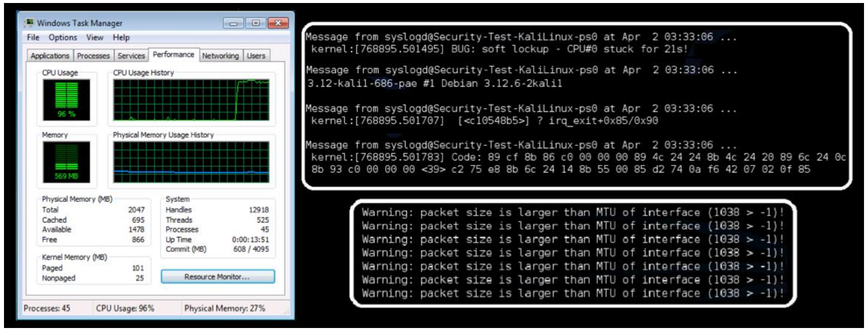
Not a usual USB key



If you need your own: http://usbrubberducky.com

IPv6 has some issues…

- IPv6 is still “new” and, therefore, not a really well known protocol
- New features and functionalities to facilitate network management:
  - Huge address space for hosts and subnets
  - Best of show: Stateless Address Auto Configuration (SLAAC) allows routers to announce themselves to hosts
  - Combined with poor handling on the host side can freeze the host by flooding it with router advertisements of bogus subnets
  - Hijack network connections in IPv4 networks by posing as a privileged IPv6 router
- New vulnerabilities are constantly being discovered
- New systems often have IPv6 enabled by default



Physical Memory (MB)
Total 2047
Cached 695
Available 1478
Free 866

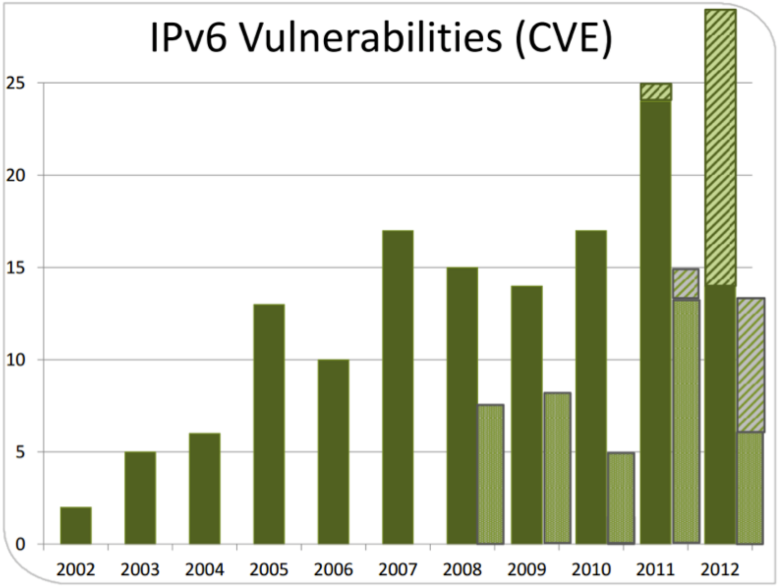
Kernel Memory (MB)
Paged 101
Nonpaged 25

System
Handles 12918
Threads 525
Processes 45
Up Time 0:00:13:51
Commit (MB) 608 / 4095

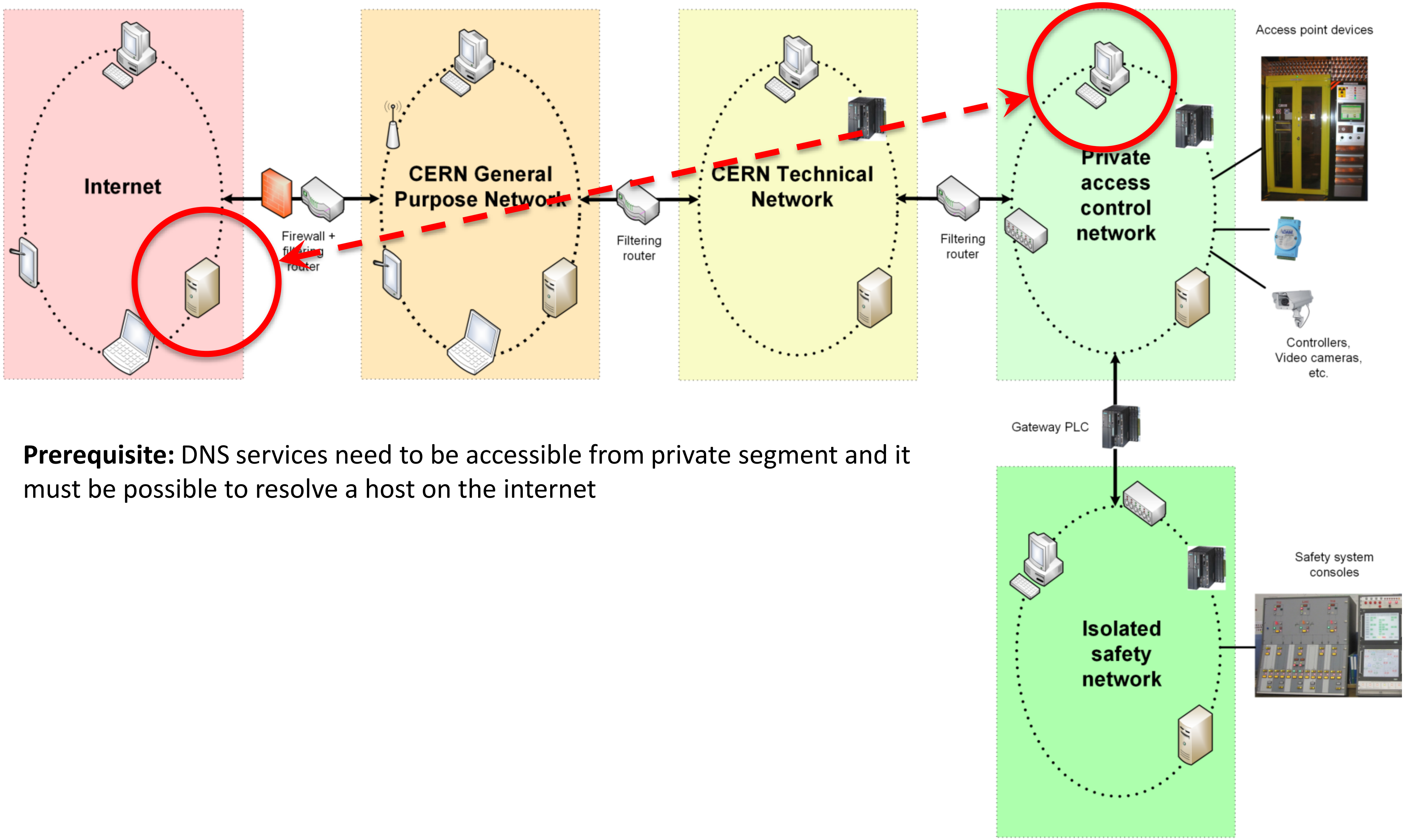
Processes: 45 CPU Usage: 96% Physical Memory: 27%

```
Message from syslogd@Security-Test-KaliLinux-ps0 at Apr  2 03:33:06 ...
 kernel:[768895.501495] BUG: soft lockup - CPU#0 stuck for 21s!

Message from syslogd@Security-Test-KaliLinux-ps0 at Apr  2 03:33:06 ...
3.12-kali1-686-pae #1 Debian 3.12.6-2kali1

Message from syslogd@Security-Test-KaliLinux-ps0 at Apr  2 03:33:06 ...
 kernel:[768895.501707]  [<c10548b5>] ? irq_exit+0x85/0x90

Message from syslogd@Security-Test-KaliLinux-ps0 at Apr  2 03:33:06 ...
 kernel:[768895.501783] Code: 89 cf 8b 86 c0 00 00 00 89 4c 24 24 8b 4c 24 20 89 6c 24 0c
 8b 93 c0 00 00 00 <39> c2 75 e8 8b 6c 24 14 8b 55 00 85 d2 74 0a f6 42 07 02 0f 85
```

```
Warning: packet size is larger than MTU of interface (1038 > -1)!
Warning: packet size is larger than MTU of interface (1038 > -1)!
Warning: packet size is larger than MTU of interface (1038 > -1)!
Warning: packet size is larger than MTU of interface (1038 > -1)!
Warning: packet size is larger than MTU of interface (1038 > -1)!
Warning: packet size is larger than MTU of interface (1038 > -1)!
Warning: packet size is larger than MTU of interface (1038 > -1)!
```

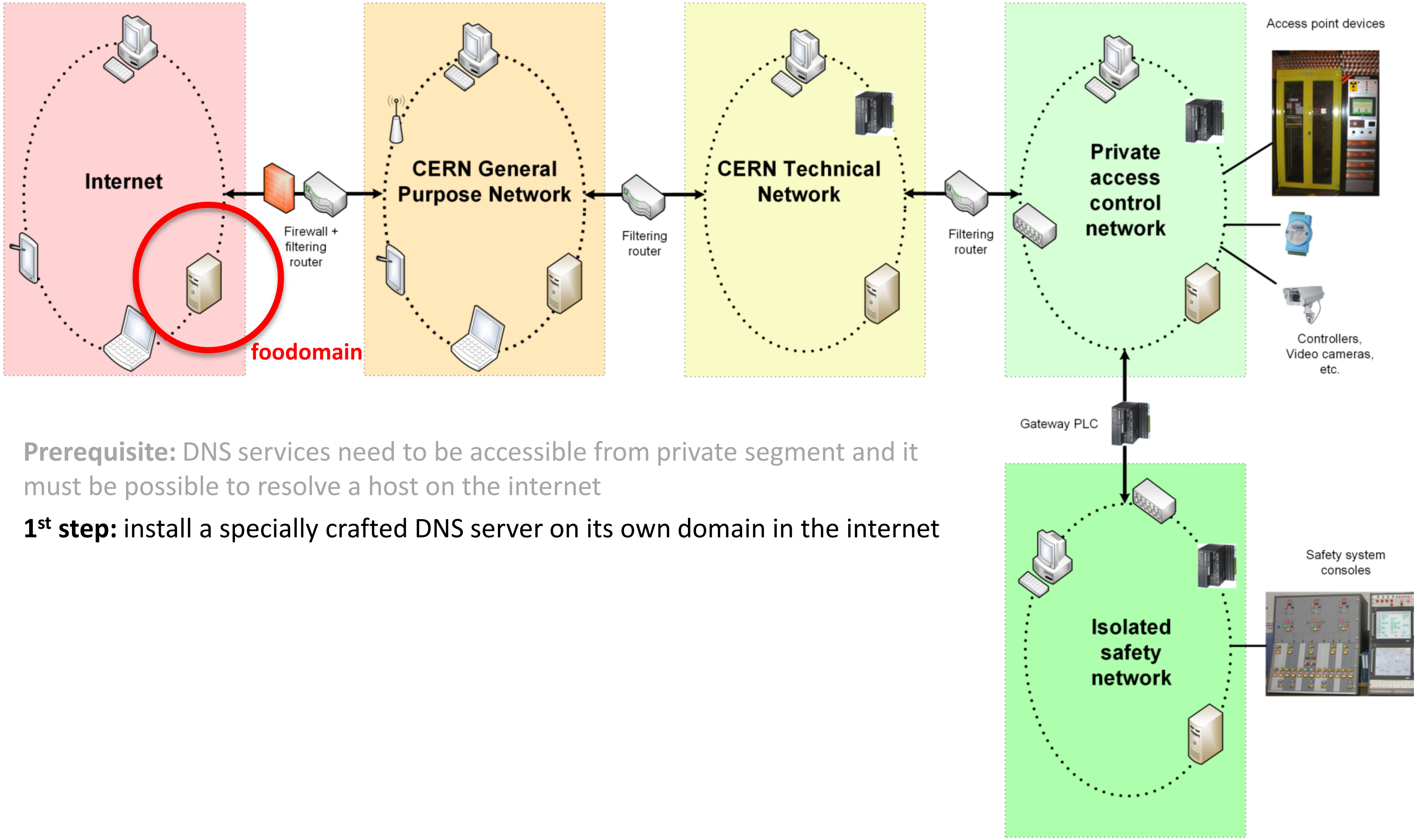


Tunneling from a private network



Prerequisite: DNS services need to be accessible from private segment and it must be possible to resolve a host on the internet

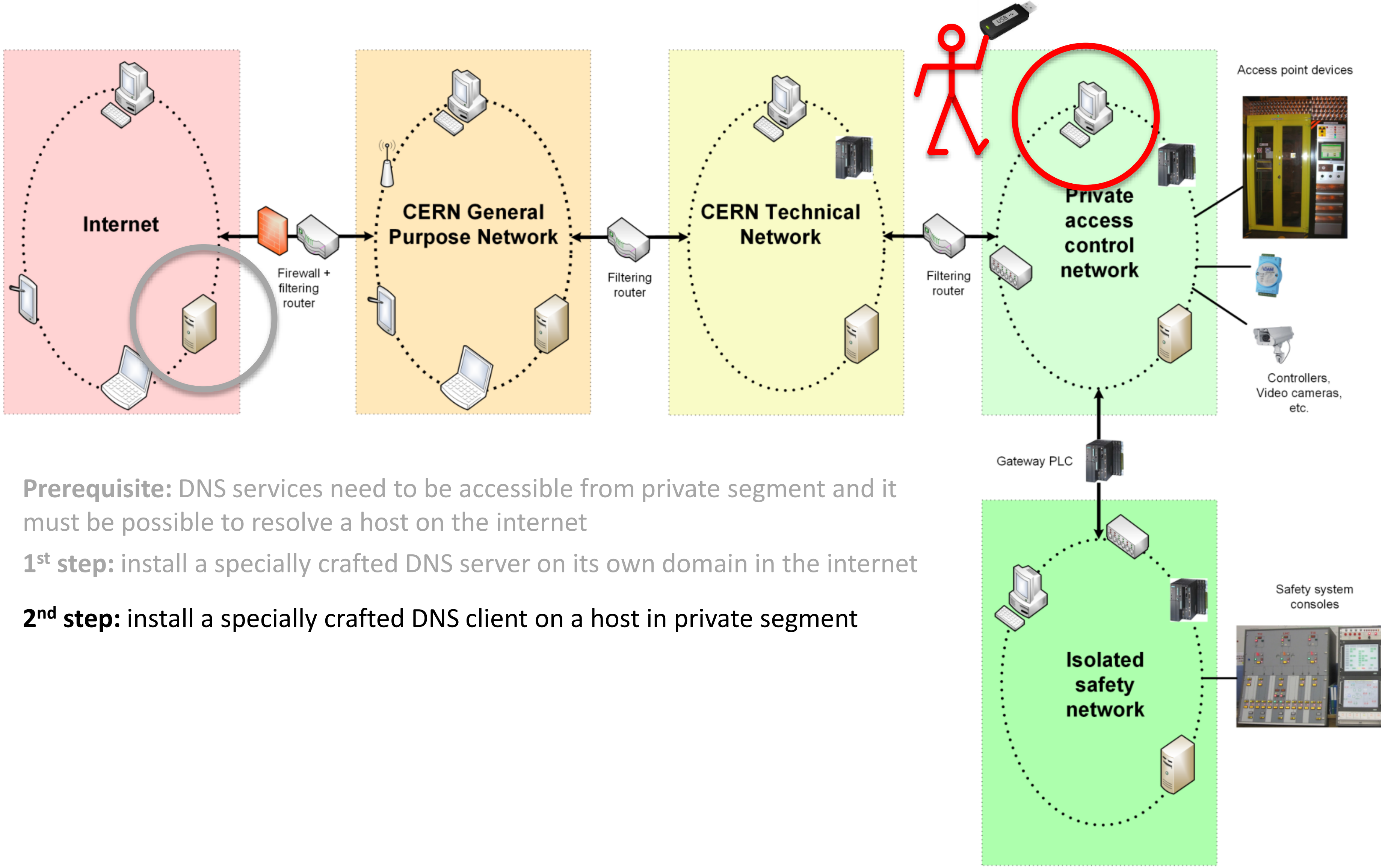
Tunneling from a private network



Prerequisite: DNS services need to be accessible from private segment and it must be possible to resolve a host on the internet

1st step: install a specially crafted DNS server on its own domain in the internet

Tunneling from a private network

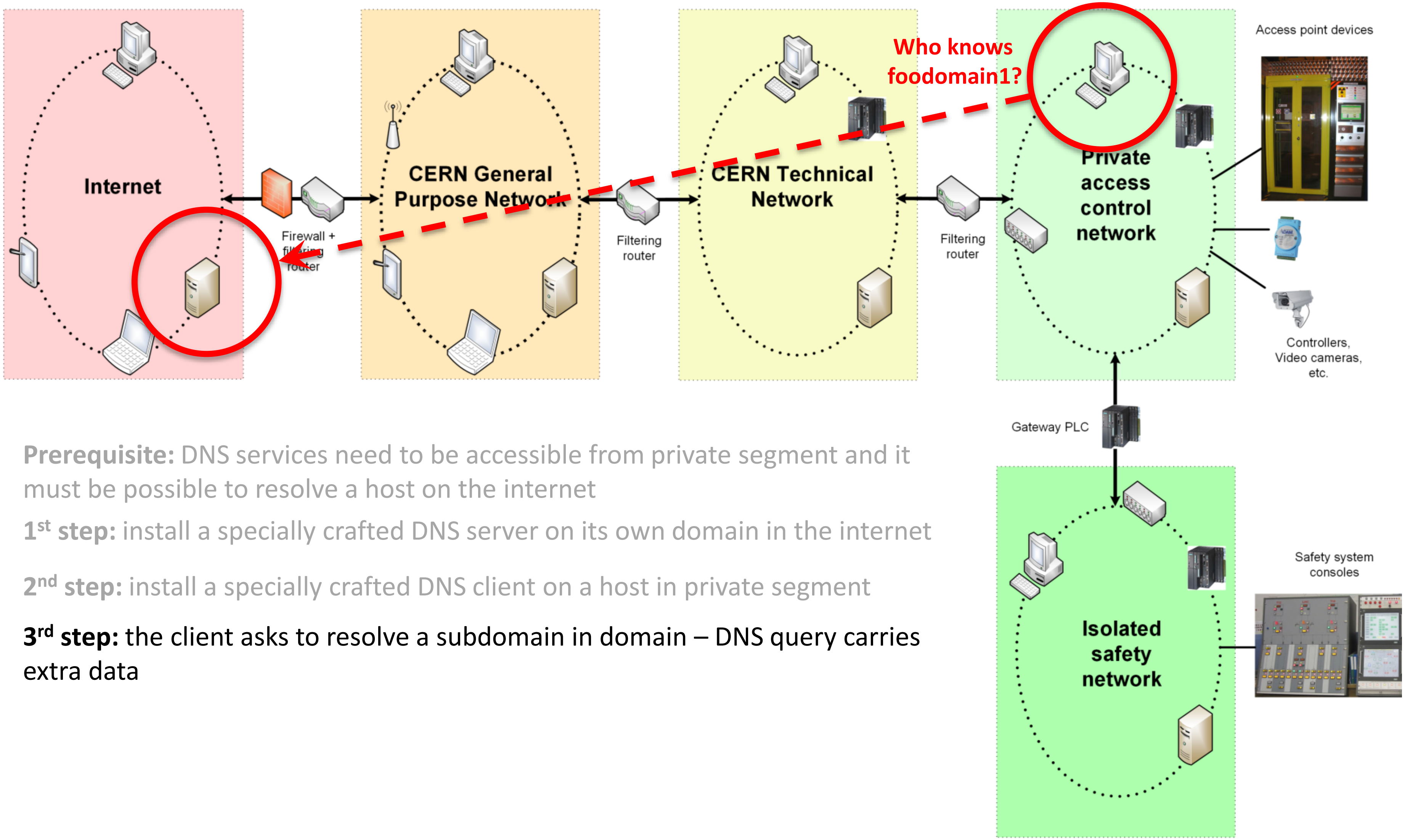


Prerequisite: DNS services need to be accessible from private segment and it must be possible to resolve a host on the internet

1st step: install a specially crafted DNS server on its own domain in the internet

2nd step: install a specially crafted DNS client on a host in private segment

Tunneling from a private network



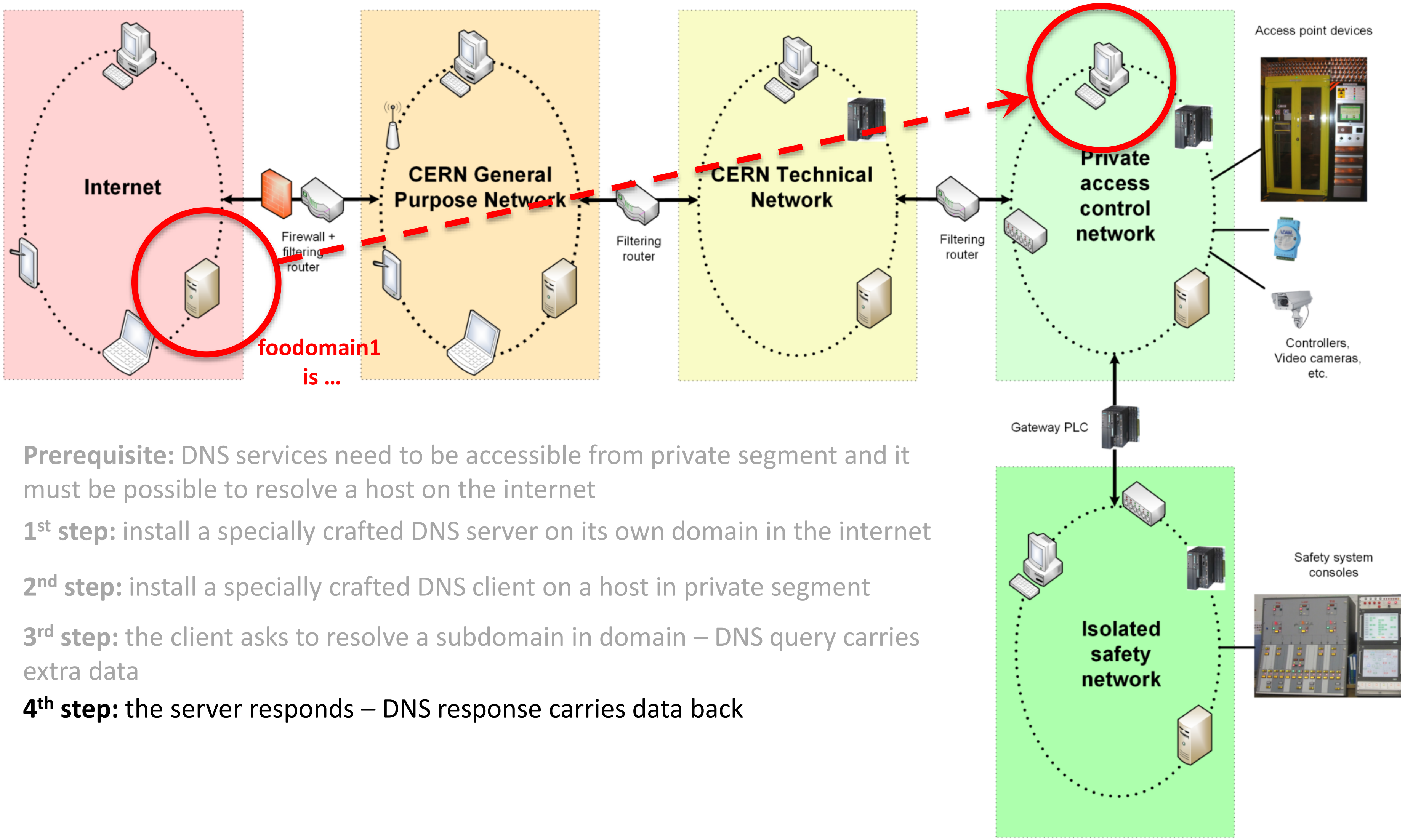
Prerequisite: DNS services need to be accessible from private segment and it must be possible to resolve a host on the internet

1st step: install a specially crafted DNS server on its own domain in the internet

2nd step: install a specially crafted DNS client on a host in private segment

3rd step: the client asks to resolve a subdomain in domain – DNS query carries extra data

Tunneling from a private network



foodomain1 is …

Prerequisite: DNS services need to be accessible from private segment and it must be possible to resolve a host on the internet

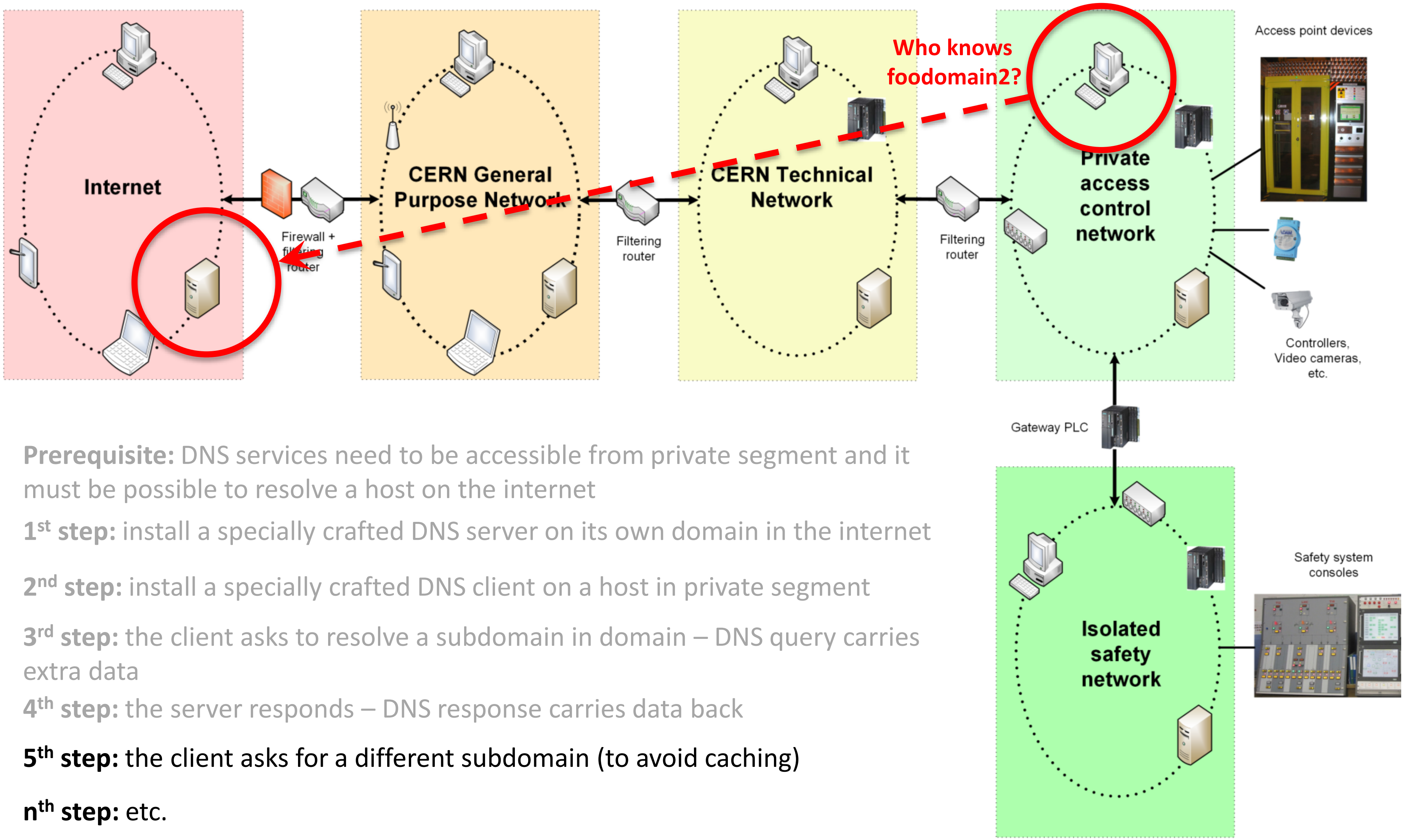
1st step: install a specially crafted DNS server on its own domain in the internet

2nd step: install a specially crafted DNS client on a host in private segment

3rd step: the client asks to resolve a subdomain in domain – DNS query carries extra data

4th step: the server responds – DNS response carries data back

Tunneling from a private network



Prerequisite: DNS services need to be accessible from private segment and it must be possible to resolve a host on the internet

1st step: install a specially crafted DNS server on its own domain in the internet

2nd step: install a specially crafted DNS client on a host in private segment

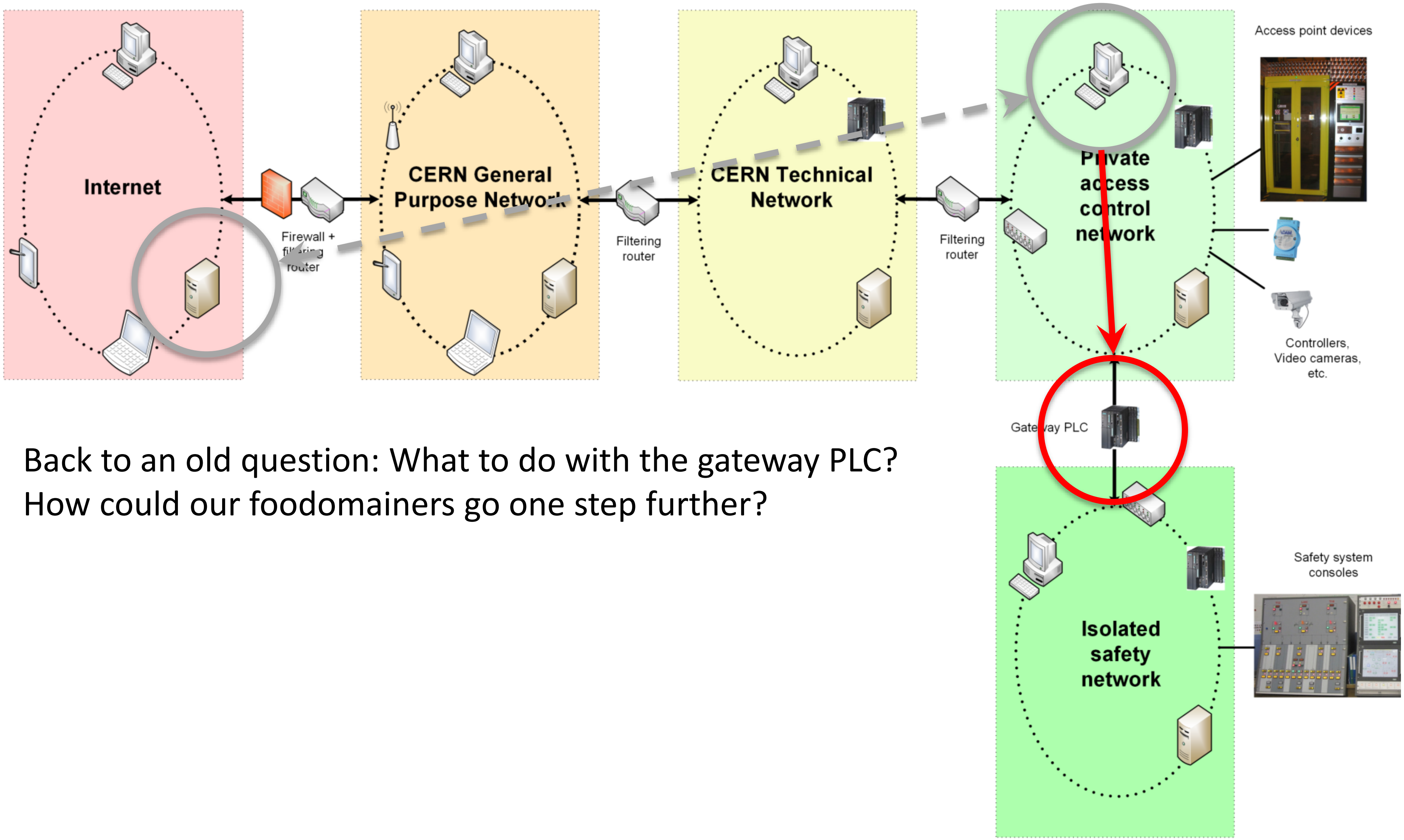
3rd step: the client asks to resolve a subdomain in domain – DNS query carries extra data

4th step: the server responds – DNS response carries data back

5th step: the client asks for a different subdomain (to avoid caching)

nth step: etc.

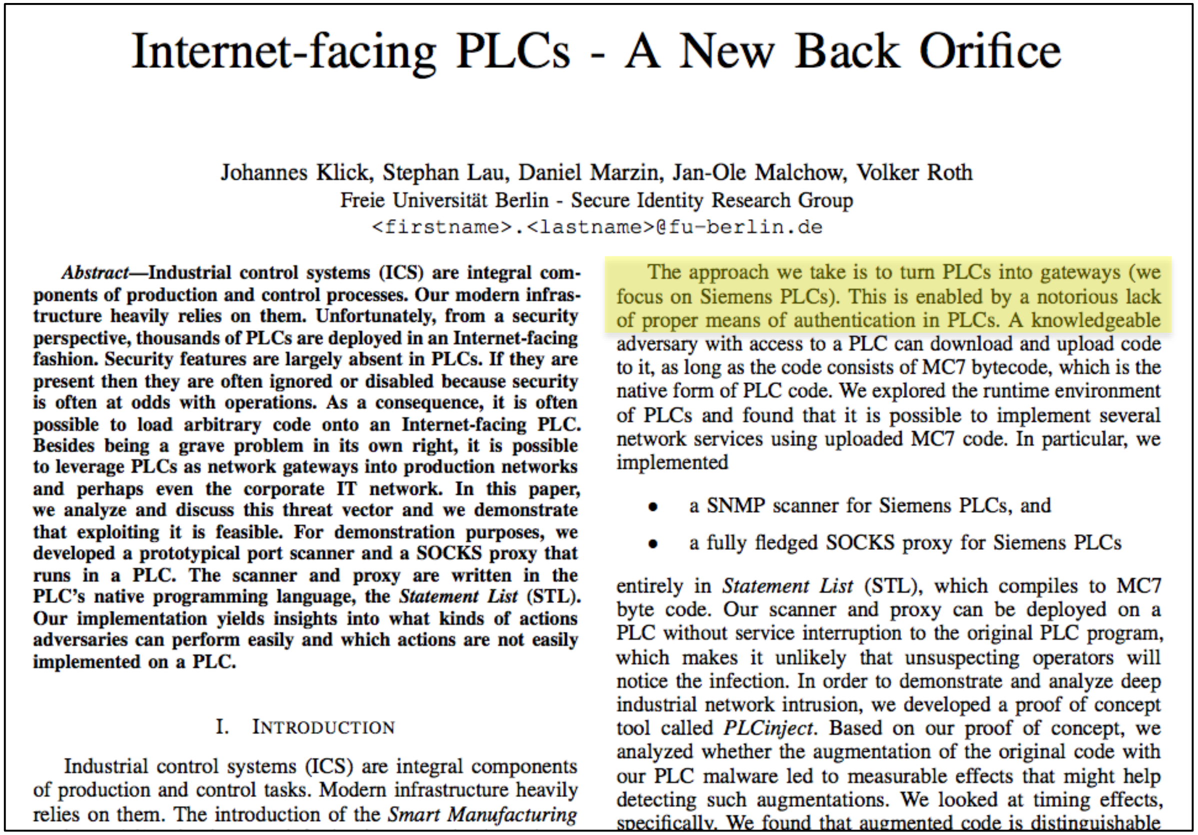
Tunneling from a private network



Back to an old question: What to do with the gateway PLC?
How could our foodomainers go one step further?

PLC also makes a great router!

Presentation at the Black Hat USA 2015 conference this summer:
https://www.blackhat.com/docs/us-15/materials/us-15-Klick-Internet-Facing-PLCs-A-New-Back-Orifice-wp.pdf



Internet-facing PLCs - A New Back Orifice

Johannes Klick, Stephan Lau, Daniel Marzin, Jan-Ole Malchow, Volker Roth
Freie Universität Berlin - Secure Identity Research Group
<firstname>.<lastname>@fu-berlin.de

***Abstract*—Industrial control systems (ICS) are integral components of production and control processes. Our modern infrastructure heavily relies on them. Unfortunately, from a security perspective, thousands of PLCs are deployed in an Internet-facing fashion. Security features are largely absent in PLCs. If they are present then they are often ignored or disabled because security is often at odds with operations. As a consequence, it is often possible to load arbitrary code onto an Internet-facing PLC. Besides being a grave problem in its own right, it is possible to leverage PLCs as network gateways into production networks and perhaps even the corporate IT network. In this paper, we analyze and discuss this threat vector and we demonstrate that exploiting it is feasible. For demonstration purposes, we developed a prototypical port scanner and a SOCKS proxy that runs in a PLC. The scanner and proxy are written in the PLC's native programming language, the *Statement List* (STL). Our implementation yields insights into what kinds of actions adversaries can perform easily and which actions are not easily implemented on a PLC.**

I. Introduction

Industrial control systems (ICS) are integral components of production and control tasks. Modern infrastructure heavily relies on them. The introduction of the *Smart Manufacturing*

The approach we take is to turn PLCs into gateways (we focus on Siemens PLCs). This is enabled by a notorious lack of proper means of authentication in PLCs. A knowledgeable adversary with access to a PLC can download and upload code to it, as long as the code consists of MC7 bytecode, which is the native form of PLC code. We explored the runtime environment of PLCs and found that it is possible to implement several network services using uploaded MC7 code. In particular, we implemented

- a SNMP scanner for Siemens PLCs, and
- a fully fledged SOCKS proxy for Siemens PLCs

entirely in *Statement List* (STL), which compiles to MC7 byte code. Our scanner and proxy can be deployed on a PLC without service interruption to the original PLC program, which makes it unlikely that unsuspecting operators will notice the infection. In order to demonstrate and analyze deep industrial network intrusion, we developed a proof of concept tool called *PLCinject*. Based on our proof of concept, we analyzed whether the augmentation of the original code with our PLC malware led to measurable effects that might help detecting such augmentations. We looked at timing effects, specifically. We found that augmented code is distinguishable

Mitigations?

- First and foremost, keep up physical barriers
  - Strict access controls to sensitive areas to know who enters, when, and by what authority
  - Hide devices in locked racks away from manipulation
- Disable any unnecessary network protocols
  - Most control systems have no use for IPv6
  - Restrict DNS queries to your domain
- Keep firewalls updated and monitor suspect traffic
  - How large do you expect, say, DNS packets to be?
  - How about other protocols? Any suprises there?
- Defense-in-depth:
  - Keep even isolated devices updated and patched as much as possible
  - Password-protect all devices that you can
  - Run console sessions in user mode – up to vendors to ensure that their SCADA systems can!

Conclusions

- Information security landscape for control systems is changing
  - Not immune to intrusion and even actively targeted
  - Control systems are notoriously hard to secure
  - Traditionally not taken seriously by vendors
  - Control systems are approaching commodity office systems with the same benefits and problems
  - Consequences of security breaches can be grave, particularly in case of personnel protection systems
- The role of PLCs is evolving
  - Resembling more and more commodity hardware
  - Powerful new CPUs and communication modules
  - Able to carry out sophisticated tasks (e.g., database and web queries)
  - Still, do the security provisions keep up?
- Again: When securing control systems, physical access is key!

Thank You!

Questions?