Security in Convoluted Systems

Simon Foley

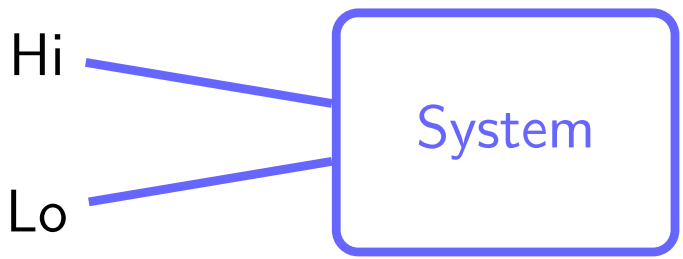
IMT Atlantique, Rennes

30 May, 2017

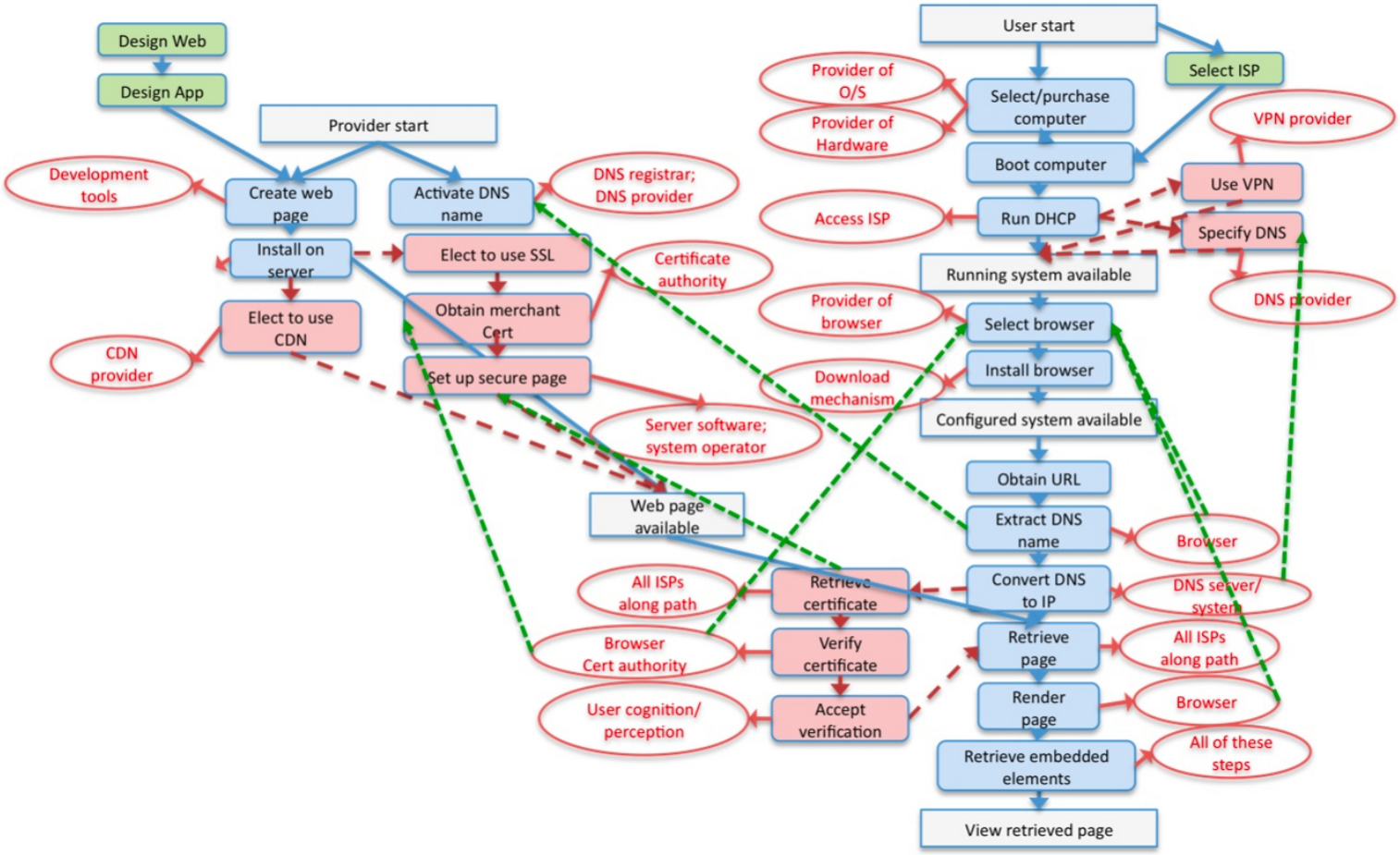
What is meant by a secure system?

Information theoretic definitions

Actions at Hi interface
do not interfere with
actions at Lo interface

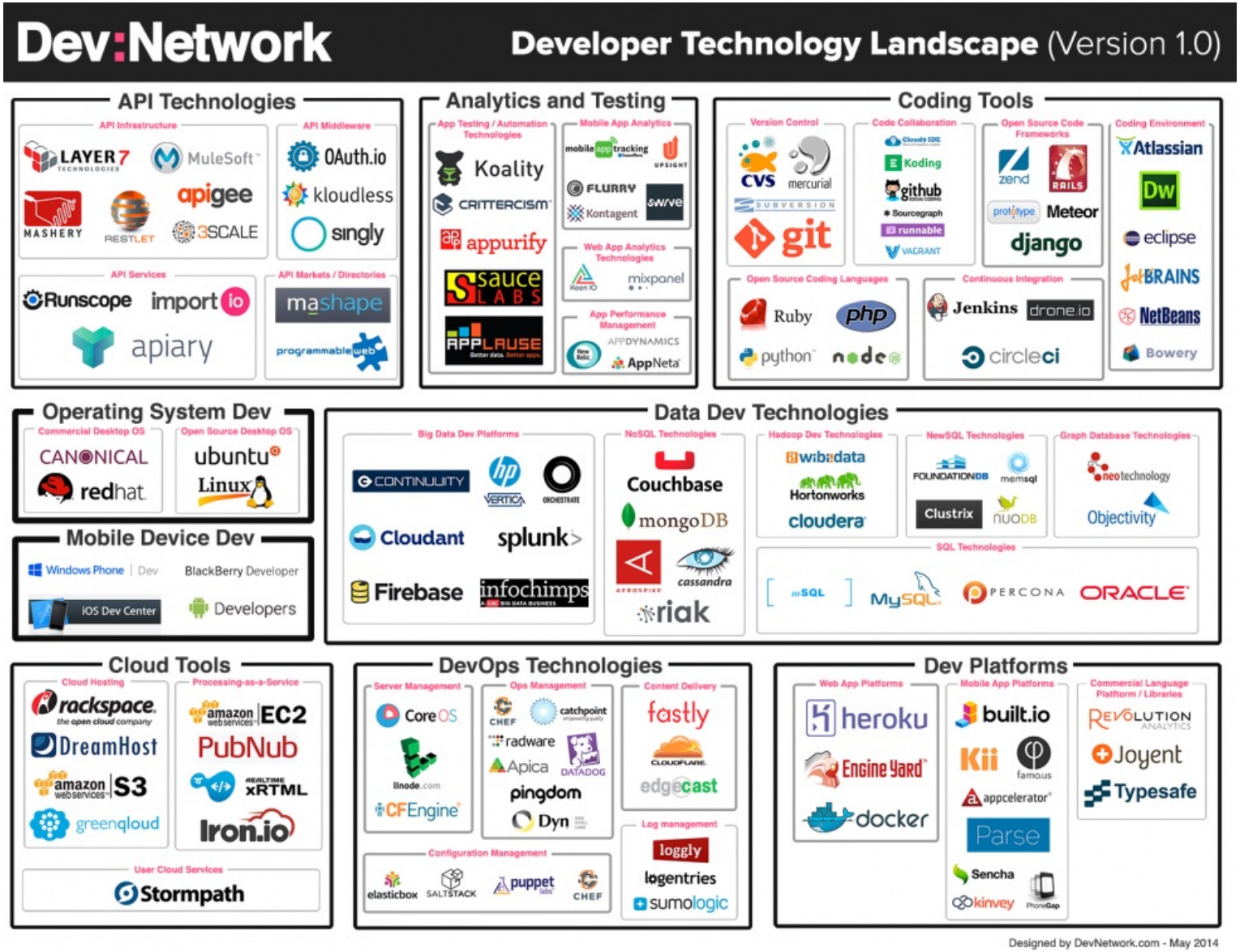


Contemporary systems are more convoluted,



[D. Clark, *Control Point Analysis*, TPRC 2012]

developed using frameworks like these,



and built and operated by humans

TIMESONLINE

NEWS | COMMENT | BUSINESS | MONEY | SPORT | LIFE & STYLE | TRAVEL | DRIVING | ART

UK NEWS | WORLD NEWS | POLITICS | SCIENCE | ENVIRONMENT | WEATHER | TECH & WEB

Where am I? › Home › News › Tech & Web

From The Times

July 6, 2009

Wife of Sir John Sawers, the future head of MI6, in Facebook security alert

Michael Evans, Defence Editor

Diplomats and civil servants are to be warned about the danger of putting details of their family and career on social networking websites. The advice comes after the wife of Sir John Sawers, the next head of MI6, put family details on Facebook — which is accessible to millions of internet users.

Lady Sawers disclosed details such as the location of the London flat used by the couple and the whereabouts of their three children and of Sir John's parents. She put no privacy protection on her account, allowing any of Facebook's 200 million users in the

EXPLORE TECH & WEB

› PERSONAL TECH

› THE WEB

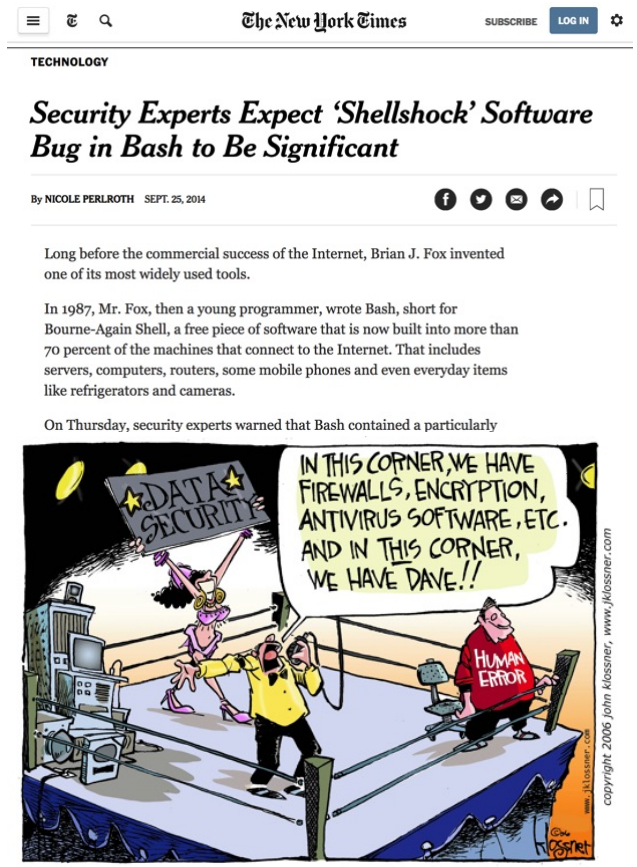
› GADGETS & GAMING

TECH CENTRAL

Latest posts on the blog

View RSS feed

TOKYO ROBOT SHOW



The New York Times SUBSCRIBE LOG IN

TECHNOLOGY

Security Experts Expect 'Shellshock' Software Bug in Bash to Be Significant

By NICOLE PERLROTH SEPT. 25, 2014

Long before the commercial success of the Internet, Brian J. Fox invented one of its most widely used tools.

In 1987, Mr. Fox, then a young programmer, wrote Bash, short for Bourne-Again Shell, a free piece of software that is now built into more than 70 percent of the machines that connect to the Internet. That includes servers, computers, routers, some mobile phones and even everyday items like refrigerators and cameras.

On Thursday, security experts warned that Bash contained a particularly

Security in convoluted systems

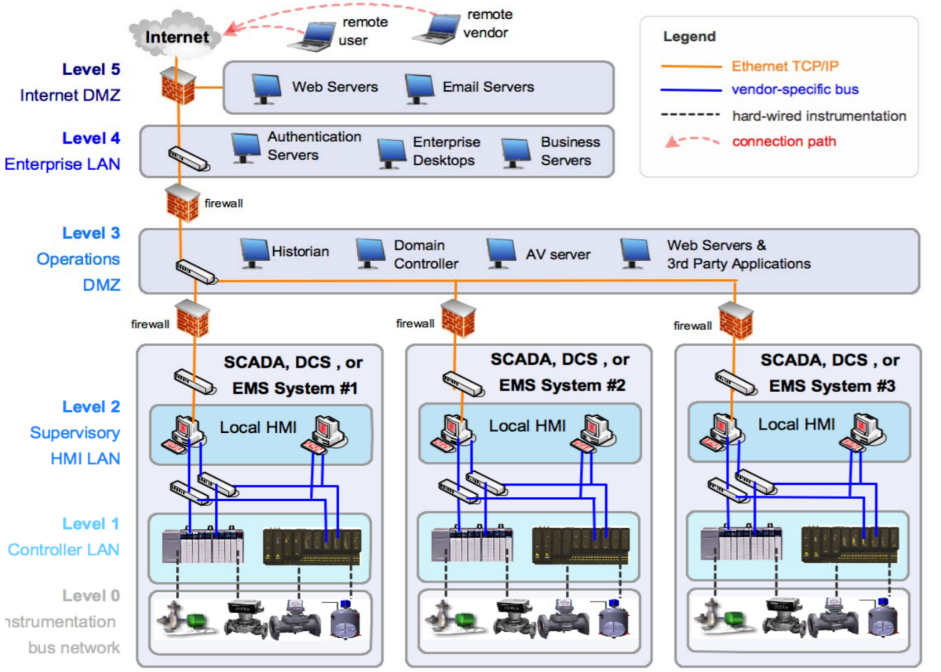
Outline of talk

SCADA over public networks

One seemingly simple objective

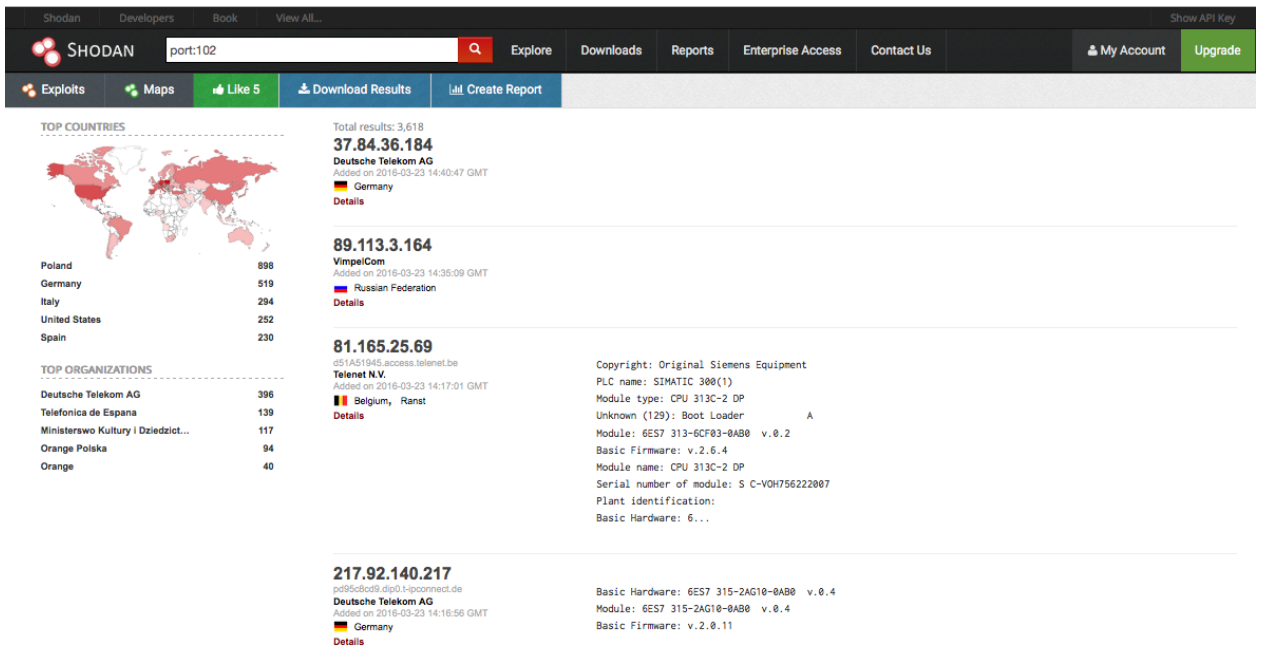
"[...] SCADA communications should be encrypted and routed through a VPN tunnel through corporate IT or other non-critical networks. [...]"

["*Securing the move to IP-based SCADA/PLC networks*", UK Centre for the Protection of National Infrastructure (CPNI), 2011]



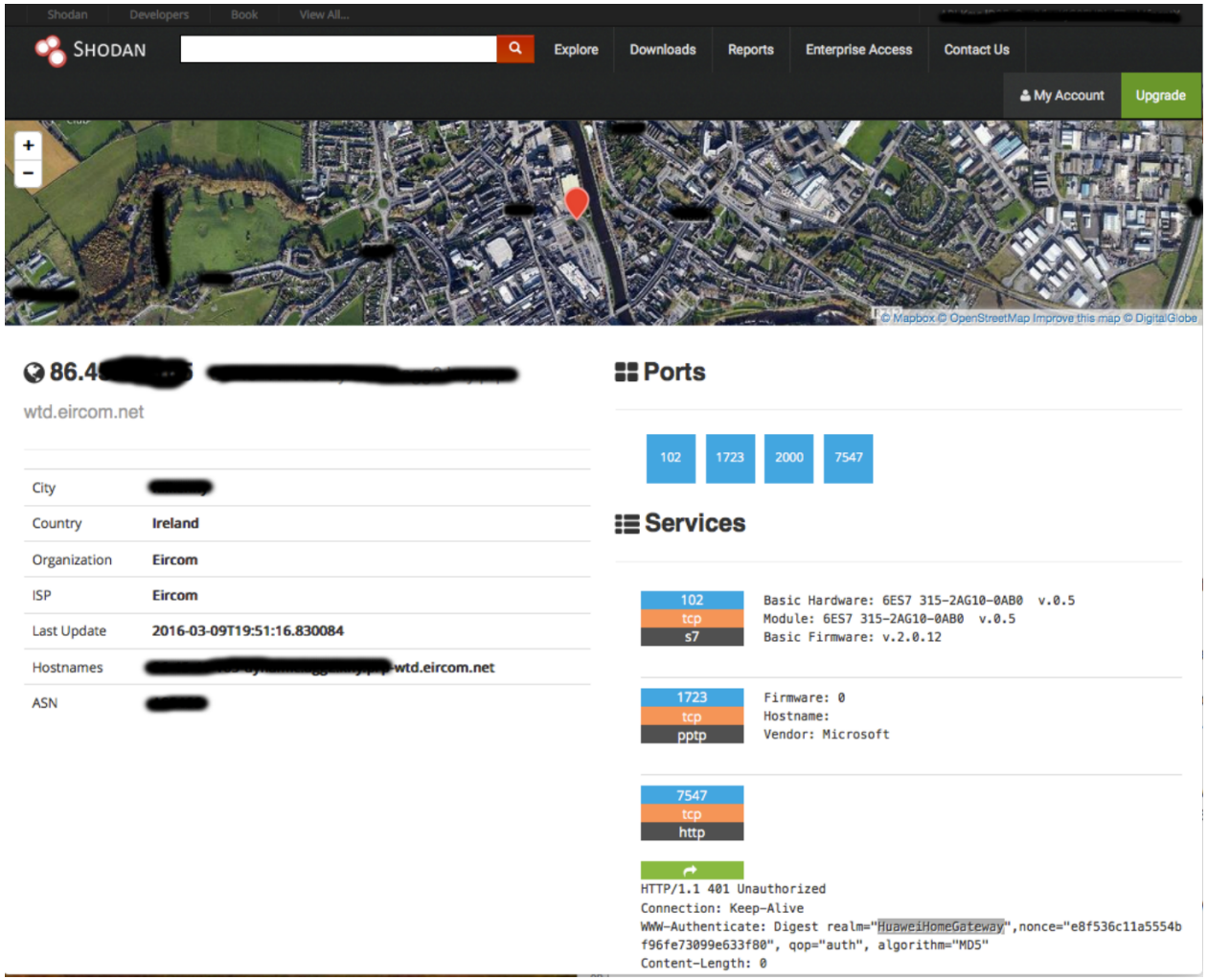
Looking for a use case

Siemens S7comm protocol over TCP/TSAP on Port 102



The ICS use case

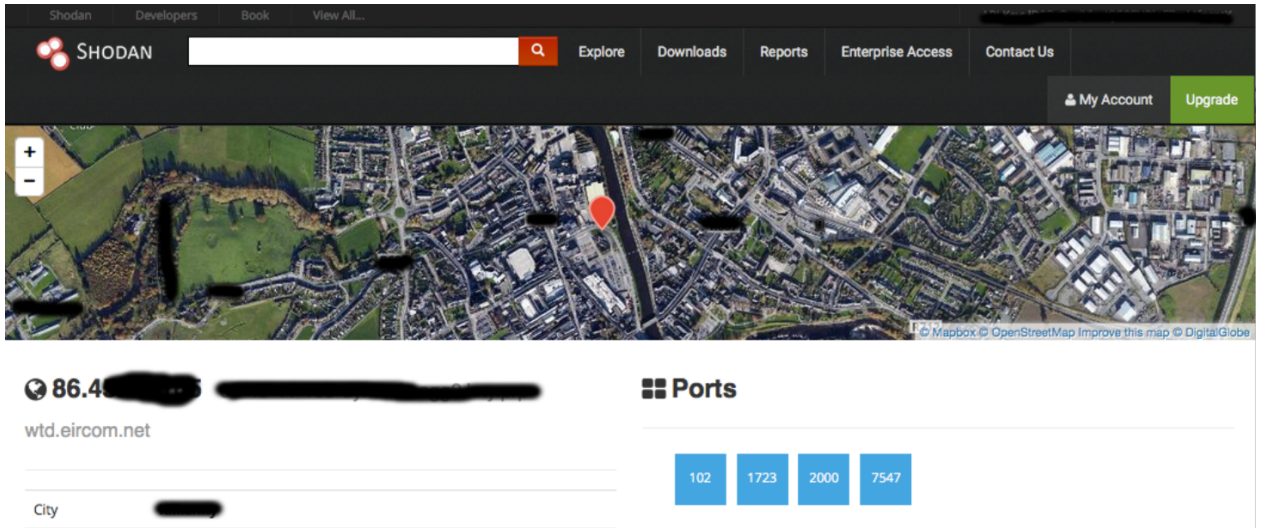
Siemens S7comm protocol over TCP/TSAP on Port 102

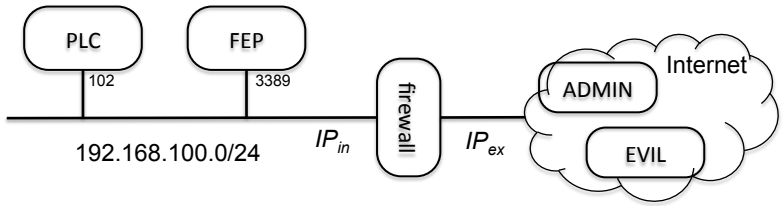


[S.N. Foley, *Getting security objectives wrong, a cautionary tale*, SPW 2017]

The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102

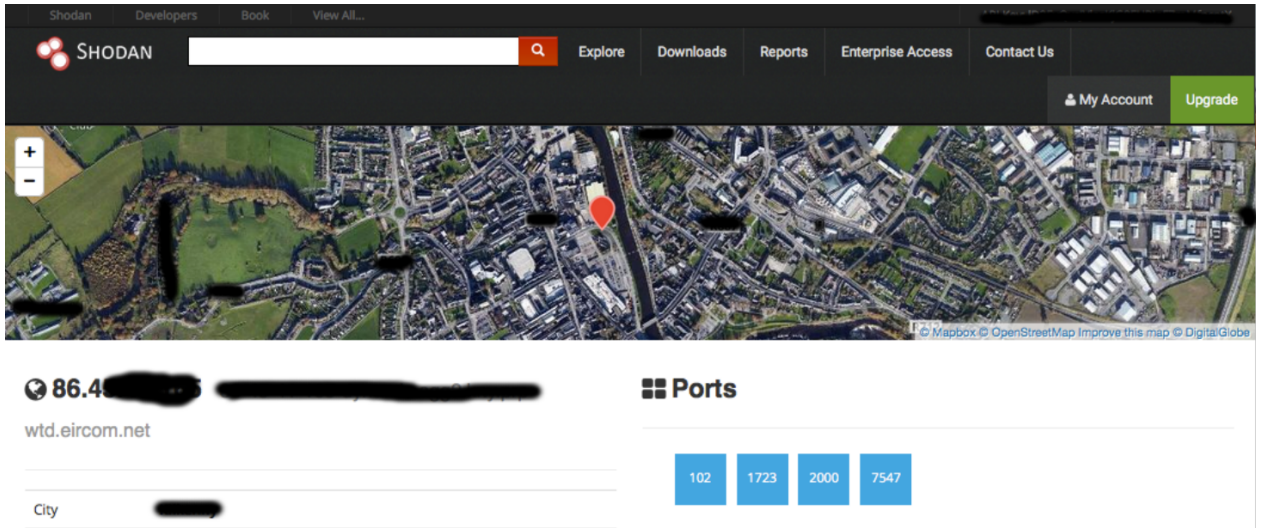


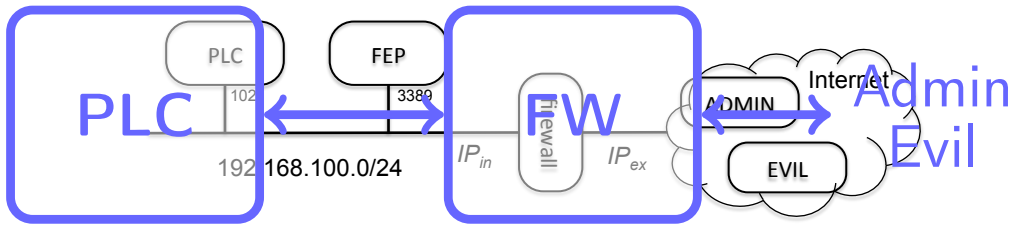


[S.N. Foley, *Getting security objectives wrong, a cautionary tale*, SPW 2017]

The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102

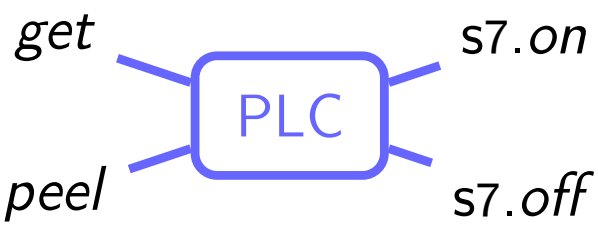




[S.N. Foley, *Getting security objectives wrong, a cautionary tale*, SPW 2017]

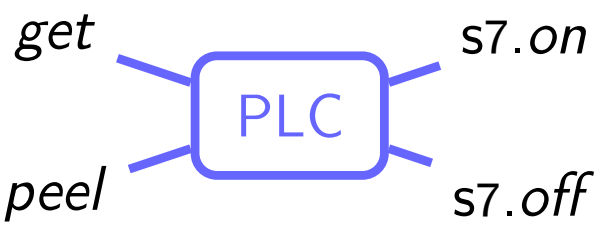
Safety properties

Imagine a potato peeling ICS



Safety properties

Imagine a potato peeling ICS

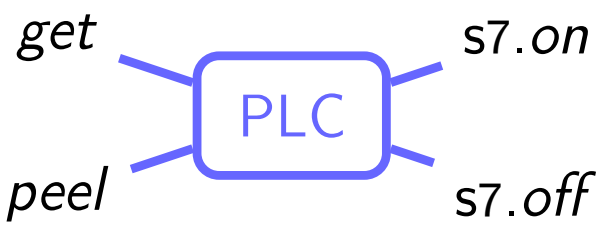


Functional Requirement

$$REQ \mathrel{\widehat{=}} (get \rightarrow peel \rightarrow REQ) \\ \Box\, (s7?x \rightarrow REQ)$$

Safety properties

Imagine a potato peeling ICS



Functional Requirement

$$REQ \mathrel{\widehat{=}} (get \rightarrow peel \rightarrow REQ) \\ \Box\, (s7?x \rightarrow REQ)$$

Idealized Implementation

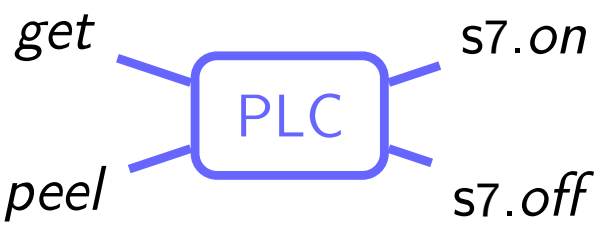
Supervision on channel s7:

$$PLC \mathrel{\widehat{=}} (s7.on \rightarrow POT)$$

$$POT \mathrel{\widehat{=}} (get \rightarrow peel \rightarrow POT) \\ \Box\, (s7.off \rightarrow PLC)$$

Safety properties

Imagine a potato peeling ICS



Functional Requirement

$$REQ \mathrel{\widehat{=}} (get \rightarrow peel \rightarrow REQ) \\ \Box\, (s7?x \rightarrow REQ)$$

Idealized Implementation

Supervision on channel s7:

$$PLC \mathrel{\widehat{=}} (s7.on \rightarrow POT)$$

$$POT \mathrel{\widehat{=}} (get \rightarrow peel \rightarrow POT) \\ \Box\, (s7.off \rightarrow PLC)$$

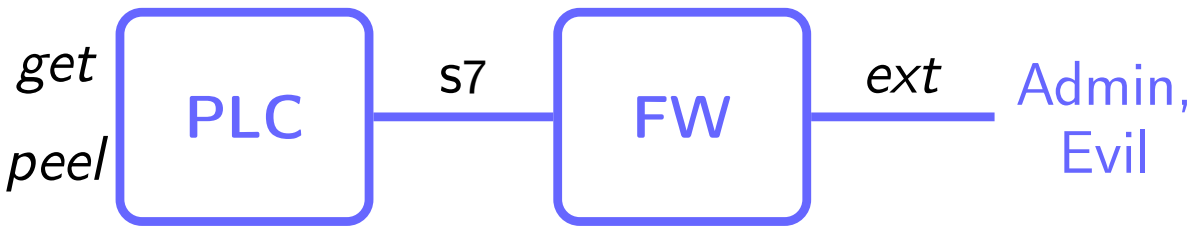
Safety Refinement

Every implementation trace is valid requirement trace.

$$PLC \sqsubseteq REQ$$

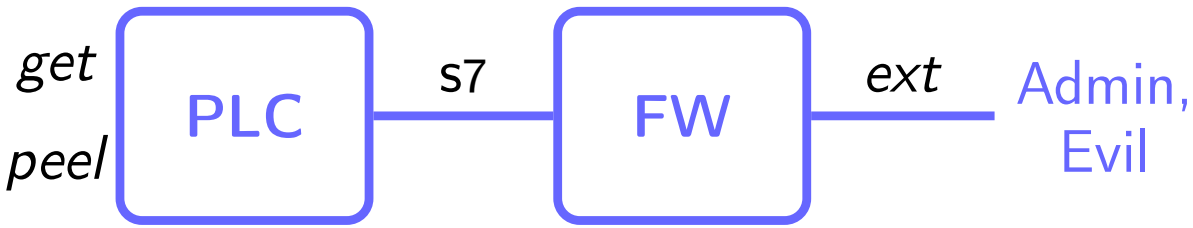
Implementing requirements in the presence of an attacker

Firewall as a security control



Implementing requirements in the presence of an attacker

Firewall as a security control

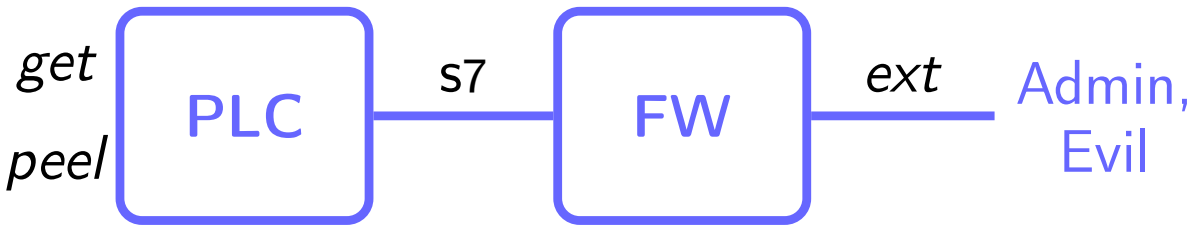


Pass only external supervision packets from Admin

$$FW \mathrel{\widehat{=}} (ext?ip?op \rightarrow (\text{if } (ip = \text{Admin}) \text{ then } s7!op \rightarrow FW \text{ else } FW))$$

Implementing requirements in the presence of an attacker

Firewall as a security control



Pass only external supervision packets from Admin

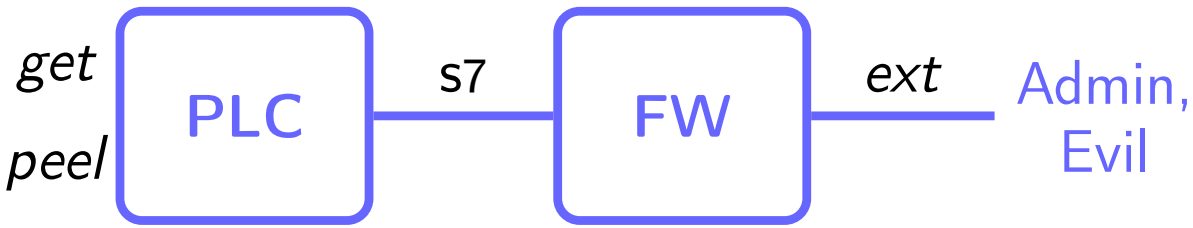
$$FW \mathrel{\widehat{=}} (ext?ip?op \rightarrow (\text{if } (ip = \text{Admin}) \text{ then } s7!op \rightarrow FW \text{ else } FW))$$

Deployed system includes its infrastructure

$$Deployed \mathrel{\widehat{=}} PLC \parallel FW$$

Implementing requirements in the presence of an attacker

Firewall as a security control



Pass only external supervision packets from Admin

$$FW \mathrel{\widehat{=}} (ext?ip?op \rightarrow (\text{if } (ip = \text{Admin}) \text{ then } s7!op \rightarrow FW \text{ else } FW))$$

Deployed system includes its infrastructure

$$Deployed \mathrel{\widehat{=}} PLC \parallel FW \parallel Evil \parallel Admin$$

A declarative definition of security

Robust satisfaction of functional requirements

Deployed system and infrastructure is sufficiently robust to be able to satisfy the functional requirements in the presence of threats.

$$(System \parallel Infrastructure) \sqsubseteq^{A} Requirement$$

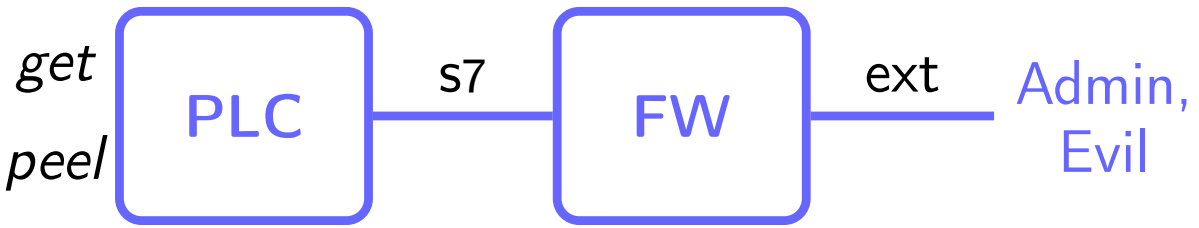
Implementation S locally refines requirement R at interface A:

$$S \sqsubseteq^{A} R \Leftrightarrow \forall s : traces(S) \bullet \exists r : traces(R) \bullet s \upharpoonright A = r \upharpoonright A$$

[S.N. Foley, *A non-functional approach to Integrity*, IEEE JSAS 21, 2003]

Robust Satisfaction

$$REQ \mathrel{\widehat{=}} (get \rightarrow peel \rightarrow REQ) \,\square\, (s7?x \rightarrow REQ)$$



$$PLC \mathrel{\widehat{=}} (s7.on \rightarrow POT)$$

$$POT \mathrel{\widehat{=}} (get \rightarrow peel \rightarrow POT) \,\square\, (s7.off \rightarrow PLC)$$

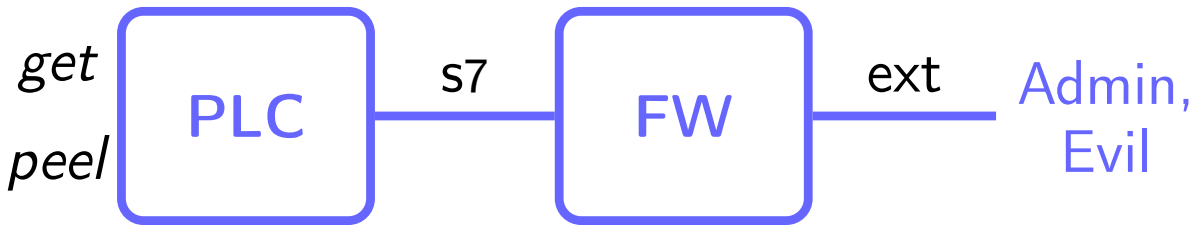
$$FW \mathrel{\widehat{=}} (ext?ip?op \rightarrow (\text{if } (ip = \text{Admin}) \text{ then } s7!op \rightarrow FW \text{ else } FW))$$

Robust satisfaction in the ICS

$$(System \parallel Infrastructure) \sqsubseteq^{A} Requirements$$

Robust Satisfaction

$$REQ \mathrel{\widehat{=}} (get \rightarrow peel \rightarrow REQ) \,\square\, (s7?x \rightarrow REQ)$$



$$PLC \mathrel{\widehat{=}} (s7.on \rightarrow POT)$$

$$POT \mathrel{\widehat{=}} (get \rightarrow peel \rightarrow POT) \,\square\, (s7.off \rightarrow PLC)$$

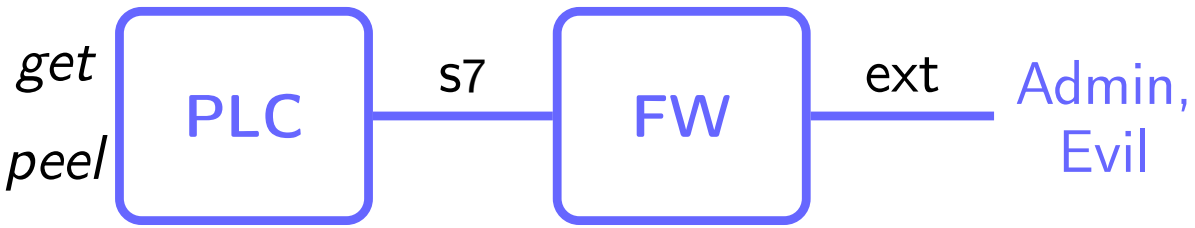
$$FW \mathrel{\widehat{=}} (ext?ip?op \rightarrow (\text{if } (ip = \text{Admin}) \text{ then } s7!op \rightarrow FW \text{ else } FW))$$

Robust satisfaction in the ICS

$$(PLC \parallel FW \parallel Admin \parallel Evil) \sqsubseteq^{\{get,peel\}} REQ$$

Robust Satisfaction

$$REQ \mathrel{\widehat{=}} (get \rightarrow peel \rightarrow REQ) \,\Box\, (s7?x \rightarrow REQ)$$



$$PLC \mathrel{\widehat{=}} (s7.on \rightarrow POT)$$

$$POT \mathrel{\widehat{=}} (get \rightarrow peel \rightarrow POT) \,\Box\, (s7.off \rightarrow PLC)$$

$$FW \mathrel{\widehat{=}} (ext?ip?op \rightarrow (\text{if } (ip = \text{Admin}) \text{ then } s7!op \rightarrow FW \text{ else } FW))$$

Robust satisfaction in the ICS

$$(PLC \parallel FW \parallel STOP_{Untrusted}) \sqsubseteq^{\{get,peel\}} REQ$$

where $Untrusted \mathrel{\widehat{=}} \{ip : IP, op : OP \mid ip \neq \text{Admin} \bullet ext.ip.op\}$

Examples of robust satisfaction

Information flow

No information flow across firewall FW from untrusted external network interfaces to the internal S7 interface.

$$(FW \| STOP_{Untrusted}) \equiv^{\{s7.on, s7.off\}} FW$$

External consistency (integrity)

No observable difference between system with benign infrastructure and system with malicious infrastructure.

Subterfuge freedom in Trust Management

Freedom from a freshness-style attack in delegation mechanisms.

Simple trace-based definition; can have other variations.

[S.N. Foley, *Noninterference analysis of subterfuge*, J. Trust Mgmt, 2013]

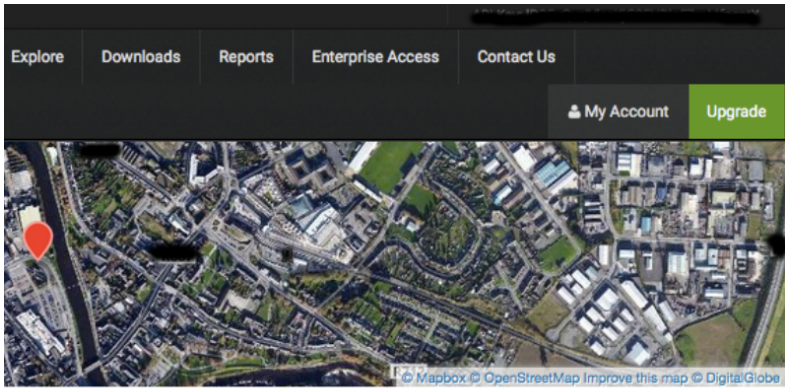
The reality of the ICS use case

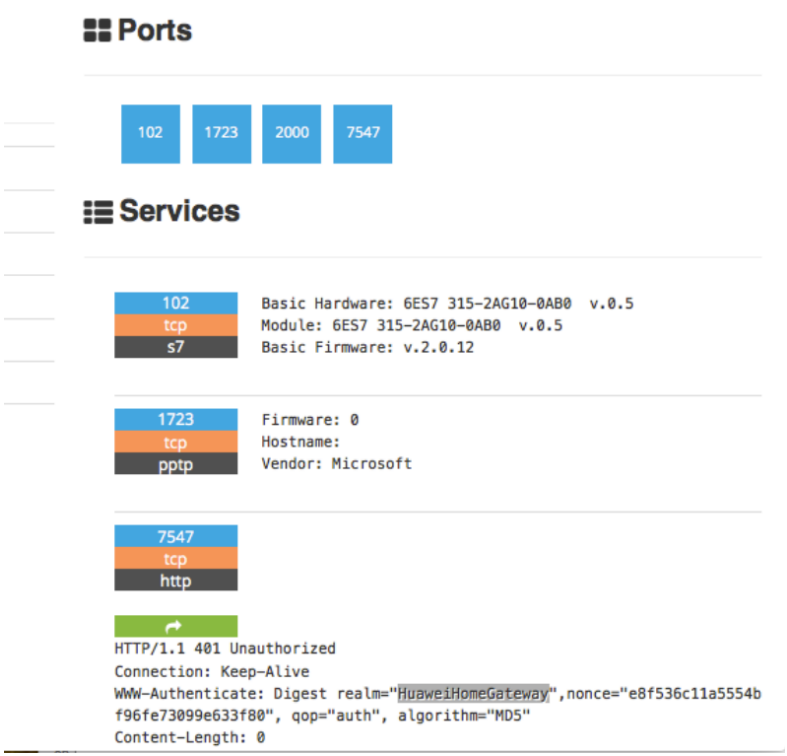
Many services, many attacks, much to go wrong

S7comm on Port 102

CVE-2015-2177/Denial of service;

Preset userid/password `Basisk`;





The reality of the ICS use case

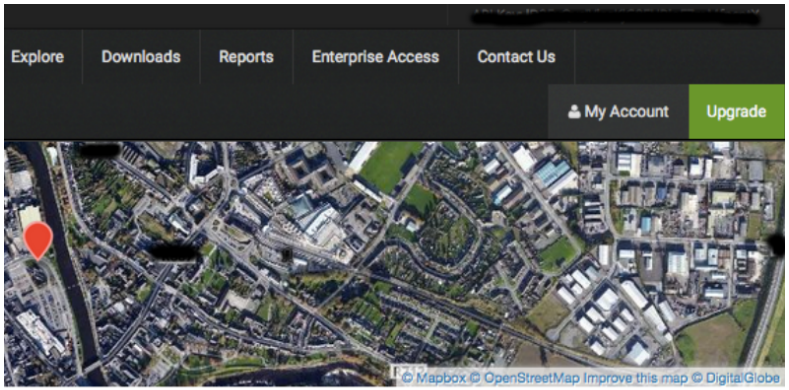
Many services, many attacks, much to go wrong

S7comm on Port 102

CVE-2015-2177/Denial of service;
Preset userid/password `Basisk`;

PPTP on Port 1723

MS Security Advisory 2743314:
MS-CHAPv2 weakness;. . .



Ports

102 1723 2000 7547

Services

102 tcp s7 — Basic Hardware: 6ES7 315-2AG10-0AB0 v.0.5
Module: 6ES7 315-2AG10-0AB0 v.0.5
Basic Firmware: v.2.0.12

1723 tcp pptp — Firmware: 0
Hostname:
Vendor: Microsoft

7547 tcp http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

The reality of the ICS use case

Many services, many attacks, much to go wrong

S7comm on Port 102

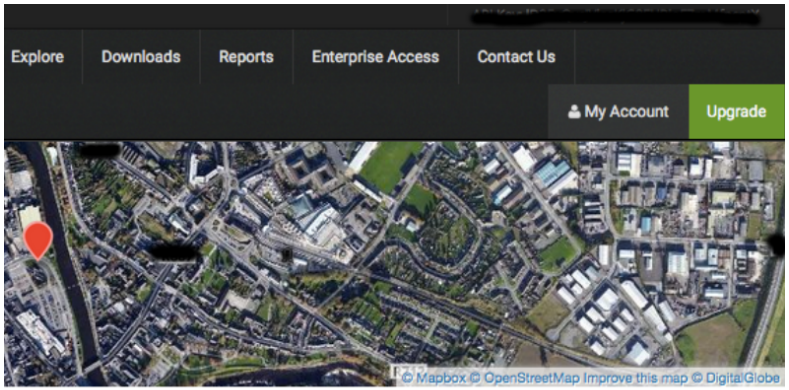
CVE-2015-2177/Denial of service;
Preset userid/password `Basisk`;

PPTP on Port 1723

MS Security Advisory 2743314:
MS-CHAPv2 weakness;. . .

CWMP over HTTP

CVE-2014-9222, CVE-2014-9223:
misfortune cookie vulnerability;. . .



Ports

102 1723 2000 7547

Services

102 tcp s7 — Basic Hardware: 6ES7 315-2AG10-0AB0 v.0.5
Module: 6ES7 315-2AG10-0AB0 v.0.5
Basic Firmware: v.2.0.12

1723 tcp pptp — Firmware: 0
Hostname:
Vendor: Microsoft

7547 tcp http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

The reality of the ICS use case

Many services, many attacks, much to go wrong

S7comm on Port 102

CVE-2015-2177/Denial of service;
Preset userid/password `Basisk`;

PPTP on Port 1723

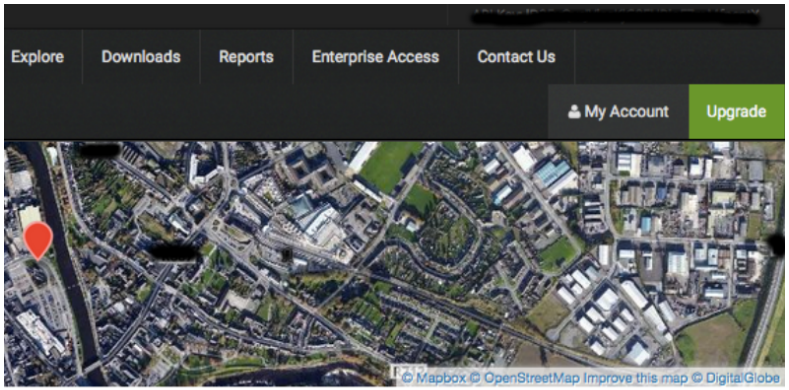
MS Security Advisory 2743314:
MS-CHAPv2 weakness;. . .

CWMP over HTTP

CVE-2014-9222, CVE-2014-9223:
misfortune cookie vulnerability;. . .

Huawei home gateway

CVE-2015-7254 path traversal;
CVE-2013-6786 XSS; . . .



Ports

102 1723 2000 7547

Services

102 tcp s7 — Basic Hardware: 6ES7 315-2AG10-0AB0 v.0.5
Module: 6ES7 315-2AG10-0AB0 v.0.5
Basic Firmware: v.2.0.12

1723 tcp pptp — Firmware: 0
Hostname:
Vendor: Microsoft

7547 tcp http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

The reality of the ICS use case

Many services, many attacks, much to go wrong

S7comm on Port 102

CVE-2015-2177/Denial of service;
Preset userid/password `Basisk`;

PPTP on Port 1723

MS Security Advisory 2743314:
MS-CHAPv2 weakness;. . .

CWMP over HTTP

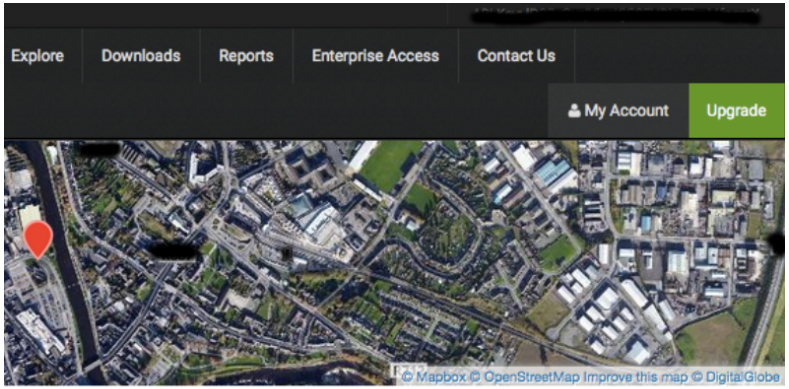
CVE-2014-9222, CVE-2014-9223:
misfortune cookie vulnerability;. . .

Huawei home gateway

CVE-2015-7254 path traversal;
CVE-2013-6786 XSS; . . .

Siemens FAQ8970169

"Port 102 [...] must be enabled for the complete transfer route"



Ports

102 1723 2000 7547

Services

102 tcp s7 — Basic Hardware: 6ES7 315-2AG10-0AB0 v.0.5
Module: 6ES7 315-2AG10-0AB0 v.0.5
Basic Firmware: v.2.0.12

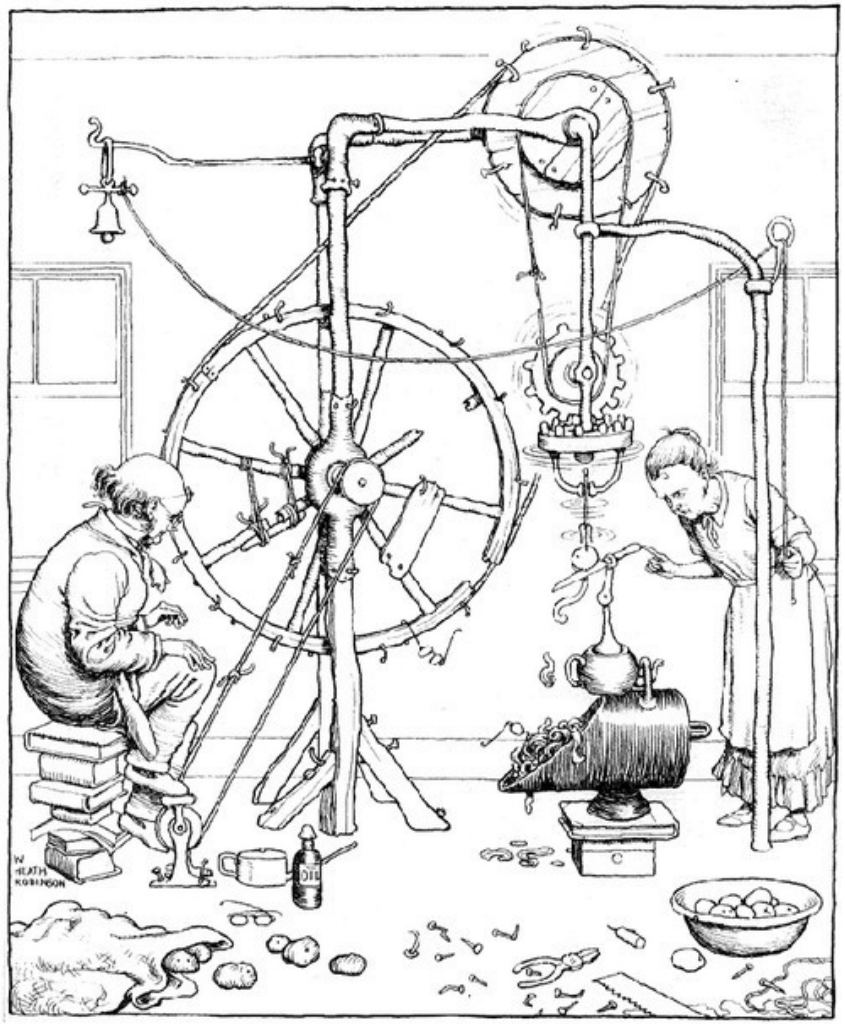
1723 tcp pptp — Firmware: 0
Hostname:
Vendor: Microsoft

7547 tcp http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

Models and reality

Models and reality



The Professor's invention for peeling potatoes.

Security Threat Management

Describing security operationally

Internal Control

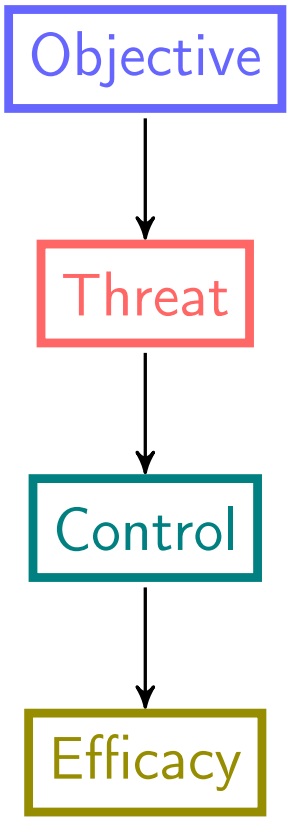
Security in terms of security controls that mitigate threats to achieving objectives.

Control catalogues and compliance

Catalogues of operational best practices for dealing with security threats.

Efficacy metrics

Metrics on outcome of tests that security controls mitigate threats as expected.



[S.N. Foley, *Security Risk Management using internal controls*, ACM WISG, 2009]

Threat management for the ICS use case

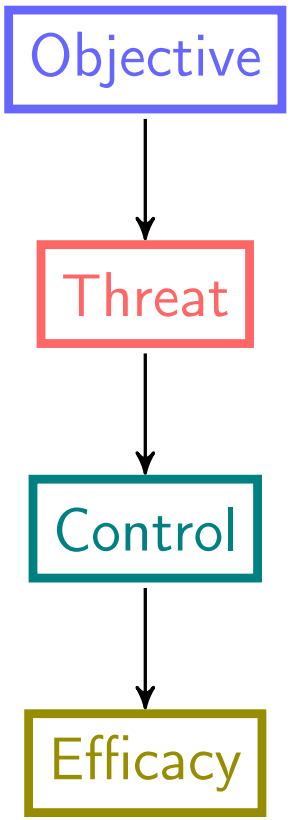
Objective: provide remote supervisory control to ICS

Threat: attacker can access PLC

- CPNI: tunnel S7 traffic over VPN.
- Only admin IP access to VPN.
- Software update mechanism.

Efficacy: Intrusion Detection System

Snort rules that check for suspicious S7 packets on internal network.



Threat management for the ICS use case

Objective: provide remote supervisory control to ICS

Threat: attacker can access PLC

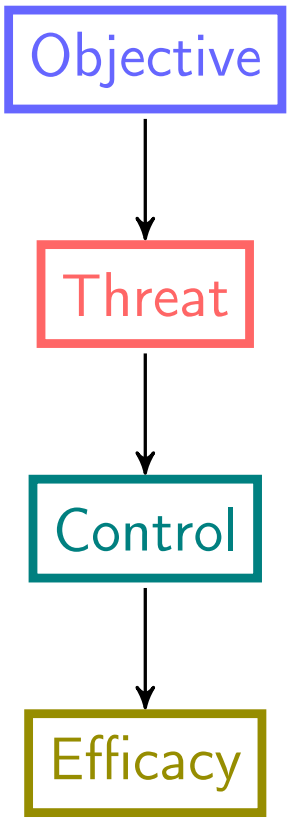
- CPNI: tunnel S7 traffic over VPN.
- Only admin IP access to VPN.
- Software update mechanism.

Efficacy: Intrusion Detection System

Snort rules that check for suspicious S7 packets on internal network.

Threat: PLC is unreachable

- FAQ: open Port 102 on router



Operational security in practice

Many threats, many controls, much to go wrong

Measuring operational security

Caculating the impact of a security control failure

A Complete Guide to the
Common Vulnerability Scoring System
Version 2.0

2.3.2 Target Distribution (TD)
This metric measures the proportion of vulnerable systems. It is meant as an environment-specific indicator in order to approximate the percentage of systems that could be affected by the vulnerability.

Value	Description
None	No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting. Effectively 0% of the environment is at risk.
Low	Targets exist inside the environment, but on a small scale. Between 1%-25% of the total environment is at risk.
Medium	Targets exist inside the environment, but on a medium scale. Between 26%-75% of the total environment is at risk.
High	Targets exist inside the environment on a considerable scale. Between 76%-100% of the total environment is considered at risk.
Not Defined	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Measuring operational security

Caculating the impact of a security control failure

A Complete Guide to the
Common Vulnerability Scoring System
Version 2.0

2.3.2 Target Distribution (TD)
This metric measures the proportion of vulnerable systems. It is meant as an environment-specific indicator in order to approximate the percentage of systems that could be affected by the vulnerability.

Value	Description
None	No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting. Effectively 0% of the environment is at risk.
Low	Targets exist inside the environment, but on a small scale. Between 1%-25% of the total environment is at risk.
Medium	Targets exist inside the environment, but on a medium scale. Between 26%-75% of the total environment is at risk.
High	Targets exist inside the environment on a considerable scale. Between 76%-100% of the total environment is considered at risk.
Not Defined	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

COMMISSION REGULATION (EC) No 2257/94
of 16 September 1994
laying down quality standards for bananas

III. SIZING
Sizing is determined by:

- the length of the fruit expressed in centimetres and measured along the convex face, from the blossom end to the point where the peduncle joins the crown,
- the grade, i.e. the measurement, in millimetres, of the **thickness of a transverse section of the fruit between the lateral faces and the middle, perpendicularly to the longitudinal axis**

The reference fruit for measurement of the length and grade is:

- the median finger on the outer row of the hand,
- the finger next to the cut sectioning the hand, on the outer row of the cluster.

The minimum length permitted is 14 cm and the minimum grade permitted is 27 mm.

Defining security

The declarative view

- Define what security denotes
- Model requirements, system, controls, infrastructure, attackers.
- Security efficacy through security properties; information flow, ...

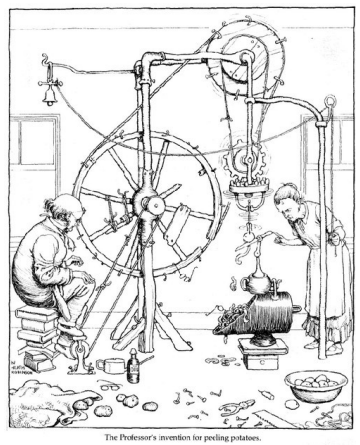
Defining security

The declarative view

- Define what security denotes
- Model requirements, system, controls, infrastructure, attackers.
- Security efficacy through security properties; information flow, ...

The operational view

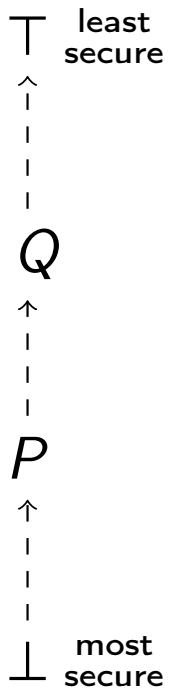
- Define security in terms of operation
- Link threats to controls based on compliance with best practices.
- Security efficacy through metrics, measuring/reporting control efficacy.



Security defined as comparison

Secure Replacement $P \sqsubseteq Q$

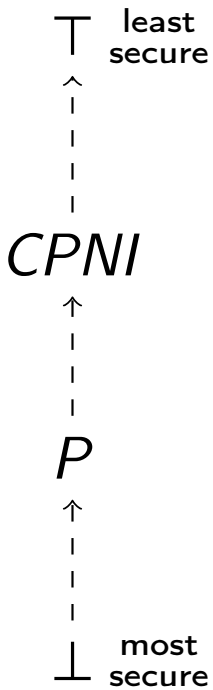
- P is no less secure than Q.
- Currently upheld objective Q can be securely replaced by objective P.



Security defined as comparison

Secure Replacement $P \sqsubseteq Q$

- P is no less secure than Q.
- Currently upheld objective Q can be securely replaced by objective P.
- Compliance: $P \sqsubseteq CPNI$



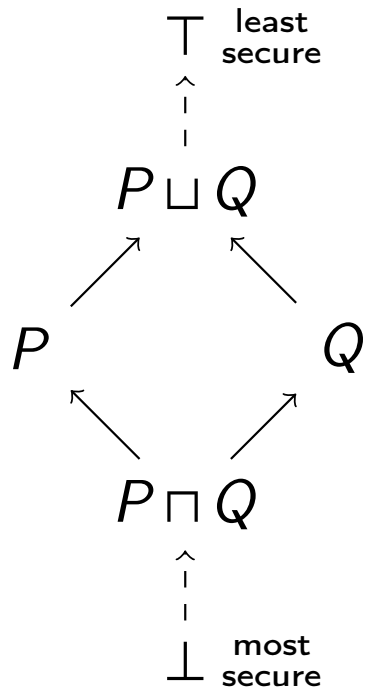
Security defined as comparison

Secure Replacement $P \sqsubseteq Q$

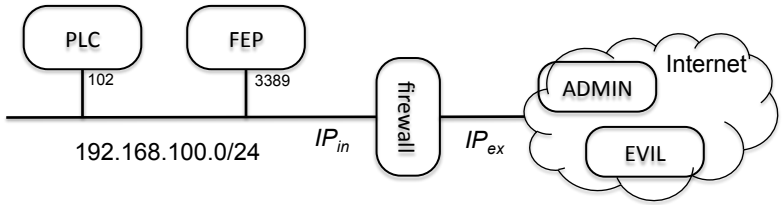
- P is no less secure than Q.
- Currently upheld objective Q can be securely replaced by objective P.
- Compliance: $P \sqsubseteq CPNI$

Secure Composition $P \sqcap Q$, $P \sqcup Q$

- A lattice of objectives.
- Objective $P \sqcap Q$ as 'best' objective that is no less secure than P and Q.
- Replace P by $P \sqcap (CPNI \sqcup RFC5735)$



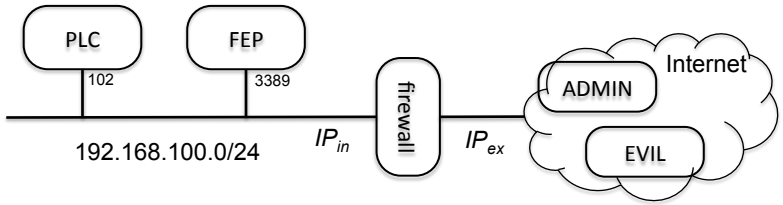
Objectives as firewall policies



Initial policy/FAQ *UPol*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	plc	102	Allow
2	...	*.*.*.*	≥ 1024	fep	3389	Allow

Objectives as firewall policies



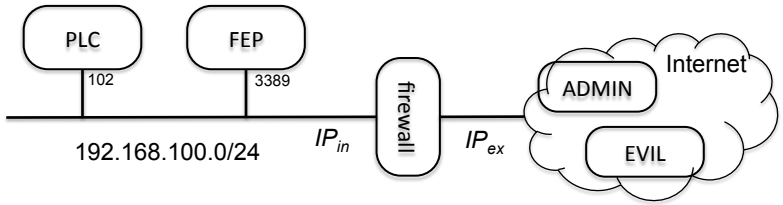
Initial policy/FAQ *UPol*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	plc	102	Allow
2	...	*.*.*.*	≥ 1024	fep	3389	Allow

CPNI Recommendations: *CPNI*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	≥ 1024	plc	102	Allow
2	...	*.*.*.*	*	plc	102	Drop
3	...	external IPs	≥ 1024	fep	3389	Allow

Objectives as firewall policies



Initial policy/FAQ *UPol*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	plc	102	Allow
2	...	*.*.*.*	≥ 1024	fep	3389	Allow

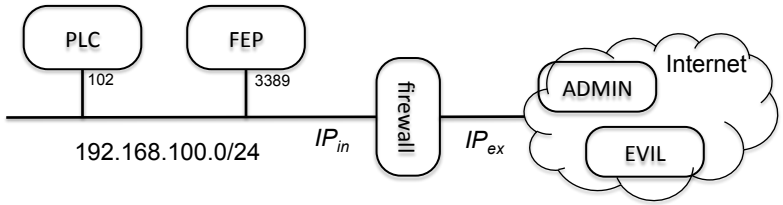
CPNI Recommendations: *CPNI*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	≥ 1024	plc	102	Allow
2	...	*.*.*.*	*	plc	102	Drop
3	...	external IPs	≥ 1024	fep	3389	Allow

Remote Desktop Policy: *RPol*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	admin	≥ 1024	fep	3389	Allow
2	...	*.*.*.*	*	fep	3389	Drop

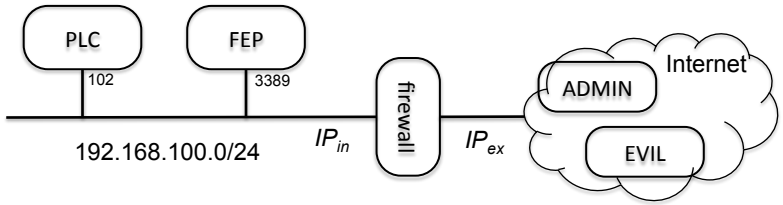
Conventional firewall policy composition



UPol;CPNI;RPol

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	plc	102	Allow
2	...	*.*.*.*	≥ 1024	fep	3389	Allow
3	...	192.168.100.0/24	≥ 1024	plc	102	Allow
4	...	*.*.*.*	*	plc	102	Drop
5	...	external	≥ 1024	fep	3389	Allow
6	...	admin	≥ 1024	fep	3389	Allow
7	...	*.*.*.*	*	fep	3389	Drop

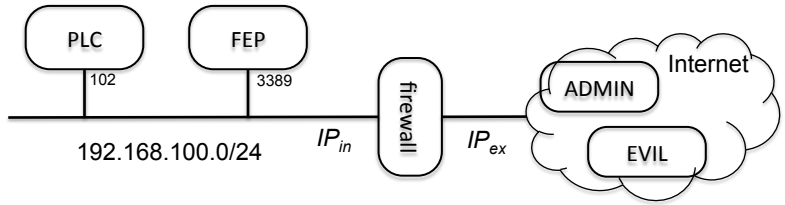
Conventional firewall policy composition



UPol;CPNI;RPol

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	plc	102	Allow
2	...	*.*.*.*	≥ 1024	fep	3389	Allow
3	...	192.168.100.0/24	≥ 1024	plc	102	Allow
4	...	*.*.*.*	*	plc	102	Drop
5	...	external	≥ 1024	fep	3389	Allow
6	...	admin	≥ 1024	fep	3389	Allow
7	...	*.*.*.*	*	fep	3389	Drop

Conventional firewall policy composition



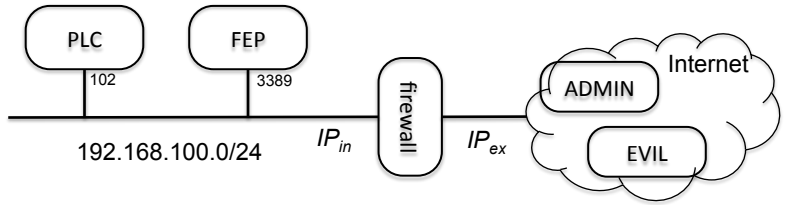
UPol;CPNI;RPol

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	plc	102	Allow
2	...	*.*.*.*	≥ 1024	fep	3389	Allow
3	...	192.168.100.0/24	≥ 1024	plc	102	Allow
4	...	*.*.*.*	*	plc	102	Drop
5	...	external	≥ 1024	fep	3389	Allow
6	...	admin	≥ 1024	fep	3389	Allow
7	...	*.*.*.*	*	fep	3389	Drop

CPNI;RPol;UPol

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	≥ 1024	plc	102	Allow
2	...	*.*.*.*	*	plc	102	Drop
3	...	external	≥ 1024	fep	3389	Allow
4	...	admin	≥ 1024	fep	3389	Allow
5	...	*.*.*.*	*	fep	3389	Drop
6	...	*.*.*.*	≥ 1024	plc	102	Allow
7	...	*.*.*.*	≥ 1024	fep	3389	Allow

Conventional firewall policy composition



UPol;CPNI;RPol

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	plc	102	Allow
2	...	*.*.*.*	≥ 1024	fep	3389	Allow
3	...	192.168.100.0/24	≥ 1024	plc	102	Allow
4	...	*.*.*.*	*	plc	102	Drop
5	...	external	≥ 1024	fep	3389	Allow
6	...	admin	≥ 1024	fep	3389	Allow
7	...	*.*.*.*	*	fep	3389	Drop

CPNI;RPol;UPol

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	≥ 1024	plc	102	Allow
2	...	*.*.*.*	*	plc	102	Drop
3	...	external	≥ 1024	fep	3389	Allow
4	...	admin	≥ 1024	fep	3389	Allow
5	...	*.*.*.*	*	fep	3389	Drop
6	...	*.*.*.*	≥ 1024	plc	102	Allow
7	...	*.*.*.*	≥ 1024	fep	3389	Allow

A policy algebra for firewall policies

A simplified version

Secure Replacement $P \sqsubseteq Q$

Policy Q can be replaced by policy P, if P is no less restrictive than Q. For all $P, Q : Policy$:

$$P \sqsubseteq Q \Leftrightarrow (accepts(P) \subseteq accepts(Q)) \wedge (denies(P) \supseteq denies(Q))$$

Lattice of policies $(Policy, \sqsubseteq, \sqcup, \sqcap)$

$Policy$ forms a lattice under $\sqsubseteq$, with lub $\sqcup$ and glb $\sqcap$.

Policy compositions

$$Pol = UPol \sqcap (CPNI \sqcup RPol)$$

$$Pol' = Pol \sqcap RFC5735$$

[Neville&Foley, *Reasoning About Firewall Policies Through Refinement and Composition*, DBSec 2016.]

Some related Work

Process calculi and security properties

Information theoretic definitions of security in all its forms.
[Jacob IEEE S&P 1988] Security refinement over specifications.
[Foley JCAS 2003] Robust satisfaction.

Policy algebras

[Foley IEEE S&P 1989] lattice of flow policies;
[Wijesekera ACMTISS-2003] policy algebras as predicates;
[ZhaoBellovin CTS 2007] Firewall policy composition algebra;
[Adão CSF-2014] Formal reasoning over firewall deployments;
[FoleyNeville DbSec2016] lattice of ipTables policies.

Conclusion

Convoluted systems

Many parts, many players, many objectives, much to go wrong.

Secure by comparison

Security objectives defined *implicitly* by comparison with past configuration, best practices, etc.

Firewall Algebra

Compute, compare and reason about firewall policies.

Conclusion

Convoluted systems

Many parts, many players, many objectives, much to go wrong.

Secure by comparison

Security objectives defined *implicitly* by comparison with past configuration, best practices, etc.

Firewall Algebra

Compute, compare and reason about firewall policies.

Challenge

Considering multiple security objectives? Find a lattice ordering.