

Security in Convolved Systems

Simon Foley

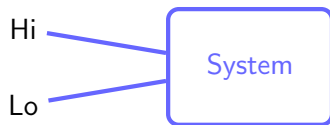
IMT Atlantique, Rennes

30 May, 2017

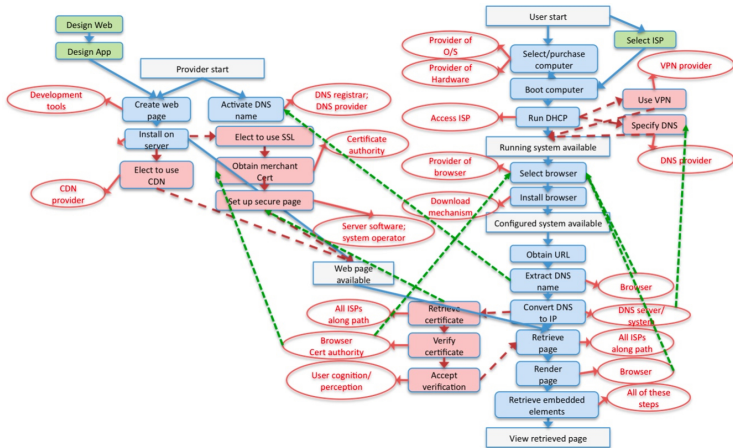
What is meant by a secure system?

Information theoretic definitions

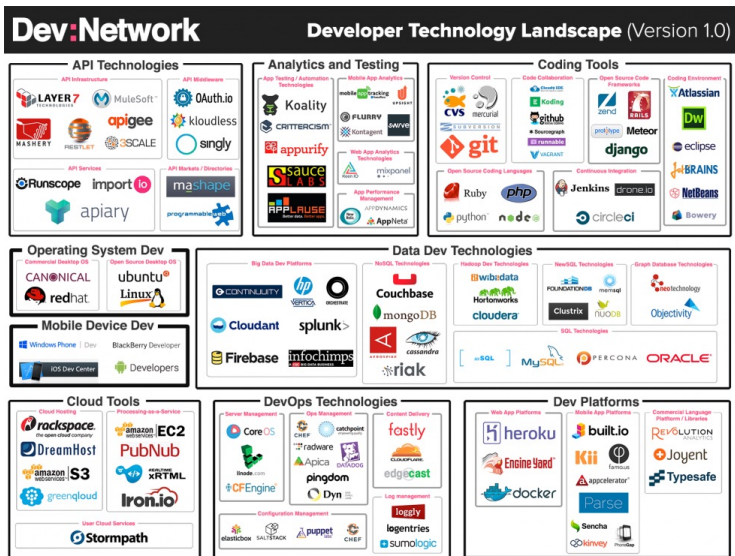
Actions at Hi interface
do not interfere with
actions at Lo interface



Contemporary systems are more convoluted,



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

TECHNOLOGY

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

By NICOLE PERLBOTH 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



copyright © 2008 John Robinson, www.johnrobinson.com

Security in convoluted systems

Outline of talk

Use Case

Declarative security

Operational security

Security by comparison

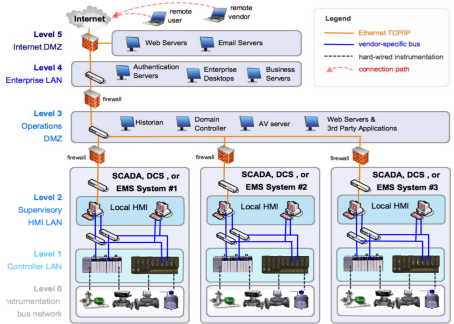
Conclusion

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

SHODAN port:102

Exploits Maps Like 0 Download Results Create Report

TOP COUNTRIES

Country	Count
Poland	898
Germany	819
Italy	294
United States	282
Spain	238

TOP ORGANIZATIONS

Organization	Count
Deutsche Telekom AG	388
Telefonos de Espana	138
Ministero Kultury i Dziedzictwa	117
Orange Polska	84
Orange	48

Total results: 5,678

37,84,36,184
Deutsche Telekom AG
Address on 2018-03-23: 14:40:47 GMT
Germany
Details

89,113,3,164
VimpacCom
Address on 2018-03-23: 14:38:09 GMT
Russian Federation
Details

81,165,25,69
Internet R X
Address on 2018-03-23: 14:37:01 GMT
Belgium, France
Details

Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(T)
Module type: CPU 313C-2 DP
Unknown (129): Boot Loader A
Module: 6ES7 313-6EG03-0AB0 v.0.2
Basic Firmware: v.2.6.4
Module name: CPU 313C-2 DP
Serial number of module: S C-V0H79622087
Plant Identification:
Basic Hardware: 6...

217,92,140,217
Deutsche Telekom AG
Address on 2018-03-23: 14:16:58 GMT
Germany
Details

Basic Hardware: 6ES7 313-6AG03-0AB0 v.0.4
Module: 6ES7 313-6AG03-0AB0 v.0.4
Basic Firmware: v.2.8.11

The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102

The screenshot shows the SHODAN search results for the IP address 86.4... The interface includes a search bar, navigation links (Explore, Downloads, Reports, Enterprise Access, Contact Us), and a 'My Account' button. A satellite map shows the location of the IP. Below the map, the following metadata is displayed:

- IP: 86.4... (redacted)
- Domain: wtd.eircom.net
- City: (redacted)
- Country: Ireland
- Organization: Eircom
- ISP: Eircom
- Last Update: 2016-03-09T19:51:16.830084
- Hostnames: (redacted), wtd.eircom.net
- ASN: (redacted)

The 'Ports' section shows four open ports: 102, 1723, 2000, and 7547. The 'Services' section provides details for each port:

- 102**: Basic Hardware: GE57 315-2AG10-0AB0 v.0.5; Module: GE57 315-2AG10-0AB0 v.0.5; s7; Basic Firmware: v.2.0.12
- 1723**: Firmware: 0; Hostnames: (redacted); Vendor: Microsoft
- 7547**: http

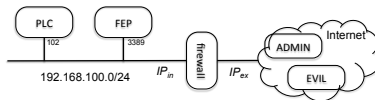
The HTTP response for port 7547 is shown as:

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

The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102

The screenshot shows a Shodan search result for the IP address 86.4... (redacted). The interface includes a search bar with the Shodan logo, navigation links (Explore, Downloads, Reports, Enterprise Access, Contact Us), and a 'My Account' section with an 'Upgrade' button. Below the search bar is a satellite map of a city with a red location pin. Underneath the map, the IP address is displayed as 86.4... (redacted) with the domain wtd.eircom.net. A 'Ports' section shows a list of open ports: 102, 1723, 2000, and 7547. The 'City' field is also redacted.

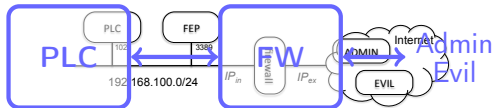


The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102

The screenshot shows a Shodan search result for the query '86.4 [redacted] wtd.eircom.net'. The search results are filtered to show ports 102, 1723, 2000, and 7547. The search results are displayed on a map of a city area, with a red pin indicating the location of the search results. The search results are listed as follows:

IP	Ports
192.168.100.24	102



Safety properties

Imagine a potato peeling ICS



Safety properties

Imagine a potato peeling ICS



Functional Requirement

$$REQ \hat{=} (get \rightarrow peel \rightarrow REQ)$$
$$\square (s7?x \rightarrow REQ)$$

Safety properties

Imagine a potato peeling ICS



Functional Requirement

$$REQ \hat{=} (get \rightarrow peel \rightarrow REQ)$$

$$\square (s7?x \rightarrow REQ)$$

Idealized Implementation

Supervision on channel s7:

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

$$POT \hat{=} (get \rightarrow peel \rightarrow POT)$$

$$\square (s7.off \rightarrow PLC)$$

Safety properties

Imagine a potato peeling ICS



Functional Requirement

$$REQ \hat{=} (get \rightarrow peel \rightarrow REQ)$$

$$\square (s7?x \rightarrow REQ)$$

Idealized Implementation

Supervision on channel s7:

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

$$POT \hat{=} (get \rightarrow peel \rightarrow POT)$$

$$\square (s7.off \rightarrow PLC)$$

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

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

Implementing requirements in the presence of an attacker

Firewall as a security control



Pass only external supervision packets from Admin

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

Deployed system includes its infrastructure

$$Deployed \hat{=} PLC \parallel FW$$

Implementing requirements in the presence of an attacker

Firewall as a security control



Pass only external supervision packets from Admin

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

Deployed system includes its infrastructure

$$Deployed \hat{=} PLC \parallel FW \parallel Evil \parallel Admin$$

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.

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

Implementation S locally refines requirement R at interface A :

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

Robust Satisfaction

$$REQ \hat{=} (get \rightarrow peel \rightarrow REQ) \square (s7?x \rightarrow REQ)$$



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

$$POT \hat{=} (get \rightarrow peel \rightarrow POT)$$

$$\square (s7.off \rightarrow PLC)$$

$$FW \hat{=} (ext?ip?op \rightarrow$$

(if ($ip = Admin$)
then $s7!op \rightarrow FW$
else FW))

Robust satisfaction in the ICS

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

Robust Satisfaction

$$REQ \hat{=} (get \rightarrow peel \rightarrow REQ) \square (s7?x \rightarrow REQ)$$



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

$$POT \hat{=} (get \rightarrow peel \rightarrow POT)$$

$$\square (s7.off \rightarrow PLC)$$

$$FW \hat{=} (ext?ip?op \rightarrow$$

(if ($ip = Admin$)
 then $s7!op \rightarrow FW$
 else FW))

Robust satisfaction in the ICS

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

Robust Satisfaction

$$REQ \hat{=} (get \rightarrow peel \rightarrow REQ) \square (s7?x \rightarrow REQ)$$



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

$$POT \hat{=} (get \rightarrow peel \rightarrow POT)$$

$$\square (s7.off \rightarrow PLC)$$

$$FW \hat{=} (ext?ip?op \rightarrow$$

(if ($ip = Admin$)

then $s7!op \rightarrow FW$

else FW))

Robust satisfaction in the ICS

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

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

Examples of robust satisfaction

Information flow

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

$$(FW \parallel STOP_{Untrusted}) \equiv_{\{s7.on, s7.off\}} FW$$

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.

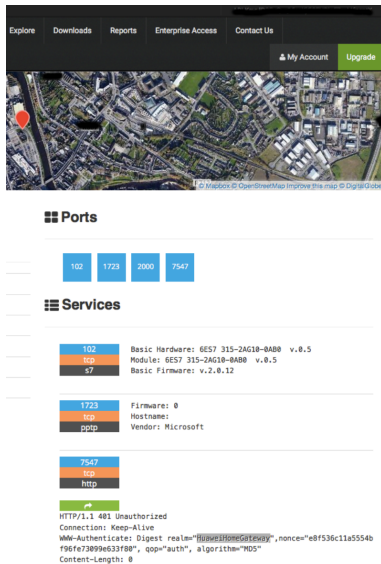
The reality of the ICS use case

Many services, many attacks, much to go wrong

S7comm on Port 102

CVE-2015-2177/Denial of service;

Preset userid/password Basisk;



The screenshot displays a network monitoring interface. At the top, there is a navigation bar with links for 'Explore', 'Downloads', 'Reports', 'Enterprise Access', and 'Contact Us'. Below this is a search bar and a 'My Account' button with an 'Upgrade' option. The main content area features a satellite map of a city with a red location pin. Below the map, there is a section titled 'Ports' with a grid of four blue buttons labeled '102', '1723', '2000', and '7547'. Underneath is a 'Services' section with a list of services. The first service is for port 102, showing 'Basic Hardware: GE57 315-2AG10-0AB0 v.0.5', 'Module: GE57 315-2AG10-0AB0 v.0.5', and 'Basic Firmware: v.2.0.12'. The second service is for port 1723, showing 'Firmware: 0', 'Hostname:', and 'Vendor: Microsoft'. The third service is for port 7547, showing 'tcp' and 'http'. Below the services list, there is a green button with a refresh icon and a text area containing the following information: 'HTTP/1.1 401 Unauthorized', 'Connection: Keep-Alive', 'WWW-Authenticate: Digest realm="Home@HomeGateway", nonce="e8f536c11a5554b f96fe73899e633f80", qop="auth", algorithm="MD5"', and 'Content-Length: 0'.

The reality of the ICS use case

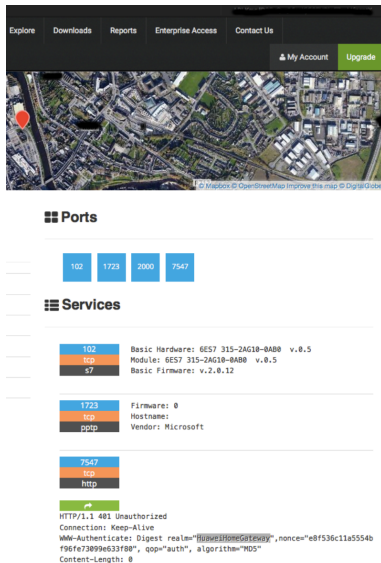
Many services, many attacks, much to go wrong

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;...



The screenshot shows a network scanner interface. At the top, there are navigation links: Explore, Downloads, Reports, Enterprise Access, and Contact Us. Below these are links for My Account and Upgrade. A map of a city is displayed, with a red location pin. Below the map, there is a section titled "Ports" with a grid of four buttons: 102, 1723, 2000, and 7547. Below the ports section, there is a section titled "Services" with a list of services. The first service is for port 102, showing details for Basic Hardware, Module, and Basic Firmware. The second service is for port 1723, showing details for Firmware, Hostname, and Vendor. The third service is for port 7547, showing details for TCP and HTTP. Below the services section, there is a section for HTTP/1.1 401 Unauthorized, showing details for Connection, WWW-Authenticate, and Content-Length.

Ports

- 102
- 1723
- 2000
- 7547

Services

- 102**
 tcp
 s7
 Basic Hardware: 6E57 315-2AG10-0AB0 v.0.5
 Module: 6E57 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="HomeHomeGateway", 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;...

The screenshot shows a network scanner interface. At the top, there are navigation links: Explore, Downloads, Reports, Enterprise Access, and Contact Us. Below these is a search bar with "My Account" and "Upgrade" buttons. The main area features a satellite map of a city with a red location pin. Below the map is a section titled "Ports" with four colored buttons: 102 (blue), 1723 (orange), 2000 (blue), and 7547 (blue). Underneath is a "Services" section with three entries:

- 102** (tcp, s7): Basic Hardware: GE57 315-2AG10-0AB0 v.0.5; Module: GE57 315-2AG10-0AB0 v.0.5; Basic Firmware: v.2.0.12
- 1723** (tcp, pptp): Firmware: 0; Hostname: ; Vendor: Microsoft
- 7547** (tcp, http):

At the bottom, there is a network log entry:

```

HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HomeHomeGateway", 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; ...

The screenshot shows a network monitoring dashboard. At the top, there are navigation links: Explore, Downloads, Reports, Enterprise Access, and Contact Us. Below these are links for 'My Account' and 'Upgrade'. A satellite map of a city is displayed, with a red location pin. Below the map, the 'Ports' section shows four colored boxes representing ports: 102 (blue), 1723 (orange), 2000 (blue), and 7547 (blue). The 'Services' section lists details for three ports:

- Port 102:** Basic Hardware: GE57 315-2AG10-0AB0 v.0.5; Module: GE57 315-2AG10-0AB0 v.0.5; Basic Firmware: v.2.0.12
- Port 1723:** Firmware: 0; Hostname: ; Vendor: Microsoft
- Port 7547:** http

At the bottom, there is a log entry for an unauthorized HTTP request:

```
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"*

The screenshot shows a network scanner interface with a map of a city at the top. Below the map, there is a section titled "Ports" with four buttons: 102, 1723, 2000, and 7547. Below that is a section titled "Services" with three entries:

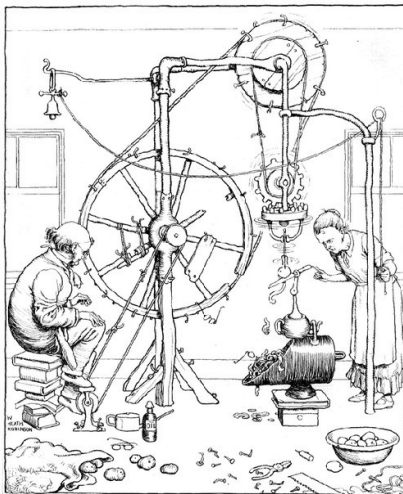
- 102**: Basic Hardware: GE57 315-2AG10-0AB0 v.0.5
tcp: Module: GE57 315-2AG10-0AB0 v.0.5
s7: Basic Firmware: v.2.0.12
- 1723**: Firmware: 0
tcp: Hostname:
pptp: Vendor: Microsoft
- 7547**: tcp: http

At the bottom, there is a status bar showing "HTTP/1.1 401 Unauthorized", "Connection: Keep-Alive", and "WWW-Authenticate: Digest realm='HuaweiHomeGateway', nonce='e8f536c11a5554b f96fe73899e633f80', qop='auth', algorithm='MD5'".

Models and reality



Models and reality



The Professor's invention for peeling potatoes.

Security Threat Management

Describing security operationally

Internal Control

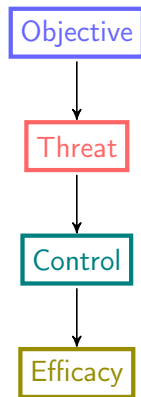
Security in terms of security controls that mitigate threats to achieving objectives.

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.



Threat management for the ICS use case

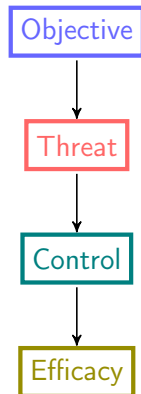
Objective: provide remote supervisory control to ICS

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

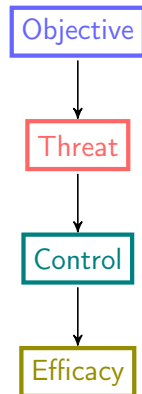
- CPNI: tunnel S7 traffic over VPN.
- Only admin IP access to VPN.
- Software update mechanism.

Efficacy: Intrusion Detection System

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

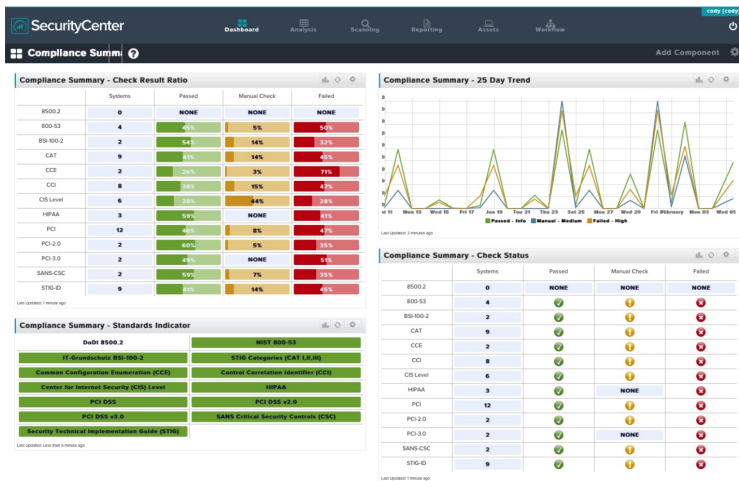
Threat: PLC is unreachable

- FAQ: open Port 102 on router



Operational security in practice

Many threats, many controls, much to go wrong



Measuring operational security

Calculating 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

Calculating 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

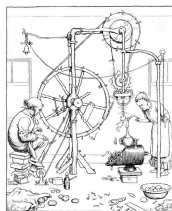
The declarative view

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



The operational view

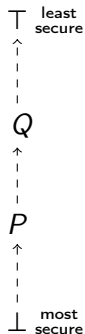
- Define security in terms of operation
- Link threats to controls based on compliance with best practices.
- Security efficacy through metrics, measuring/reporting control efficacy.



Security defined as comparison

Secure Replacement $P \sqsubseteq Q$

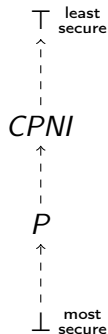
- P is no less secure than Q .
- Currently upheld objective Q can be securely replaced by objective P .



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: $P \sqsubseteq CPNI$



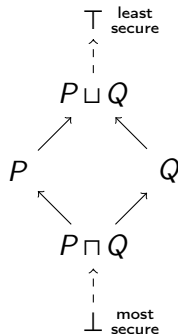
Security defined as comparison

Secure Replacement $P \sqsubseteq Q$

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

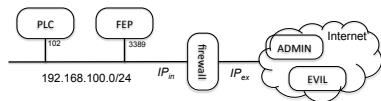
Secure Composition $P \sqcap Q, P \sqcup Q$

- 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

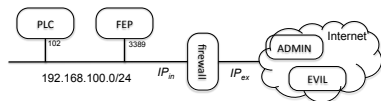
Initial policy/FAQ *UPoI*



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 *UPoI*

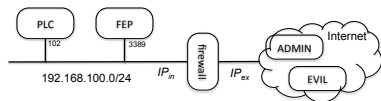


Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	plc	102	Allow
2	...	*.*.*.*	≥ 1024	fep	3389	Allow

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 *UPoI*

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

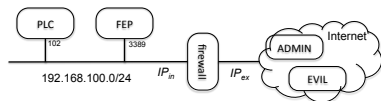
CPNI Recommendations: *CPNI*

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: *RPoI*

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

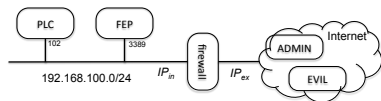
Conventional firewall policy composition



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

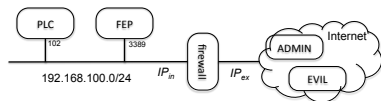
Conventional firewall policy composition



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



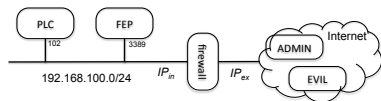
UPol;CPNI;RPol

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

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

$$Pol' = Pol \sqcap RFC5735$$

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

Convolutd 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

Convolutated 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.