

# Security in Convoluted Systems

Simon Foley

IMT Atlantique, Rennes

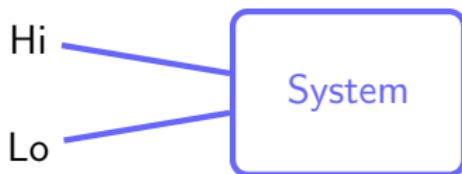
30 May, 2017



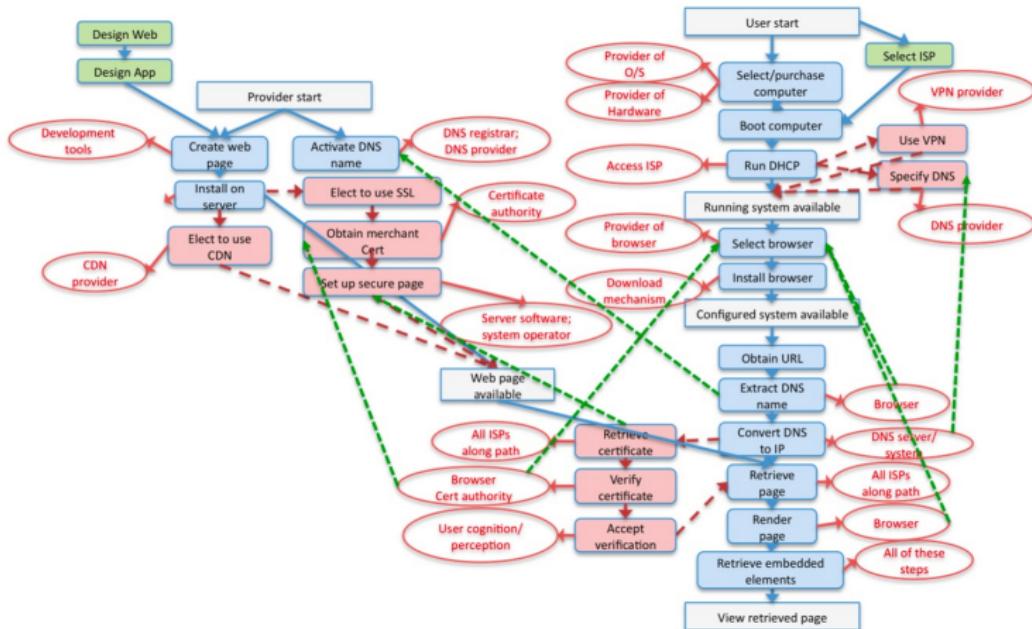
# What is meant by a secure system?

Information theoretic definitions

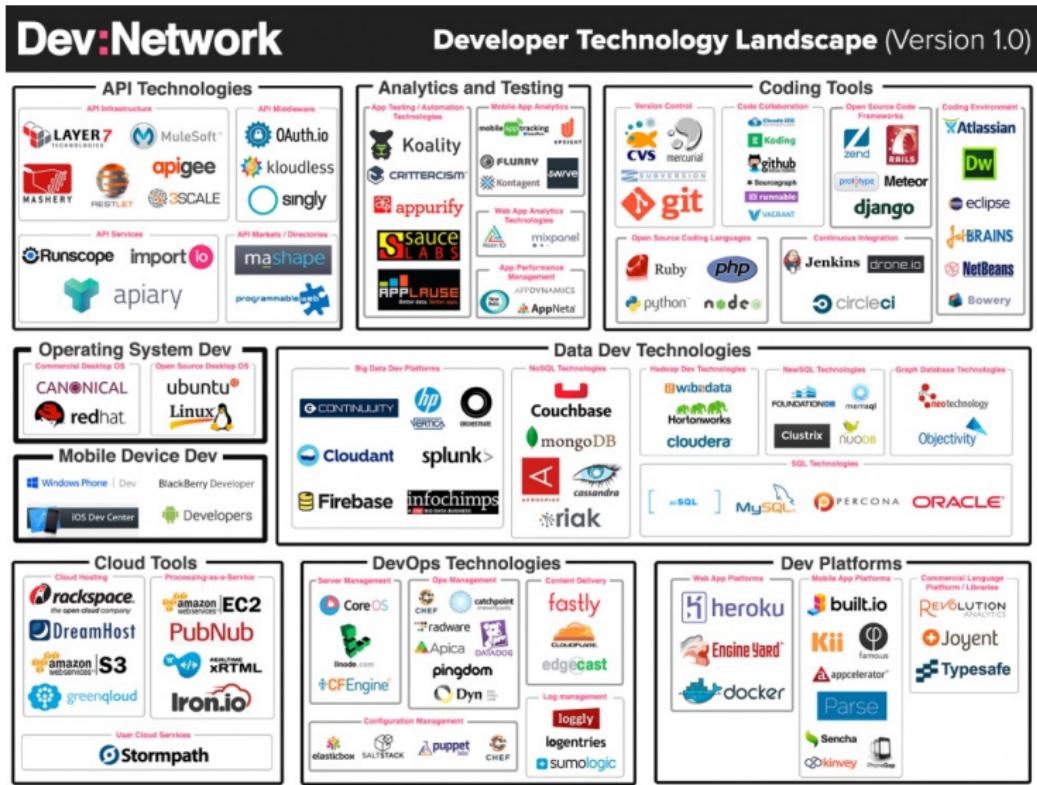
Actions at Hi interface  
do not interfere with  
actions at Lo interface



# Contemporary systems are more convoluted,



developed using frameworks like these,



Designed by DevNetwork.com - May 2014

# and built and operated by humans

**TIMES ONLINE**

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 careers 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



**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 PERINOTHE 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

Use Case

Declarative security

Operational security

Security by comparison

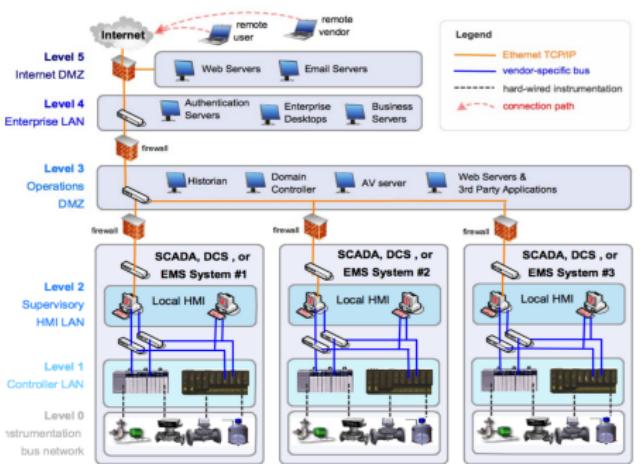
Conclusion

# 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 Developers Book View All... Show API Key

port:102

Exploits Maps Like It Download Results Create Report

TOP COUNTRIES

Country	Count
Poland	998
Germany	919
Italy	204
United States	202
Spain	238

TOP ORGANIZATIONS

Organization	Count
Deutsche Telekom AG	386
Telentia de Espana	138
Ministeren Kultury / Dziedzictwa Kultury	117
Orange Polska	94
Orange	48

**37.84.36.184**  
Deutsche Telekom AG  
Germany  
Details

**89.113.3.164**  
VimpelCom  
Russia  
Russia Federation  
Details

**81.165.25.69**  
Original Siemens Equipment  
Germany  
Germany  
Details

Copyright: Original Siemens Equipment  
PLC name: SIMATIC 300(1)  
Module type: SIMATIC 300 DP  
Hardware: 6ES7 315-4EF33-0AB0 A  
Module: 6ES7 315-4EF33-0AB0 v.0.2  
Basic Firmware: v.2.4.4  
Module name: CPU 314C-2 DP  
Serial number of module: 5 C-HOH194222087  
Plant identification:  
Basic Hardware: 6...

**217.92.140.217**  
Deutsche Telekom AG  
Germany  
Germany  
Details

Basic Hardware: 6ES7 315-2AD18-0AB0 v.0.4  
Module: 6ES7 315-2AD18-0AB0 v.0.4  
Basic Firmware: v.2.0.11

# The ICS use case

## Siemens S7comm protocol over TCP/TSAP on Port 102

The screenshot shows a SHODAN search result for a Siemens device. At the top, there's a navigation bar with links for Dashboard, Developers, News, and User API, along with a search bar, explore, download, reports, enterprise access, and contact us buttons. Below the navigation is a map showing the location of the device, with a red dot indicating its position. The main search results are displayed below the map.

**Ports**

- 102
- 1723
- 2000
- 7547

**Services**

- 102**  
Basic Hardware: E657 315-2AG1B-0AB0 v.0.5  
Module: E657 315-2AG1B-0AB0 v.0.5  
Basic Firmware: v.2.6.12
- 1723**  
Firmware: 0  
Hostname:  
Vendor: Microsoft
- 7547**  
tcp  
http

**HTTP/1.1 401 Unauthorized**

```
Connection: Keep-Alive
WWW-Authenticate: Digest realm="SiemensOneGateway",nonce="e8f536c11a5554b
f96fe73899e633fb0",qop="auth",algorithm="H05"
Content-Length: 8
```

# The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102

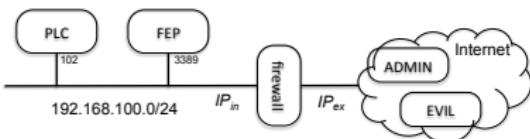
SHODAN | Developers | Book | View All... | My Account | Upgrade

86.4. [REDACTED] Ports

wtd.eirc.com.net

City [REDACTED]

102 1723 2000 7547



# The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102

The screenshot shows the SHODAN search interface. At the top, there are links for "Search", "Developers", "Book", and "View All...". The main search bar contains "SHODAN" and a magnifying glass icon. To the right of the search bar are buttons for "Explore", "Downloads", "Reports", "Enterprise Access", and "Contact Us". A "My Account" button with a gear icon and an "Upgrade" button are also present. Below the header is a map showing a location in a city area. The IP address "86.4 [REDACTED]" is displayed, along with the domain "wtd.eirc.com.net". On the right side of the map, there are buttons for "Ports": 102, 1723, 2000, and 7547. Below the map, the word "City" is followed by a redacted area. A detailed network diagram is shown at the bottom, illustrating the connection between a PLC, FEP, FW, and external networks.

**Ports**

86.4 [REDACTED]  
wtd.eirc.com.net

City [REDACTED]

102 1723 2000 7547

```
graph LR; PLC["PLC<br/>IP: 192.168.100.0/24"] <--> FEP["FEP<br/>IP: 10.0.0.1<br/>Port: 3389"]; FEP <--> FW["FW<br/>IP: IP_in<br/>IP_ex"]; FW --> Internet["Internet<br/>ADMIN<br/>EVIL"]
```

# Safety properties

Imagine a potato peeling ICS



# Safety properties

Imagine a potato peeling ICS



## Functional Requirement

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

# Safety properties

Imagine a potato peeling ICS



## Functional Requirement

$$\begin{aligned} REQ &\equiv (get \rightarrow peel \rightarrow REQ) \\ &\square (s7?x \rightarrow REQ) \end{aligned}$$

## Idealized Implementation

Supervision on channel s7:

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

$$\begin{aligned} POT &\hat{=} (get \rightarrow peel \rightarrow POT) \\ &\square (s7.off \rightarrow PLC) \end{aligned}$$

# Safety properties

Imagine a potato peeling ICS



## Functional Requirement

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

## Idealized Implementation

Supervision on channel  $s7$ :

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

$$\begin{aligned} POT &\hat{=} (get \rightarrow peel \rightarrow POT) \\ &\square (s7.off \rightarrow PLC) \end{aligned}$$

## 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

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

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.

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

Implementation  $S$  locally refines requirement  $R$  at interface  $A$ :

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

# Robust Satisfaction

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



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

$$\begin{aligned} POT \hat{=} & (get \rightarrow peel \rightarrow POT) \\ & \square (s7.off \rightarrow PLC) \end{aligned}$$

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

Robust satisfaction in the ICS

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

# Robust Satisfaction

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



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

$$\begin{aligned} POT \hat{=} & (get \rightarrow peel \rightarrow POT) \\ & \square (s7.off \rightarrow PLC) \end{aligned}$$

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

## Robust satisfaction in the ICS

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

## Robust Satisfaction

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



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

$$\begin{aligned} POT \hat{=} & (get \rightarrow peel \rightarrow POT) \\ & \square (s7.off \rightarrow PLC) \end{aligned}$$

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

### Robust satisfaction in the ICS

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

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

## Examples of robust satisfaction

### Information flow

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

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

### 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.

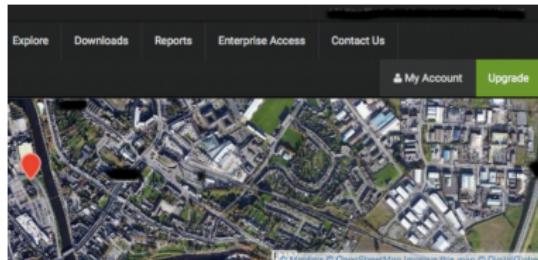
Simple trace-based definition; can have other variations.

# 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 reality of the ICS use case

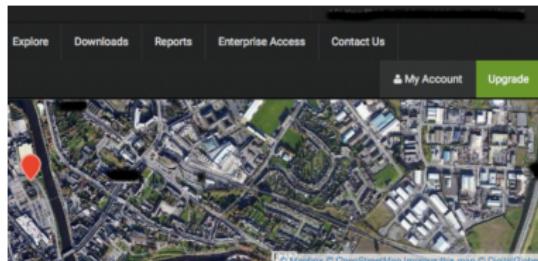
Many services, many attacks, much to go wrong

## 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 reality of the ICS use case

Many services, many attacks, much to go wrong

## S7comm on Port 102

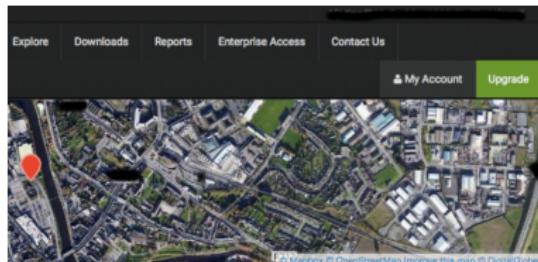
CVE-2015-2177/Denial of service;  
Preset userid/password Basisk;

## 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 Basic Hardware: 6E57 315-2AG1B-0AB0 v.0.5  
tcp Module: 6E57 315-2AG1B-0AB0 v.0.5  
57 Basic Firmware: v.2.0.12

1723 Firmware: 0  
tcp Hostname:  
ppp 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

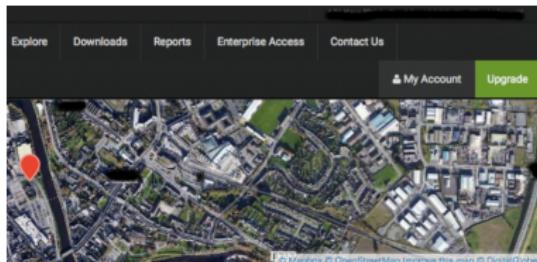
MS Security Advisory 2743314:  
MS-CHAPv2 weakness; ...

## 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 Basic Hardware: 6E57 315-2AG1B-0AB0 v.0.5  
tcp Module: 6E57 315-2AG1B-0AB0 v.0.5  
s7 Basic Firmware: v.2.0.12

1723 Firmware: 0  
tcp Hostname:  
pptp 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

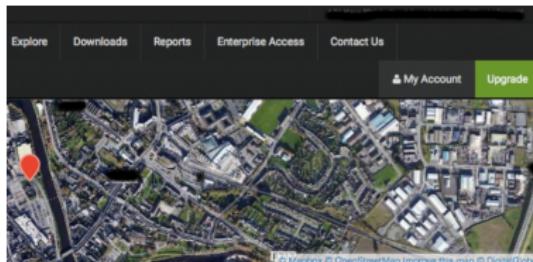
CVE-2014-9222, CVE-2014-9223:  
misfortune cookie vulnerability; ...

## Huawei home gateway

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

## Siemens FAQ8970169

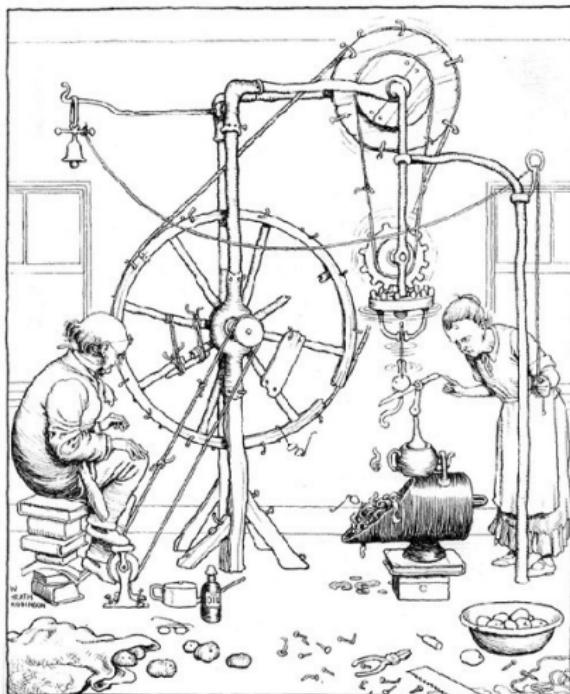
*"Port 102 [...] must be enabled for  
the complete transfer route"*



# Models and reality



# Models and reality



The Professor's invention for peeling potatoes.

# Security Threat Management

Describing security operationally

## Internal Control

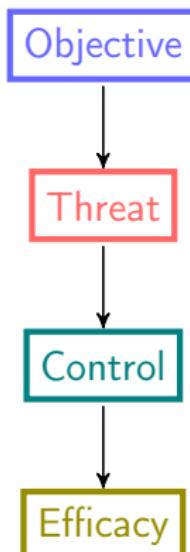
Security in terms of security controls that mitigate threats to achieving objectives.

## 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

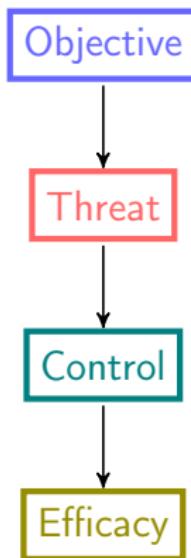
Objective: provide remote supervisory control to ICS

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

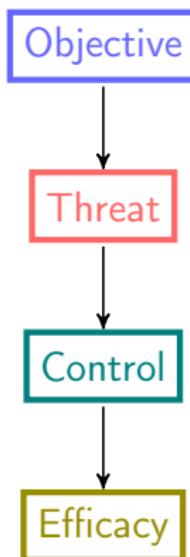
- CPNI: tunnel S7 traffic over VPN.
- Only admin IP access to VPN.
- Software update mechanism.

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

**SecurityCenter**

Dashboard Analysis Scanning Reporting Assets Workflow

Compliance Summary

Compliance Summary - Check Result Ratio

	Systems	Passed	Manual Check	Failed
8500.2	0	NONE	NONE	NONE
800-53	4	40%	5%	50%
BSI-100-2	2	54%	14%	32%
CAT	9	81%	14%	4%
CCE	2	26%	3%	71%
CCI	8	38%	15%	47%
CIS Level	6	28%	44%	28%
HIPAA	3	59%	NONE	31%
PCI	12	46%	8%	47%
PCI 2.0	2	60%	5%	35%
PCI-3.0	2	45%	NONE	55%
SANS-CSC	2	59%	7%	35%
STIG-ID	9	81%	14%	4%

Last Updated 1 minute ago

Compliance Summary - 25 Day Trend

Compliance Summary - Check Status

	Systems	Passed	Manual Check	Failed
8500.2	0	NONE	NONE	NONE
800-53	4	🟡	🟡	🔴
BSI-100-2	2	🟡	🟡	🔴
CAT	9	🟡	🟡	🔴
CCE	2	🟡	🟡	🔴
CCI	8	🟡	🟡	🔴
CIS Level	6	🟡	🟡	🔴
HIPAA	3	🟡	NONE	🔴
PCI	12	🟡	🟡	🔴
PCI 2.0	2	🟡	🟡	🔴
PCI-3.0	2	🟡	NONE	🔴
SANS-CSC	2	🟡	🟡	🔴
STIG-ID	9	🟡	🟡	🔴

Last Updated 1 minute ago

Compliance Summary - Standards Indicator

DeDI 8500.2	NIST 800-53
IT-Grundschutz BSI-100-2	STIG Categories (CAT I,II,III)
Common Configuration Enumeration (CCE)	Control Correlation Identifier (CCI)
Center for Internet Security (CIS) Level	HIPAA
PCI DSS	PCI DSS v2.0
PCI DSS v3.0	SANS Critical Security Controls (CSC)
Security Technical Implementation Guide (STIG)	

Last Updated Less than a minute ago

# 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

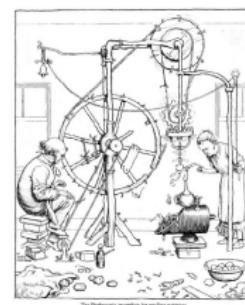
## The declarative view

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



## The operational view

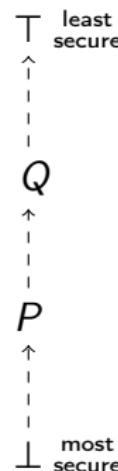
- Define security in terms of operation
- Link threats to controls based on compliance with best practices.
- Security efficacy through metrics, measuring/reporting control efficacy.



# Security defined as comparison

## Secure Replacement $P \sqsubseteq Q$

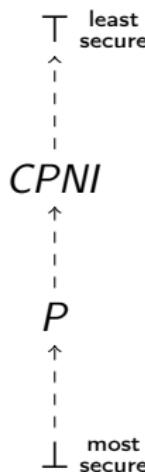
- $P$  is no less secure than  $Q$ .
- Currently upheld objective  $Q$  can be securely replaced by objective  $P$ .



# 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:  $P \sqsubseteq CPNI$



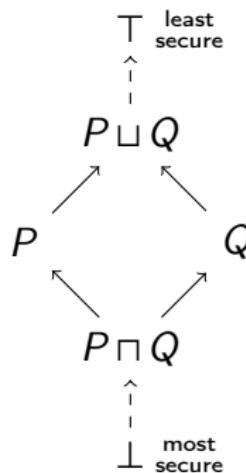
# Security defined as comparison

## Secure Replacement $P \sqsubseteq Q$

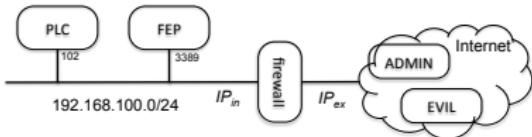
- $P$  is no less secure than  $Q$ .
- Currently upheld objective  $Q$  can be securely replaced by objective  $P$ .
- Compliance:  $P \sqsubseteq CPNI$

## 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  $P \sqcap (CPNI \sqcup RFC5735)$



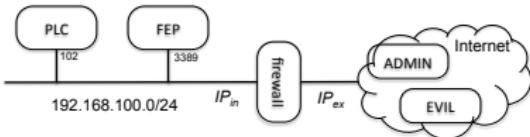
# Objectives as firewall policies



## 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



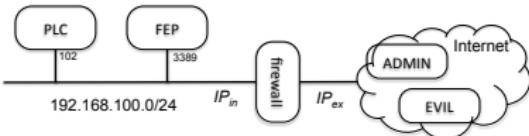
## Initial policy/FAQ UPoL

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

## CPNI Recommendations: CPNI

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

# Objectives as firewall policies



## Initial policy/FAQ *UPol*

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

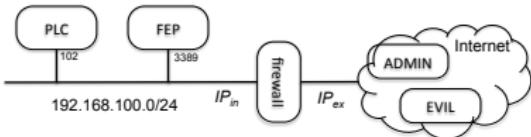
## CPNI Recommendations: *CPNI*

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

## Remote Desktop Policy: *RPol*

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

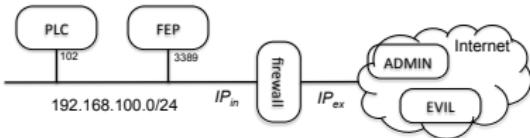
# Conventional firewall policy composition



*UPol;CPNI;RPol*

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

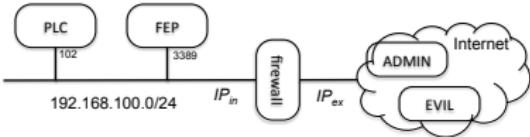
# Conventional firewall policy composition



*UPol;CPNI;RPol*

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

# Conventional firewall policy composition



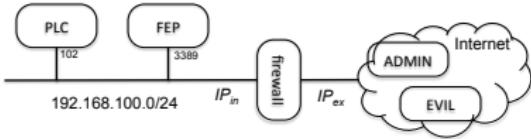
*UPol;CPNI;RPol*

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	...	*.*.*.*	$\geq 1024$	plc	102	Allow
2	...	*.*.*.*	$\geq 1024$	fep	3389	Allow
3	...	192.168.100.0/24	$\geq 1024$	plc	102	Allow
4	...	*.*.*.*	*	plc	102	Drop
5	...	external	$\geq 1024$	fep	3389	Allow
6	...	admin	$\geq 1024$	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	$\geq 1024$	plc	102	Allow
2	...	*.*.*.*	*	plc	102	Drop
3	...	external	$\geq 1024$	fep	3389	Allow
4	...	admin	$\geq 1024$	fep	3389	Allow
5	...	*.*.*.*	*	fep	3389	Drop
6	...	*.*.*.*	$\geq 1024$	plc	102	Allow
7	...	*.*.*.*	$\geq 1024$	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  $P, Q : Policy$ :

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

### 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

## Convolved 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

## Convolved 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.