Getting security objectives wrong
A cautionary tale of an Industrial Control System

Simon N. Foley

IMT Atlantique, LabSTICC,
Université Bretagne Loire, France.
simon.foley@imt-atlantique.fr

Abstract. We relate a story about an Industrial Control System in order to illustrate that simple security objectives can be deceptive: there are many things that can and do go wrong when deploying the system. Rather than trying to define security explicitly, this paper takes the position that one should consider the security of a system by comparing it against others whose security we consider to be acceptable: Alice is satisfied if her system is no less secure than Bob's system.

1 Introduction

Contemporary systems are convoluted arrangements of frameworks, software stacks, services and third party components. It is in this complexity, that mistakes are made and that security threats emerge. Despite our best efforts, we continue to have difficulty accurately capturing security objectives, identifying threats and implementing and configuring the security mechanisms that mitigate the threats. The history of the definition of information flow security style properties is a case in point: in the course of forty years of research [5, 12, 18, 21, 22], there has been much debate over its meaning and how it might be used in practice. If there can be such variations over what appears to be a conceptually simple security objective—preventing high information from flowing down to low—then what hope have we of providing a meaning for security in a convoluted enterprise system, scalability notwithstanding?

Security practitioners have tended to take a more operational approach to dealing with security in convoluted systems. Rather than attempting to provide a declarative meaning for security, security objectives are defined operationally. Threats are identified and operational controls are used to mitigate those threats, usually according to some notion of best practice. Thus, for instance, the network administrator does not define the meaning of security of an N-tier enterprise network in a declarative sense, rather, the security of the system is defined in terms of its operation: by organising the enterprise network in tiers, the innermost subnet hosts critical data, following best practices, and so forth.

Security Risk/Threat Management [9,17,25] is an example of this operational approach to security, and, while it may scale to convoluted systems, it is in itself convoluted and error-prone. Standards and best practices may help an administrator to identify security risks and to deploy defences, however their extensive

catalogues encourage a focus on checkbox-style security compliance, rather than security outcomes. At the extreme, approaches such as the Security Content Automation Protocol (SCAP) family of standards [26] champion catalogues with a tremendous amount of detail, leading to challenges in comprehension. For example, the scope for inconsistencies within and between OVAL, CPE, CVE and CCE repositories in SCAP are considered in [6].

Rather than attempting to define security objectives declaratively or operationally, this paper takes the position that one should consider the security of a system by comparing it against others whose security we consider to be acceptable. This is characterised as a refinement relation between systems: Alice is satisfied if her system is no less secure than Bob's system, or, if Alice makes a change to her system configuration then it should be no less secure than her previous configuration. For consistency, one would expect this ordering relation to form a partial order, with the properties of reflexivity, anti-symmetry and transitivity. If it can be shown than the refinement relation also forms a lattice then its greatest lower, and lowest upper bound, operators provide useful forms of composition. If Alice is happy when her system is no less secure than Bob's system and no less secure than Clare's system then the lattice join operator ensures Alice has the best possible secure replacement.

In this paper we do not attempt to put forward a general refinement relation (other than it should form a lattice), nor suggest what is meant by a system or security objectives. Rather, we suggest that one should use the notion of refinement as a strategy when considering convoluted systems, or protocols, that have multiple security objectives. This strategy of defining security in terms of comparison has been previously considered for mandatory access control policies [7,10] and formal security properties [8,16]. It is revisited in this paper, where we consider how it might be used in a broader and less-formal setting as a potential approach to dealing with convoluted systems.

This challenges of capturing the full meaning of security in a convoluted system is illustrated in the paper using a ethnographic style study of the connection of an Industrial Control System to the Internet. Shodan.io was used to locate what appeared to be a vulnerable ICS connected to the Internet; the apparent operators of the system were contacted, the vulnerability highlighted and remediation suggested. No further contact was made and Shodan.io was used to track subsequent changes between March 2016 and March 2017. At face value, securing this ICS infrastructure connection should be trivial in terms of network security objectives. However, in our use case we see that there are many objectives to be understood and met, some of which can be contradictory, others are out of the operator's control, and mistakes are made. Focussing on just the firewall aspects of the system, we illustrate how thinking about the security in terms of refinement may provide a means to deal with this convolution.

2 A convoluted system use case

Despite the widespread availability of information on how to defend against infrastructure threats, security can be overlooked or misunderstood when Industrial Control Systems are connected to the Internet. For instance, the UK Centre for the Protection of National Infrastructure (CPNI) recommends that the control network should not be accessible from the public network. Siemen's S7comm protocol runs over Port 102 and is used for supervisory communications in SCADA systems. When we began this work a Shodan search found a large number of systems with Port 102 open to the Internet, that is, they appeared not to follow best security practice. In this section we explore one such case: a Siemens SIMATIC S7-300 universal controller that was believed to be used by a public organisation, as depicted in Figure 1.

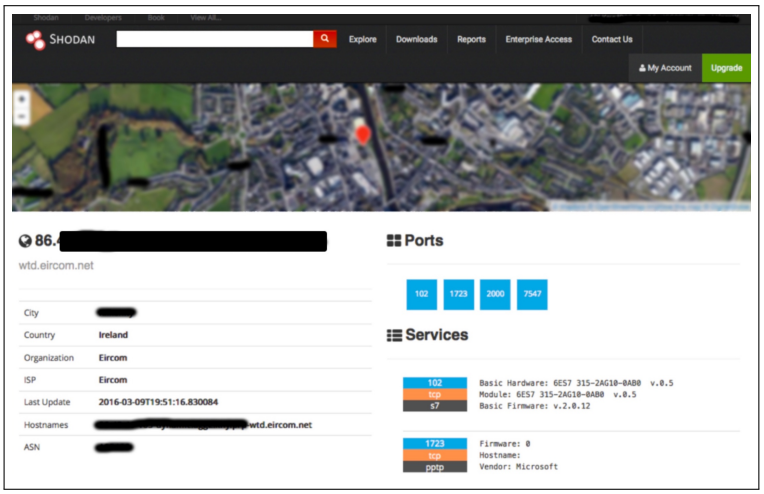

Fig. 1. Shodan report on an Internet connected S7 Service.

Based on CPNI best practice [2, 3] the controller and PLCs should be deployed on an internal control network and a VPN tunnel used when accessing the controller over the Internet/public network. The service should not be directly accessible over a public network. In the following discussion we *speculate* on the threats to which this system might be exposed, based on the information provided by Shodan, vulnerability repositories, and other information in the public domain. Our purpose here is to illustrate the convoluted nature of the system and the security objectives. No attempt was made to access the system nor test our speculation.

CPE. An Internet connection is provided via a commercial ISP. Based on the headers (Figure 1), the Customer Premise Equipment (CPE)/gateway router appears to be a Huawei Home Gateway.

It is not immediately evident which particular model is used, however various vulnerabilities have been reported against numerous Huawei Home Gateway models. For example, CVE-2015-7254 (CVSS 5.0) reports *"Directory traversal vulnerability on Huawei HG532e, HG532n, and HG532s devices allows remote attackers to read arbitrary files via a .. (dot dot) in an icon/ URI"*. Huawei routers use the Allegrosoft embedded webserver, which, for example, has had reported buffer overflow vulnerabilities CVE-2014-9223 (CVSS 10.0) and cross-site scripting vulnerabilities CVE-2013-6786 (CVSS 4.3). Huawei [13] reason that backdoor password vulnerabilities on older Home Gateway models can be mitigated by replacement/identifying them as being at *"End of Service"*.

CWMP. The gateway router is deployed with the CPE WAN Management Protocol (CWMP) running on TCP/HTTP at Port 7547 of the router. CWMP provides communication between the router and the ISP and supports auto-configuration and management of the router by the ISP.

Running on HTTP, means that the router may be vulnerable to a misfortune cookie attack (CVE-2014-9222,CVE-2014-9223) [4], among others. This vulnerability is a consequence of an HTTP cookie mechanism that allows an attacker to forge session cookies so that its session has administrator privileges. A number of Huawei Home Gateway routers are vulnerable [29] which can be mitigated via a firmware update. However, we note that the installation relies on HTTP digest authentication, which is not generally advised: a remarkable number of routers run CWMP over an unencrypted connection and that an authenticated HTTPS connection would be more appropriate [4], although this is something over which the user has little control.

VPN connection. VPN access to the local Control Network appears to be provided via PPTP on Port 1723.

A variety of security vulnerabilities related to using the PPTP protocol have been published over the years [19, 23]. Rather than using PPTP, it is suggested, for example, to use OpenVPN or IPSec in certificate mode [19].

Control Network. Access to a SCADA/PLC controller uses the S7comm protocol over TCP/TSAP on Port 102, possibly intended via the VPN service.

While this may be the intended configuration, Port 102 remains open to the Internet, meaning that the controller is directly accessible via the S7Comm protocol from the Internet. This does not follow best practice recommendations [2,3], although the (subsequently removed) Siemens FAQ [24] at the time of the study could be misinterpreted when it noted that

> *"[...] if the data is transferred over routers or if firewalls are used, the port must be enabled in the router or firewall according to the service implemented"* and recommends that *"Port 102 is blocked by default*

in routers and firewalls and must be enabled for the complete transfer route". [...]

CVE-2015-2177 notes that versions of the SIMATIC S7-300 is vulnerable to a denial of service attack via this protocol as described by Beresford [1], who also discovered a hardcoded user-id/password (`'Basisk'`) used to access internal diagnostic functions [14]. Based on the header information provided by Shodan, we conclude that the SIMATIC S7-300 is a 315-2DP CPU, running firmware V2.6, which has this vulnerability [14]. Our speculation here is that in setting up VPN access, closing direct access to the S7 service via Port 102 was overlooked in the firewall/CPE settings.

Web servers. Its not evident from the network footprint, nor the documentation, that the SCADA system in the use case incorporates an embedded web-server. Embedded web-servers are supported by some SCADA devices and are used to serve up SCADA administration panels.

An example of an embedded web server is GoAhead. Various vulnerabilities have been published for the GoAhead server, including an application-level (Slow Loris) denial of service attack (CVE-2009-511) and a directory path traversal (CVE-2014-9707). While a software update is recommended to mitigate the directory path traversal vulnerability, it is also suggested that a larger `ulimit` helps defend against the Slow Loris attack. However, this latter recommendation is an example of the need for a trade off, as a larger `ulimit` may make the hosting system vulnerable to a fork-bomb attack.

Changing configurations. Based on the geographic location of the system as reported by Shodan (Figure 1), the (likely) Director of IT responsible for the system was informally contacted by email in March 2016. The mis-configuration of the S7/VPN and its vulnerabilities were hi-lighted and remediation by blocking Internet access to Port 102 suggested, with reference to the CPNI Best Practices [2, 3]. Receipt of the email was acknowledged, with a response that it would be investigated. No further contact was made and Shodan was used to track subsequent changes between March 2016 and March 2017.

- March 2016. Shortly after sending the email, the configuration changed with the addition of Microsoft Remote Desktop Protocol on Port 3389, however Port 102 remained open.
- May 2016. The system and all services disappeared from Shodan. This might indicate that the system was successfully configured and VPN access concealed. However, we speculate that all services, including Port 102, were blocked from the Internet, since it re-appeared the following month.
- June 2016. The system re-appeared, this time with Port 102 (S7), Port 3389 (RDP) and Port 7547 (CWMP) open.
- October 2016. Port 102 was closed, however Port 3389 (RDP) was discoverable, displaying a Windows login with a specific user-id and prompting for a password.

– December 2016. The system and all services disappeared from Shodan. At the time, the hope was that Port 3389 (RDP) was successfully concealed, however in
– March 2017, the system re-appeared, this time with Port 2000 discoverable with a "RemotelyAnywhere" login prompt that was available over HTTPS.

3 What is the likely setup behind the scenes?

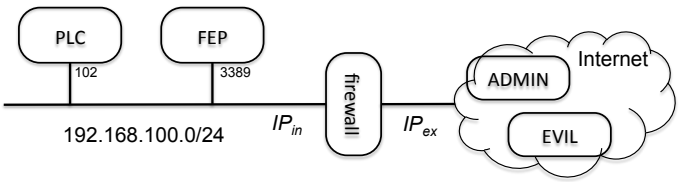

Fig. 2. A network connected ICS

The use case is intended to illustrate the convoluted nature of a contemporary system and how easily mistakes are made in achieving security objectives. Informed by this, we give a simplified interpretation of how deploying the VPN went wrong. The configuration is depicted in Figure 2 where a PLC/controller (Port 102) and Front End Processor FEP (Port 3389) are on an internal network, behind a firewall. Access is required by the external enterprise/administrator (ADMIN), but the attacker (EVIL) should not have access.

Policy UPol. In the initial configuration, following Siemens FAQ8970169 *"Port 102 is blocked by default in routers and firewalls and must be enabled for the complete transfer route"*, and naively setting up a VPN, gives rise to the following firewall policy.

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
2	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW

For ease of presentation we assume that RDP provides the VPN from the outset.

Policy CPNI. CPNI recommendation *"SCADA communications should be encrypted and routed through a VPN tunnel through corporate IT or other non-critical networks"* is implemented as the policy:

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
2	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW

Policy RPol. Access to the VPN should be limited to authorised IPs:

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	ADMIN	≥ 1024	FEP	3389	ALLOW
2	...	*.*.*.*	*	FEP	3389	DROP

Composition I. A common strategy for managing firewall policies is to compose policies in sequence. On understanding that policy *CPNI* must be enforced, we speculate that the policy was revised as (*UPol* ; *CPNI*) and then further extended to (*UPol* ; *CPNI* ; *RPol*) in order to limit RDP access (Table 1). The resulting anomalies whereby *CPNI* and *Rpol* are shadowed/redundant by *UPol* mean that we do not achieve the *CPNI* nor *RPol* objectives.

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

Table 1. Composition *UPol* ; *CPNI* ; *RPol*

Composition II. Having realised the mistake, the administrator revises the policy to enforce the *CPNI* policy objectives first, followed by the remaining policy, that is, *CPNI* ; *RPol* ; *UPol* (Table 2). However, while blocking Port 102, there is an anomaly between Rules 2 and 4, which means that the RDP objective that only ADMIN should have access to the FEP is not enforced.

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

Table 2. *CPNI* ; *RPol* ; *UPol*

Composition III. The administrator tries another re-arrangement of the policy as *RPol* ; *CPNI* ; *UPol* (Table 3) which happens to be anomaly-free and meets our objectives. However, re-arranging policies in this ad-hoc manner so that they are anomaly-free does not necessarily always achieve our objectives, especially when policies may run to a large number of rules.

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	ADMIN	≥ 1024	FEP	3389	ALLOW
2	...	*.*.*.*	*	FEP	3389	DROP
3	...	192.168.100.0/24	≥ 1024	PLC	102	ALLOW
4	...	*.*.*.*	*	PLC	102	DROP
5	...	external	≥ 1024	FEP	3389	ALLOW
6	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
7	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW

Table 3. Composition *RPol* ; *CPNI* ; *UPol*

4 Comparing configurations

4.1 Refining firewall policies

In the following we use a refinement relation for firewall policies that is a simplification of the more general iptables firewall algebra described in [11, 20]. In particular, packets are modelled in terms of source and destination IP addresses and Ports:

$$Packet == IP \times PORT \times IP \times PORT$$

where (ip_s, p_s, ip_d, p_d) denotes a packet from source IP ip_s, source port p_s, with destination IP ip_d and destination port p_d. A firewall policy $P : Policy$ defines a set of packets $accepts(P)$ that are accepted and a set of packets $denies(P)$ that are denied/dropped. We have

$$Policy == \{Accepts, Denies : \mathbb{P}\, Packet \mid Accepts \cap Denies = \emptyset\}$$

and we assume a default deny for packets not referenced by P. This is a very simple representation of an anomaly-free policy that is adequate for our purposes; our discussion here can be extended to the more general firewall algebra [20] that supports iptables policies with IP and port ranges, and numerous other attributes. Two types of constructor provide a simple policy notation.

Weak allow/deny. Packets not in $X : \mathbb{P}\, Packet$ are default deny:

$$\mathsf{Allow}\, X = (X, \emptyset); \qquad \mathsf{Deny}\, X = (\emptyset, X)$$

For example, permit S7 traffic from the internal network (IP_{in}) to the PLC:

$$\mathsf{Allow}(IP_{in} \times PORT \times \{\text{PLC}\} \times \{102\})$$

Strong allow/deny. Packets not mentioned in X are explicitly denied/accepted:

$$\mathsf{Allow}^+\, X = (X, Packet \setminus X); \qquad \mathsf{Deny}^+\, X = (Packet \setminus X, X)$$

For example, block external S7 traffic to PLC, everything else permitted:

$$\mathsf{Deny}^+(IP_{ex} \times PORT \times \{\text{PLC}\} \times \{102\})$$

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

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

The most restrictive policy is $\bot == (\emptyset, Packet)$ and the least restrictive policy is $\top == (Packet, \emptyset)$ and we have $\bot \sqsubseteq P \sqsubseteq \top$ for any policy P.

Policy intersection and union. The least restrictive safe replacement for P and Q is $P \sqcap Q$, where

$$P \sqcap Q == (accepts(P) \cap accepts(Q), denies(P) \cup denies(Q))$$

The most restrictive policy that can be safely replaced by P or Q is $P \sqcup Q$:

$$P \sqcup Q == (accepts(P) \cup accepts(Q), denies(P) \cap denies(Q))$$

The set *Policy* is a lattice under partial order $\sqsubseteq$, greatest lower bound operator $\sqcap$, and lowest upper bound operator $\sqcup$ [11, 20]. Figure 3 gives an example of some policy orderings.

4.2 Comparing the ICS firewalls

CPNI recommendation. The CPNI objective specifies that internal S7 traffic to the PLC is permitted while external traffic should be blocked but no constraints on other external traffic.

$$\begin{aligned} CPNI == {} & \mathsf{Allow}(IP_{in} \times PORT \times \{\text{PLC}\} \times \{102\}) \\ & \sqcap \mathsf{Deny}^+(IP_{ex} \times PORT \times \{\text{PLC}\} \times \{102\}) \end{aligned}$$

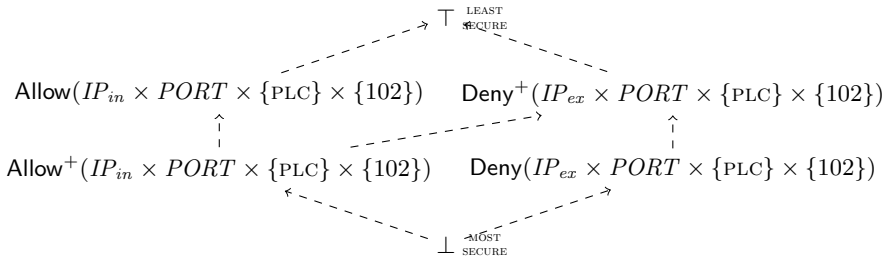

Fig. 3. Some policy orderings

Remote Desktop recommendation. The RDP objective permits administrator VPN access to the Front end processor, and to deny all other traffic.

$$\begin{aligned} RDP == \mathsf{Allow}(\{\text{ADMIN}\} \times PORT \times \{\text{FEP}\} \times \{3389\}) \\ \sqcap \mathsf{Deny}^{+}(IP_{ex} \times PORT \times \{\text{FEP}\} \times \{3389\}) \end{aligned}$$

For any packet the *CPNI* or *RDP* policy should apply. Therefore, if the initial policy was *Pol*, then changing it to incorporate CPNI on a RDP based VPN gives:

$$Pol' == Pol \sqcap (CPNI \sqcup RDP)$$

and since $(Policy, \sqsubseteq)$ forms a lattice the administrator can be sure that the new policy Pol' a safe replacement of the original policy, and the new security objectives. Furthermore, it is the best secure replacement under $\sqsubseteq$.

5 Conclusion

In the spirit of Jackson [15] we have related a story about an Industrial Control System in order to illustrate that simple security objectives can be deceptive: there are many things that can and do go wrong when deploying the system. We suggest that rather than tying to reason about the security objectives explicitly, we capture them indirectly by comparison in the form of a refinement relation. In developing this idea, we limit ourselves in this paper to just firewall policies which is a homogenous collection of objectives.

We believe that this strategy of defining security by comparison can be extended to heterogenous objectives and we are currently exploring how other, non-firewall, aspects of the ICS use case can be incorporated into the refinement relation. In doing this, one must be mindful to ensure that the composition of the underlying security mechanisms is consistent/preserves the composition of the respective objectives that they uphold [27]. Additionally, while the use-case helps to illustrate the difficulty in securing convoluted systems, and, we believe, provides a convincing technical argument, research is required to establish whether the proposed strategy of security through comparison is conducive to a more user-centered approach [28] to security.

Acknowledgement. This research was supported in part by the CHIST-ERA project *DYPOSIT: Dynamic Policies for Shared Cyber-Physical Infrastructures under Attack* and by the Cyber CNI Chair of Institute Mines-Télécom which is held by IMT Atlantique and supported by Airbus Defence and Space, Amossys, EDF, Orange, La Poste, Nokia, Société Générale and the Regional Council of Brittany; the Chair is recognized by the French Centre of Excellence in Cybersecurity.

References

1. Beresford, D.: Exploiting Siemens SIMATIC S7 PLCs. In: Black Hat (2011)
2. Center for the Protection of National Infrastructure: Firewall deployment for SCADA and process control networks. Guide (2005)
3. Center for the Protection of National Infrastructure: Securing the move to IP-based SCADA/PLC networks. Guide (November 2011)
4. Checkpoint Software Technologies: Protecting against misfortune cookie and TR-069 vulnerabilities. Web page http://mis.fortunecook.ie/ (2014)
5. Cohen, E.: Information transmission in sequential programs. In: DeMillo, R., et al. (eds.) Foundations of Secure Computation. Academic Press (1978)
6. Fitzgerald, W.M., Foley, S.N.: Avoiding inconsistencies in the Security Content Automation Protocol. In: Proc. 6th Symposium on Security Analytics and Automation. IEEE (2013)
7. Foley, S.N.: A model for secure information flow. In: IEEE Symposium on Security and Privacy. Oakland, CA (May 1989)
8. Foley, S.N.: A non-functional approach to system integrity. IEEE Journal on Selected Areas in Communications 21(1) (Jan 2003)
9. Foley, S.N.: Security risk management using internal controls. In: ACM CCS Workshop on Information Security Governance (2009)
10. Foley, S.N.: The specification and implementation of commercial security requirements including dynamic segregation of duties. In: CCS '97, Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 1-4, 1997. pp. 125–134 (1997)
11. Foley, S.N., Neville, U.: A firewall algebra for openstack. In: 2015 IEEE Conference on Communications and Network Security, CNS 2015, Florence, Italy, September 28-30, 2015. pp. 541–549 (2015)
12. Goguen, J.A., Meseguer, J.: Security policies and security models. In: Proceedings 1982 IEEE Symposium on Security and Privacy. pp. 11–20. IEEE Computer Society (1982)
13. Huawei: Security notice - statement on password disclosure/change vulnerability in huawei home gateway products. URL http://www.huawei.com/en/psirt/security-notices/hw-443302 (2015)
14. ICS-ALERT-11-204-01-A: SIEMENS S7-300 hardcoded credential (2011)
15. Jackson, M.: Getting it wrong: A cautionary tale. In: Cameron, J. (ed.) JSP & JSD: The Jackson Approach to Software Development;. IEEE CS Press (1989)
16. Jacob, J.: Security specifications. In: Proceedings 1988 IEEE Symposium on Security and Privacy. pp. 14–23. IEEE Computer Society Press, New York, NY (Apr 1988)
17. Johnson, M., Goetz, E., Pfleeger, S.: Security through information risk management. Security & Privacy, IEEE 7(3), 45–52 (2009)

18. Mantel, H.: Information flow and noninterference. In: Encyclopedia of Cryptography and Security (2nd Ed.), pp. 605–607. Springer (2011)
19. Marlinspike, M.: Divide and conquer: Cracking MS-CHAPv2 with a 100% success rate. In: DefCON 20 (2012)
20. Neville, U., Foley, S.N.: A firewall algebra. In: IFIP Working conference on data and application security (DBSEC). Springer Verlag (2016)
21. Ryan, P.: Mathematical models of computer security. In: Focardi, R., Gorrieri, R. (eds.) Foundations of Security Analysis and Design, Lecture Notes in Computer Science, vol. 2171, pp. 1–62. Springer, Berlin, Heidelberg (2001)
22. Schneider, F.B.: Enforceable security policies. ACM Trans. Inf. Syst. Secur. 3(1), 30–50 (Feb 2000), http://doi.acm.org/10.1145/353323.353382
23. Schneier, B., Mudge, Wagner, D.: Cryptanalysis of microsoft's PPTP authentication extensions (MS-CHAPv2). In: Proceedings of the International Exhibition and Congress on Secure Networking (1999)
24. Siemens: FAQ: Which ports are used by the various services for data transfer by means of TCP and UDP and what should you watch out for when using routers and firewalls? Frequently Asked Question 8970169 (2012, retrieved 1/3/2017 (subsequently removed)), https://support.industry.siemens.com/cs/document/8970169/which-ports-are-used-by-the-various-services-for-data-transfer-by-means-of-tcp-and-udp-and-what-should-you-watch-out-for-when-using-routers-and-firewalls?dti=0&lc=en-WW
25. Stoneburner, G., Goguen, A.Y., Feringa, A.: SP 800-30: Risk management guide for information technology systems. Tech. rep., National Institute of Standards & Technology, Gaithersburg, MD, United States (2002)
26. Waltermire, D., Quinn, S., Scarfone, K., Halbardier, A.: The Technical Specification for the Security Content Automation Protocol: SCAP Version 1.2. Recommendations of the National Institute of Standards and Technology, NIST-800-126 (September 2011)
27. Zhou, Z., Yu, M., Gligor, V.D.: Dancing with giants: Wimpy kernels for on-demand isolated I/O. In: 2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014. pp. 308–323 (2014)
28. Zurko, M.E., Simon, R.T.: User-centered security. In: Proceedings of the 1996 Workshop on New Security Paradigms. pp. 27–33. ACM Press (1996), http://doi.acm.org/10.1145/304851.304859
29. Zyxel: Guard against "misfortune cookie" vulnerability. Web page http://www.zyxel.com/support/announcement_misfortune_cookie_vulnerability.shtml