Universiteit Twente - EIT Digital

Economics of Cybersecurity

Course Project Report

The Effect of Patch Management on Cybersecurity - An Economical Perspective

---

Authors:
Vincent Rocher-Monnier
Diego Sainz
Uraz Seddigh
Ikram Ullah

Lecturers:
Michel van Eeten
Carlos H. Gañán

October 12, 2015

Abstract

Devices such as routers, or SCADA systems, are the target of cyber attacks everyday. The most famous and common attack is named Denial of Service (DoS). This type of attack causes a lack of productivity, that is an important issue in the industry and companies, resulting in major financial losses. Avoiding DoS attacks is an important goal and a serious challenge at the same time. That is why, in this report, we propose a set of metrics in order to find the link between the patch management of hardware device firmware and the exposed attack surface. Finally, we focus on identifying the actors that play a role in this particular security problem, as well as strategies to be followed by them.

Contents

1 Introduction

The assignment involves gathering datasets on security vulnerabilities and relevant metadata, to be able to produce realistic, or unrealistic, i.e. ideal, metrics over the dataset. The goal is to be able to methodically use the gathered data in security related decision making and risk mitigation.

Our approach involves the on-line metadata search engine, Shodan, as well as vulnerability databases, National Vulnerability Database (NVD) and CVE Details. Other useful resources will also be used if necessary. During the study, we have looked into specific categories of on-line devices, namely Routers and SCADA systems. At the same time, on the aspect of vulnerabilities, our focus was Denial of Service attacks (DoS).

From an economic perspective, any successful DoS attack has a financial impact because of the lost productivity and lost resources. This is the least effect. Depending on the operational importance of the device under attack, DoS has hefty consequences. Consider SCADA systems running the industry and infrastructure of a country coming under attack and becoming unresponsive. The effects can be considered as boldly as, *strategically destabilising*.

The reason we focus on DoS is the fact that, these attacks are much more feasible for the perpetrator and for this exact reason, we can see a high percentage of associated vulnerabilities for these systems are categorised as DoS. Just as an example, if you search for known vulnerabilities for Siemens SIMATIC S7 (a type of industrial control hardware) in NVD, 14 out of 26 listed vulnerabilities are of the type DoS. The number of DoS vulnerabilities are 12 out of 24 for VxWorks, the most widely deployed realtime embedded operating system in industrial setups.

Routers on the other hand, might not be considered as strategic as industrial systems, but given the sheer number of installed devices, any vulnerability provides a vast attack surface. Concerning D-Link routers as an example, 17.3% of attacks are DoS, which is in the top 3 of the most common attacks against D-Link routers since 2001.

As you can imagine, one of the main priorities of any organisation, big or small, should be the development of risk mitigation strategies against such threats. I this report, we will see how this development process is affected by different factors such as the nature of the organisation in relation with the threat, or operational attributes and goals. These can be the amount of risk to be mitigated, consistency of attacks, or the exposure cost.

2 Security issue - the security question

Let us formulate a security question, which would be beneficial from a defence perspective to be answered.

Is there a relationship between patch management of hardware device firmwares and the exposed attack surface?

In other words: *Can we improve attack resistance by keeping devices up-to-date and what is the actual practice in a production environment? How industrial devices compare to domestic devices?*

2.1 Involved parties in the security issue

Just like any other complex problem, there are different parties involved in such a broad question, forming numerous aspects of it. At the same time, there are different parties affected from the potential negative impacts of the issue as well. The first category can be considered as *actors* involved in the problem in one way or other and the latter as *potential problem owners*. Here we go through a list of both categories.

Immediate users These are the users utilising the service, software, or appliance without any proxy. Another descriptive term for them is the end-user. We will argue later why we are considering this group as the number one problem owner.

Indirect users This group of users are customers, or partners of the immediate users. Depending on the business model, services, software, or appliances used by the immediate users can play a role in providing solutions for indirect users. These are either customers of the immediate users, or their business partners. Clearly, since the indirect users utilise the functionality of products, they are also prone to the same risks, but maybe in a different fashion.

Vendors/manufacturers Any security problem has a direct effect on the vendor itself. IT products and services are under constant scrutiny for present deficiencies and the news of an incident is quickly publicised. This results in vendors loosing reputation and as a result, business value and income.

Universities/researchers Academic and research community is a major actor when it comes to technology and in our case, cybersecurity. Numerous products are based on the research carried out by academic bodies or research institutes. One can assume that the quality and depth of the research has an impact on the quality of the product and thus, on the security problem.

Governmental agencies When it comes to strategic systems, services and infrastructure, governmental agencies are involved in steering their national subjects. This is also the case for cybersecurity. As an example, The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), as part of the Department of Homeland Security in United States, is one such entity. Although these are umbrella organisation, they have an influence in the final outcome.

Standardisation and regulatory bodies Following published and proven best-practices, is a known cornerstone of cybersecurity. These best-practices are provided by regulatory bodies or industrial consortia, sharing their collective knowledge as proven set of instructions. From another perspective, IT solutions are saturated by protocols and communication mediums and methods. These are also defined by standardisation bodies and industrial consortia. When it comes to compliance, companies and organisations need to follow regulatory agencies' instructions. All this makes such institutions an important actor for our topic.

Private advisers and consultants Whenever the operational environment becomes bigger, when a corporate steps from being an SME towards being an enterprise for instance, decision making becomes complex. Whether working for the immediate user, or as a third-party, full-time, or project-based, consultants define the solution to be used. Therefore, they can be considered one of the important actors and where their presence is strong, they can even be a problem owner.

2.2 The main problem owner

For the purpose of this report, we are focusing on a single owner. We consider the immediate user of a service, a software, or an appliance as the problem owner, since this user is the one experiencing the most impact from the security issue.

It is important to mention that, it is also possible to consider other involved parties as problem owners. For instance, an indirect user such as someone receiving the services of the immediate user can also be the problem owner. Another example is a higher umbrella organisation. When talking about Industrial Control Systems (ICS), there is always a governmental agency coordinating the practical and educational efforts, to improve the cybersecurity of the country's infrastructure. The important factor here is to evaluate the amount of impact to these actors. The bigger the impact, the stronger the ownership.

3 Data gathering techniques for devices under scrutiny

Problem owners (defenders), have the advantage of defending a limited number of devices, owned by them. There can be three different cases though. The case we will consider is a company, owning an already in place network of legacy devices. Another case is implementation of brand new devices by the company, which will result in having up-to-date software and the chance for configuration during installation. Lastly, a company might migrate its existing network of devices to a new location. Since these devices have to be implemented again, the process of updating and proper configuration can be integrated with the move.

Our focus, the first case, brings up the importance of keeping a detailed inventory list of all devices with their respective details, such as firmware version, etc. This is one of the most overlooked practices in the IT industry.

3.1 Residential routers

We will consider two different brands of routers, Netgear and D-Link. The dataset for Netgear shows that, almost every version of Netgear devices is vulnerable to one attack or the other. Shodan search results shows around 30,000 Netgear and 30,000 D-Link routers that are vulnerable but still in use. Around 10,000-20,000 of the total are vulnerable to DoS attacks.

According to another resource, CVE Details, 35.3 % of vulnerabilities for D-Link devices are related to DoS. The distribution of different vulnerabilities can be seen in Figure 3.1.

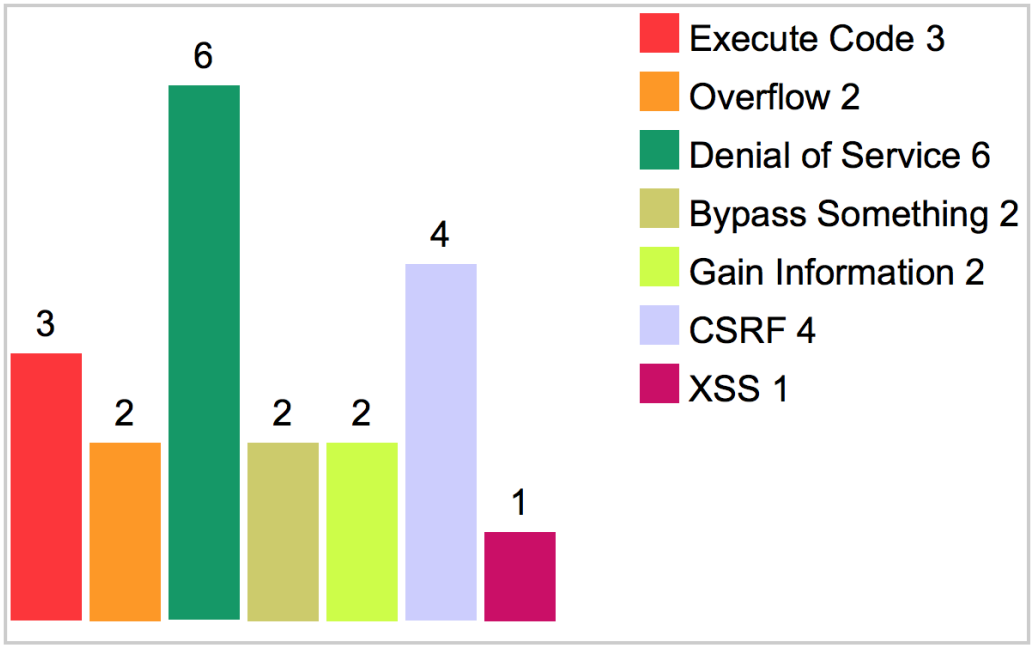


Figure 3.1: Vulnerabilities by type for D-Link

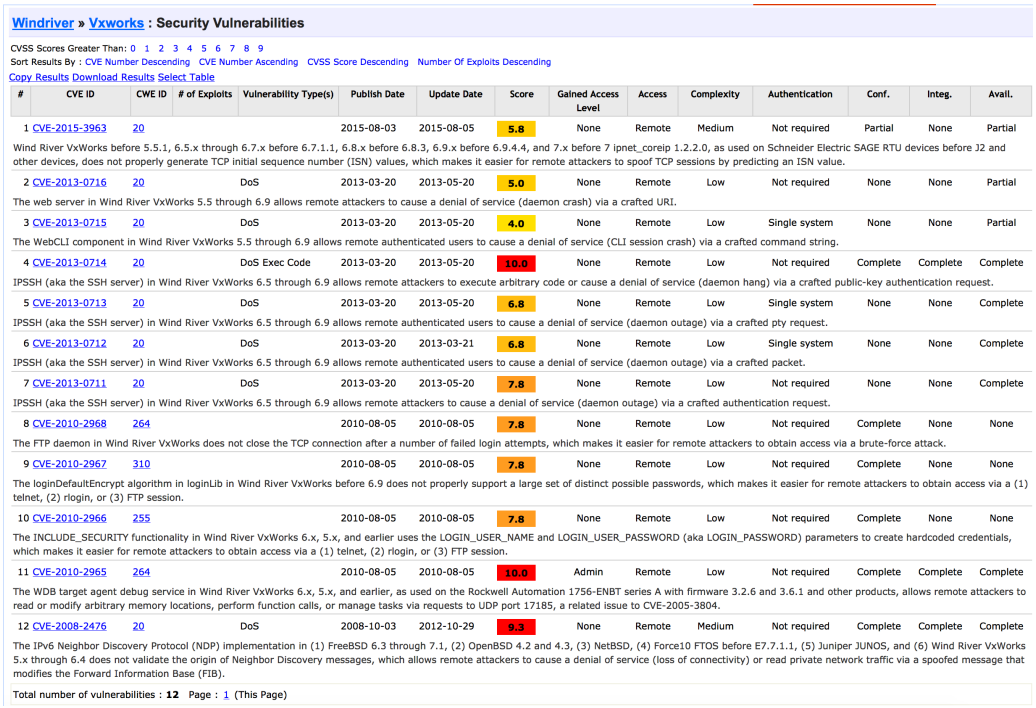
3.2 SCADA ICS systems

Before we start accumulating data and analysing it, there are a number of immediate known facts.

- SCADA systems have and use different WAN connections and remote communication protocols, making up the attack surface and. As a result, DoS attacks are highly feasible.
- It is important to consider two important facts regarding this, the priority in industrial systems is Availability. This is in contrast to general purpose IT environments and their first priority, data Security. These facts affect the analysis and chosen metrics.
- The effectiveness of having the latest patch for a firmware also depends on how fast the vendor responds to vulnerabilities. There might be a big time gap from the current version, till the next fixed version.
- An updated firmware can solve both *Software Flaws (CVE)* and *Misconfiguration (CCE)*. As an example for the latter case, a vulnerable firmware, could have a form of remote login enabled by default, using default credentials. In fact, this very example has been the case for many vendors.
- Legacy devices may not be capable of running the latest versions of available firmwares. This is a result of limited hardware performance, or an obsolete hardware platform. This point is one of the main reasons behind the fact that, legacy devices are vulnerable by definition.

Since SCADA systems are mostly devices with embedded operating systems and in many cases proprietary ones, attacks against them are based on present vulnerabilities and misconfiguration. Therefore the starting point is vulnerability databases. National Vulnerability

Database and CVE Details are two good resources for this purpose. An example from CVE Details is depicted in Figure 3.2.



Windriver » Vxworks : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2015-3963	20			2015-08-03	2015-08-05	5.8	None	Remote	Medium	Not required	Partial	None	Partial
	Wind River VxWorks before 5.5.1, 6.5.x through 6.7.x before 6.7.1.1, 6.8.x before 6.8.3, 6.9.x before 6.9.4.4, and 7.x before 7 ipnet_coreip 1.2.2.0, as used on Schneider Electric SAGE RTU devices before J2 and other devices, does not properly generate TCP initial sequence number (ISN) values, which makes it easier for remote attackers to spoof TCP sessions by predicting an ISN value.													
2	CVE-2013-0716	20		DoS	2013-03-20	2013-05-20	5.0	None	Remote	Low	Not required	None	None	Partial
	The web server in Wind River VxWorks 5.5 through 6.9 allows remote attackers to cause a denial of service (daemon crash) via a crafted URI.													
3	CVE-2013-0715	20		DoS	2013-03-20	2013-05-20	4.0	None	Remote	Low	Single system	None	None	Partial
	The WebCLI component in Wind River VxWorks 5.5 through 6.9 allows remote authenticated users to cause a denial of service (CLI session crash) via a crafted command string.													
4	CVE-2013-0714	20		DoS Exec Code	2013-03-20	2013-05-20	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
	IPSSH (aka the SSH server) in Wind River VxWorks 6.5 through 6.9 allows remote attackers to execute arbitrary code or cause a denial of service (daemon hang) via a crafted public-key authentication request.													
5	CVE-2013-0713	20		DoS	2013-03-20	2013-05-20	6.8	None	Remote	Low	Single system	None	None	Complete
	IPSSH (aka the SSH server) in Wind River VxWorks 6.5 through 6.9 allows remote authenticated users to cause a denial of service (daemon outage) via a crafted pty request.													
6	CVE-2013-0712	20		DoS	2013-03-20	2013-03-21	6.8	None	Remote	Low	Single system	None	None	Complete
	IPSSH (aka the SSH server) in Wind River VxWorks 6.5 through 6.9 allows remote authenticated users to cause a denial of service (daemon outage) via a crafted packet.													
7	CVE-2013-0711	20		DoS	2013-03-20	2013-05-20	7.8	None	Remote	Low	Not required	None	None	Complete
	IPSSH (aka the SSH server) in Wind River VxWorks 6.5 through 6.9 allows remote attackers to cause a denial of service (daemon outage) via a crafted authentication request.													
8	CVE-2010-2968	264			2010-08-05	2010-08-05	7.8	None	Remote	Low	Not required	Complete	None	None
	The FTP daemon in Wind River VxWorks does not close the TCP connection after a number of failed login attempts, which makes it easier for remote attackers to obtain access via a brute-force attack.													
9	CVE-2010-2967	310			2010-08-05	2010-08-05	7.8	None	Remote	Low	Not required	Complete	None	None
	The loginDefaultEncrypt algorithm in loginLib in Wind River VxWorks before 6.9 does not properly support a large set of distinct possible passwords, which makes it easier for remote attackers to obtain access via a (1) telnet, (2) rlogin, or (3) FTP session.													
10	CVE-2010-2966	255			2010-08-05	2010-08-05	7.8	None	Remote	Low	Not required	Complete	None	None
	The INCLUDE_SECURITY functionality in Wind River VxWorks 6.x, 5.x, and earlier uses the LOGIN_USER_NAME and LOGIN_USER_PASSWORD (aka LOGIN_PASSWORD) parameters to create hardcoded credentials, which makes it easier for remote attackers to obtain access via a (1) telnet, (2) rlogin, or (3) FTP session.													
11	CVE-2010-2965	264			2010-08-05	2010-08-05	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
	The WDB target agent debug service in Wind River VxWorks 6.x, 5.x, and earlier, as used on the Rockwell Automation 1756-ENBT series A with firmware 3.2.6 and 3.6.1 and other products, allows remote attackers to read or modify arbitrary memory locations, perform function calls, or manage tasks via requests to UDP port 17185, a related issue to CVE-2005-3804.													
12	CVE-2008-2476	20		DoS	2008-10-03	2012-10-29	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
	The IPv6 Neighbor Discovery Protocol (NDP) implementation in (1) FreeBSD 6.3 through 7.1, (2) OpenBSD 4.2 and 4.3, (3) NetBSD, (4) Force10 FTOS before E7.7.1.1, (5) Juniper JUNOS, and (6) Wind River VxWorks 5.x through 6.4 does not validate the origin of Neighbor Discovery messages, which allows remote attackers to cause a denial of service (loss of connectivity) or read private network traffic via a spoofed message that modifies the Forward Information Base (FIB).													

Total number of vulnerabilities : **12** Page : 1 (This Page)

Figure 3.2: A query result for known vulnerabilities

4 Metrics to measure the situation

Before considering practical metrics from the current dataset at hand, we will define ideal metrics for a best case scenario, in terms of data collection. What we define here basically applies to a hypothetical situation, were we can collect any reasonable kind of metadata for devices under scrutiny. Many of the attributes to be introduced, can be gathered in a real scenario as well. The truth of the matter is that, the amount of time and energy required to collect and process all this data, is the main constraint for categorising the situation as *ideal*. One might deduce acceptable enough results to answer questions, from a more practical dataset, as long as the error margin is within the acceptable boundaries of a production environment. Amongst other considerations, we must also opt for the speed of the analysis.

4.1 Ideal metrics

When we talk about security on the cyber space, we most of the time deal with metrics. A metric is formally defined as, "a mathematical function defined for a coordinates system that assigns a value to each pair of elements equal to the distance between them, or to a property analogous to distance between points on a line". In other words, metrics are measurements, that are compared to a known scale, or benchmark, to produce a meaningful result. Metrics are tools, enabling stakeholders to make decisions based on qualitative or quantitative assessments.

For cybersecurity purposes, metrics are very important for all types of organisations, in need of practical security benchmarking tools, in order to plan efficient security strategies. Any vulnerability can have a huge impact and organisations should be able to measure the risk involved with every vulnerability.

Different types of metrics can be put in place, depending on the organization. These metrics are both applicable to routers and SCADA devices. We usually try to separate them into three categories, technical, organisational and operational metrics. Examples are,

Organizational metrics:

- Cost of incident on a device
- Percentage of systems with known vulnerabilities
- Mean cost to mitigate one particular vulnerability
- Mean incident recovery cost
- Mean cost to patch

Operational metrics:

- Mean time between security incidents
- Mean time to incident recovery
- Mean time to patch a vulnerability

Technical metrics:

- Number of incidents
- Number of known vulnerabilities

4.2 Practical metrics

The proposed ideal metrics, either cannot be acquired, or at the very least, are hard to come by. Following this, a sensible approach would be to focus only on metrics directly relevant to the vulnerability under the focus. Going back to the initial security problem, in this case, we are focusing on DoS attacks and the effect of patch management practices on it.

For the sake of easing the cost estimation, it can be highly beneficial to consolidate metrics as a risk scale, for each device category and each device model. This scale can be actively updated, giving a good overall picture to the management about their inventory. In regards with DoS attacks, we have defined a function to display the relation between the risk scale and patch management. The function can be written as

$$S = -(M - M_p)^4 + C_p,$$

where M is the difference between the installed firmware and the latest firmware, in months, M_p is the number of months at peak cost and C_p is the peak cost. Solving the equation for $(S, M) = (0, 0)$ will result in

$$C_p = M_p^4.$$

As an example, we can plot the function for $M_p = 5$ months, as Figure 4.1 depicts.

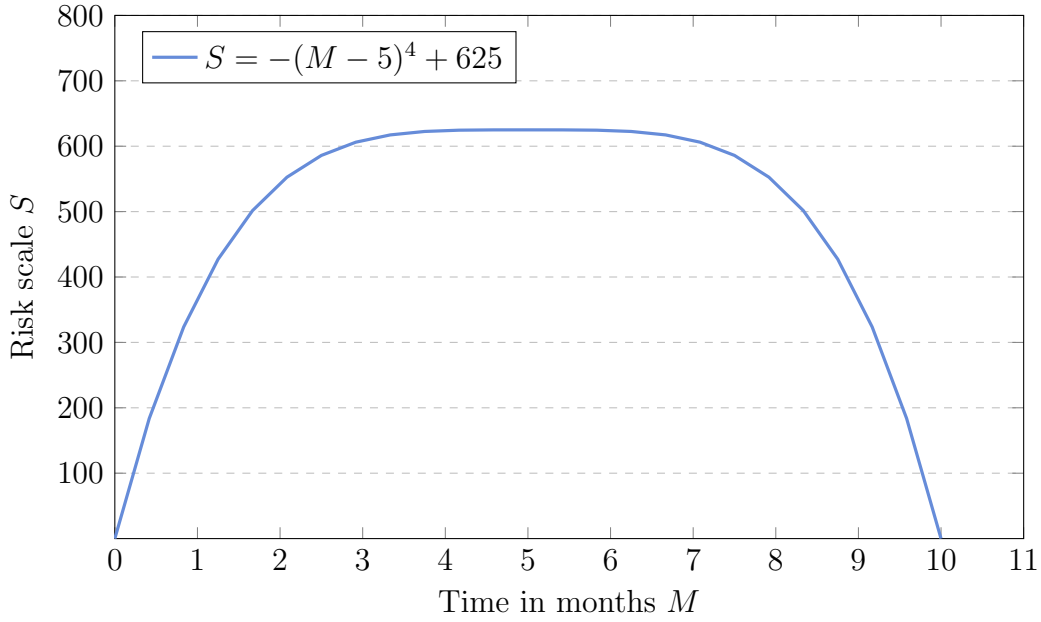


Figure 4.1: Scale function

What lies behind the choice of this forth degree polynomial is the fact that, the shape of the function closely simulates the real-world risk factor. As firmwares get old and vulnerabilities discovered, the risk increases. After a period of peak risk, as the device gets older and older, the risk also decreases. This can be explained by the fact that, devices older than a certain limit are less appealing to attackers.

This, of course is firmware-version-specific and applies to one device and one vulnerability. Now, if there is more than one vulnerability involved with that version, or there are multiple devices in operation, the equation can be updated as

$$S = [-(M - M_p)^4 + M_p^4] \cdot V_{fw} \cdot n,$$

where V_{fw} is the number of vulnerabilities associated with the firmware and n is the number of devices. Needless to say, the function can be tweaked as required to achieve a more accurate simulation.

4.3 Observable results

As an example, consider a problem owner with *Simatic S7 CPU 1200 series* ICS devices. According to the vulnerability statistics from CVE Details, 57.1% of the vulnerabilities for this model are DoS. All DoS vulnerabilities are related to firmwares previous to version 4.0. These DOS vulnerabilities were published on 2014-03-24. A quick search in Shodan reveals that only

15 from 50 devices (just a sample) are of v.4.0 or above. Therefore, only 30% are secure against these known DoS attacks. None of the devices have the latest v4.1.3 firmware. This can give the owner an indication of the seriousness of the situation and if it is worth looking into. The distribution of vulnerabilities by type is depicted in Figure 4.2.

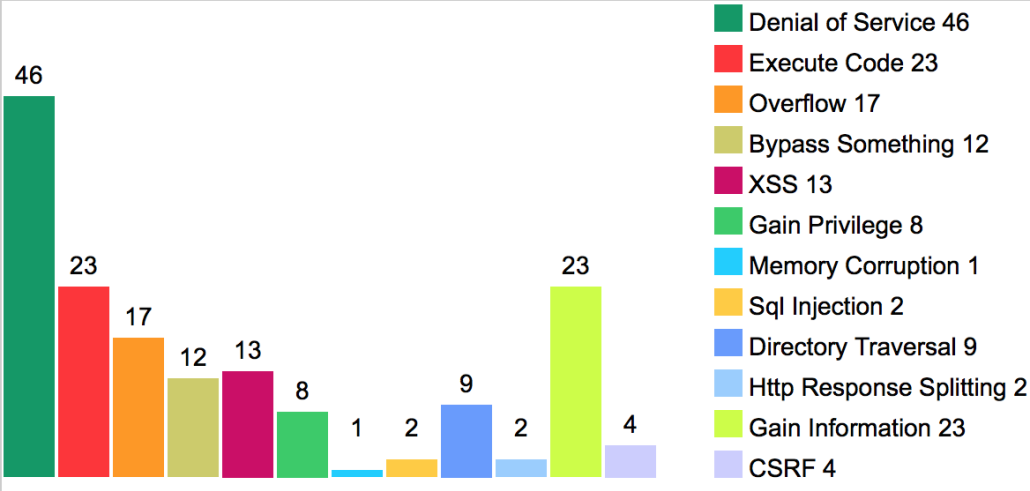


Figure 4.2: Vulnerability distribution for CPU-1200 series by type

5 The approach for remediation

5.1 Risk strategies for the problem owner

One risk reduction strategy might be to use 6-layers of security for defence-in-depth firewall agents. This strategy is effective because it is a multi layer approach to secure real-time control systems software, hardware and Ethernet-enabled plant equipment without impacting the speed or performance. Although it is 6 layers strategy but we will concentrate on 3rd layer because at this layer we can implement preventions against DoS attacks [8].

There is no way to completely protect your network from denial-of-service attacks, especially with the prevalence of distributed denial-of-service (DDoS) attacks on the Internet today. It's extremely difficult to differentiate an attack request from a legitimate request because the attackers often use the same protocols/ports and may resemble each other in content [2]. The limitation with these DDoS defences is that if the attacker can generate network traffic at a higher rate than your network's Internet connection can handle, it will be hard to avoid a meltdown. But what these defence strategies do accomplish is at least force the attacker to get a bigger gun [11].

5.1.1 For SCADA systems users

Users of SCADA systems are a major victim of DoS attacks. To counter the situation, a number of strategies can be adopted, limiting the risk to some extent.

Firewall One good practice to avoid DoS attacks and packet floods can be to decide which packet and packets with what contents can enter in your network. There are different types of firewall. It depends on the company which one it can afford and how much they are ready to accept the risk.

The main objectives behind installing a firewall is to minimise security risks. In order to fully be advantageous the following objectives need to be accomplished.

- Denied unauthorized access from external devices to SCADA networks by blocking direct connections from Internet to SCADA networks and from SCADA networks to the Internet.
- There should be well-defined rules about the type of traffic that can enter the network. In this way unwanted traffic can easily be blocked from the network.
- Authentication services requiring users wishing to connect to devices on the other side of the firewall to authenticate to the firewall using either passwords or strong two-factor authentication methods such as public-key encryption [1].

Intrusion Detection System (IDS) If firewall helps in blocking the attack, IDS is important in identifying the malicious activities and providing a proper response to the attack. IDS will help in modelling the network traffic. So by analysing the network traffic it is possible to find anomalies in the network. It always depends on the owner to deploy the IDS before firewall or keep IDS after the firewall.

Although firewalls can help to reduce the number of DoS attacks but only to some extent because firewalls itself are computers and they are susceptible to attacks like DoS, and backdoor attacks. So it is more optimal to have firewall and other defence at different layers. An example of a 6-layer design is depicted in Figure 5.1 [8].

Change of default configuration It is important to go through ALL default factory configuration, including default passwords for any remote access channel. This also includes the state of these channels and their enable/disable default setting. If something is not required, it should not be enabled.

5.1.2 For router users

The strategy that the problem owner can use to reduce the risk might be, to avoid using outdated protocols like CHARGEN and adding additional patches to some protocols like SNMP.

Vulnerabilities in protocols used by routers make them weak against DDoS attacks. Protocols like Simple Network Management Protocol (SNMP) and Character Generator protocol (CHARGEN) make routers vulnerable. SNMP is vulnerable to IP spoofing, because the source of SNMP request cannot be verified. CHARGEN is UDP based protocol and is also vulnerable to IP spoofing. Some of the steps and strategies that can be taken by the user are as follows.

- SNMP should include source authentication before making SNMP request.
- Stop using CHARGEN protocol.

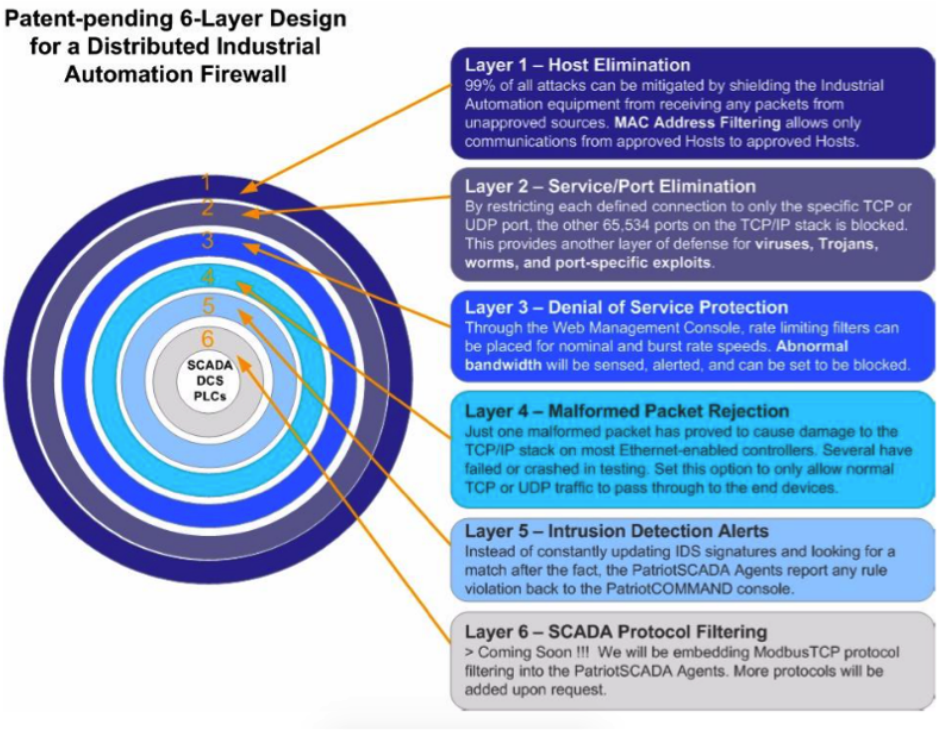


Figure 5.1: 6-layer defence design for distributed firewall agents

- Access Control Lists (ACL) - Routers that use ACLs to filter out unwanted traffic can avoid simple DDoS attacks such as ping to death attack. But ACLs will not provide any defence against some sophisticated attacks like SYN, RST, and ACK.
- Unicast Reverse path forwarding: This strategy will help to avoid spoofing attacking that uses IP addresses that do not belong to the subnet. But this strategy will fail if the attacker used source IP addresses from the subnet.
- Deactivate ANY query.
- Install new updates as soon as they are available.
- Change any default passwords.

5.2 Risk strategies for the actors

To tackle the problem, actors such as the vendor of the device and the IT department of the targeted company can use several strategies. Mind you that we are considering the most involved parties, an actor and the problem owner. The analysis of risk strategies for other actors is out of the scope of this report.

5.2.1 Risk strategies form vendor's perspective

First of all, the most important risk strategy for the vendor concerning routers and SCADA devices is the patch management, a reactive task which consists in fixing newly discovered

software vulnerabilities while keeping system operational. A patching distribution has to be created between the vendor and the consumer to allow a quick reaction to new vulnerabilities. A good communication is very important in that process.

5.2.2 Risk strategies form attacked company's perspective

Then, in a proactive perspective, other risk strategies can be chosen by the IT service of the targeted company to allow risk reduction (mitigation), risk acceptance, risk avoidance or risk transfer. A simple but significant risk strategy for SCADA devices is the password management for the different employees of the targeted companies. Indeed, we have previously seen that many attacks were perpetrated by the use of default passwords on SCADA devices. As a result, you can easily enter into the system.

Another method developed by Intel is called TARA (Threat Agent Risk Assessment) [9]. An example view is given in Figure 5.2. In an anticipating goal, the process consists in listing all the possible threat agents, attacker objectives and attack methods. Next, these data have to be filtered and prioritized and controls can be defined to avoid exposures. In the SCADA case, the main threat agents are opponents of the company using the devices, hacker inspired by environmental issues for example, and cyber terrorists. The objectives can be getting a technical or business advantage, or destroying the organization. Concerning domestic routers, threat agents can be script kiddies or booters, and the objective is blocking the router by DoS attack.

AGENT NAME	ATTACKER					OBJECTIVE		METHOD									IMPACT				
	Access	Trust				Motivation	Goal	Acts					Limits								
		None	Partial Trust	Employee	Administrator			Copy, Expose	Deny, Withhold, Ransom	Destroy, Delete, Render Unavailable	Damage, Alter	Take, Remove	Code of Conduct	Legal	Crimes Against Property	Crimes Against People	Loss of Financial Assets	Business Operations Impact	Loss of Competitive Advantage, Market Share	Legal or Regulatory Exposure	Degradation of Reputation, Image, or Brand
Employee Error	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X		X				X	X	X	X	X
Reckless Employee	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X			X			X	X	X	X	X
Information Partner	Internal		X			Accidental/Mistake	No malicious intent, accidental	X		X	X						X	X	X	X	X
Competitor	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Radical Activist	External	X				Social/Moral Gain	Change Public Opinion or Corporate Policy	X	X	X	X	X				X		X			X
Data Miner	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Vandal	External	X				Personal Gain (Emotional)	Personal Recognition or Satisfaction			X	X				X			X			X
Disgruntled Employee	Internal		X	X	X	Personal Gain (Emotional)	Damage or Destroy Organization		X	X	X				X			X	X		X

Figure 5.2: Example of TARA methods and objectives library

Another relevant method is CRAC (Confidentiality Risk Assessment and IT-Architecture Comparison) [7], which is an IT-architecture-based method for assessing and comparing confidentiality risks of distributed IT systems. CRAC analysis is composed of 4 steps: collecting basic information (assets, confidentiality level, component of IT architecture), analysing information flow (logical and physical connections between components), attack propagation paths (estimate of the likelihood that a threat agent compromises each component by following an attack propagation path) and risk calculation and comparison. Concerning SCADA devices and routers, password is the most important confidentiality issue. Moreover, an interesting

probabilistic method is FAIR (Factor Analysis of Information Risk) [6], which is a method for measuring the factors that drive information risk, including threat event frequency, vulnerability, and loss (depicted in Figure 5.3). For example, using our data set, we can use the number of DDoS attacks per year to get the threat event frequency, and we listed the vulnerabilities as well.

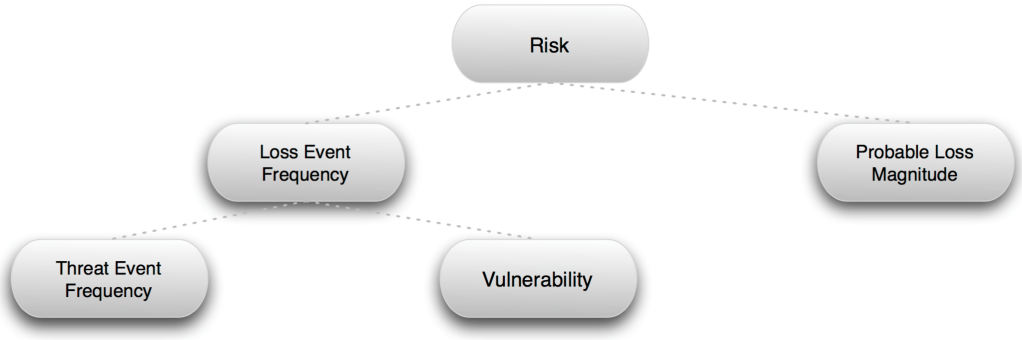


Figure 5.3: FAIR method standard graph

Finally, adversarial risk assessment in Game Theory [4] is very interesting because it consists in predicting the strategy and behaviour of the attacker. Consequently, the defender minimizes the maximum damage that the attacker can do after the defender has moved. This strategies changed over time in a way that reduces risks, for example, for the D-Link routers, the patching is so much faster than in 2008.

6 Exempli gratia

In this section, we will through two different examples of ROSI estimation for vulnerabilities. The first example focuses on unwanted remote access, as a result of misconfiguration. This can be an effect of default remote access channels being open after the installation.

The second example focuses on DoS attacks, which can be related vulnerable firmware. Overall, DoS attacks are a cybersecurity issue for all kinds of on-line devices, up-to-date, or not.

6.1 Tackling unwanted remote access

6.1.1 Components of ROSI equation

In every public or private organisation, each budget investment has to be justified and its effectiveness is often evaluated afterwards. But calculating a security metric is sometimes difficult as we have seen in the metrics-related parts on first assignment. Therefore, in finance, one of the most useful evaluation for decision-makers is called the Return On Security Investment. It can be one of the most effective way of measuring and determining existing security measures, and the potential need for additional ones. The ROSI is calculated as,

$$\text{ROSI} = ((\text{Risk Exposure } \times \%\text{Risk Mitigated}) - \text{Solution Cost}) \ / \ \text{Solution Cost}.$$

The *Risk Exposure* refers to the security breaches and risks that a company's computer system might be exposed to. It includes things such as intentional attacks by hackers or inadvertent downloads of various computer viruses, adware, etc. This figure is difficult to calculate, because the risks a company's computer system faces can differ from one week to another, or even fluctuate daily.

The *percentage of risk mitigated* is also difficult to calculate. This can be done by quantitative methods using metrics, in order to compare the state of your system before and after the risk is eliminated, or mitigated.

The final component of the Return On Security Investment (ROSI) equation is the *cost of implementing a solution to mitigate the security threat.* It can be tempting to integrate this amount by simply integrating the direct cost of the solution, including the acquisition, deployment and maintenance of security controls costs. However, a lot more naturally goes into determining the actual cost of a solution in terms of a Return On Security Investment equation. We also have to take into consideration the indirect costs and the effects it can have on productivity.

One the one hand, in some cases, implementing a security solution can actually decrease the productivity of an organization's employees. This sometimes happens because the new security measure forces employees to apprehend the new system. For example we have to take into account the monetary equivalent of time lost due to forgotten passwords after enforced changes or the inconvenience of transferring data between security zones, or incompatibilities between the previous and the new system put in place. In other words, increased security can translate into a loss of ease and convenience, and productivity can be impacted. The difference spent on a system before and after implementation can sometimes be very hard to measure however [5].

One the other hand, taking a security measure might actually increase the productivity of an organization's employee. Obviously, before implementing a security solution, for example repeated crashes and long down time can diagrammatically alter productivity. Due to the implementation of a security measure, then most employees are likely to experiences greater productivity. Whether a measure increases or decreases productivity, though, we must take into consideration this related fact into the total cost of the security cost [10].

6.1.2 Estimation of the costs involved in the strategy

We are now able to calculate the ROSI and the different costs related on a concrete case of one of the strategies shown above. We have chosen to estimate the cost related to an awareness-raising campaign about password changing on SCADA devices. This could be seen as a mundane strategy, easy to put in place. However we have noticed since the beginning of the work on SCADA devices that many vulnerabilities and a large amount of risk are due to misconfiguration and default passwords, and password attacks can be easily done by a remote-access control. All figures mentioned in the following section have been estimated because we have not found any relevant dataset dealing with the type of metrics mentioned above and that could be relevant for our ROSI calculation.

In the following calculation, we will assume two companies C1 and C2 employing respectively 100 employees and 2000 employees. The aim is to compare the situation between two companies towards risk and attack threats.

First, one can try to make a cost estimation of implementing this password-awareness campaign. As mentioned above, cost is divided into direct and indirect cost. Direct cost includes,

- The price of training for employees in both companies C1 and C2. Let's assume that one hour of training costs 25 EUR per employees, and that 4 hours of formation are necessary to be aware of the security risk. This cost gathers the amount of money spent to employ an external expert on security purposes, but also the hourly cost of employing the person attempting the meeting.
- The cost of effectively change password on SCADA devices. If we assume that companies both own 100 SCADA devices, and that each device takes ten minutes to change password, the whole amount of time is almost 17 hours. We will assume a cost per hour of 20 EUR (cost of hiring the employee).
- The cost of controlling, for each SCADA device, that the password has actually been changed. We estimate the monetary equivalent of time for this task at 100 EUR (approximately five hours for the whole amount of devices).

This strategy to mitigate the risk of attack also involves indirect costs.For instance, changing passwords can have an impact on the productivity of employees working on the SCADA devices. They need to enter new passwords that are unfamiliar on the SCADA interface and sometimes need help to recover password. This cost is very difficult to estimate. Let's assume here that impact on productivity is about 1 hour a month per employee (12 hours a year per person). It means a monetary equivalent of 240 EUR per employee per year.

Here we do not take into consideration any increase on the productivity. We can now sum up the total estimated cost of such a solution. The result is shown in Table 6.1.

	Company C1 (100 employees)	Company C2 (2000 employees)
Awareness campaign	$25 \times 100 \times 4 = 10{,}000$ EUR	$25 \times 2000 \times 4 = 200{,}000$ EUR
Cost of changing password	$100 \times 17 = 1700$ EUR	$100 \times 17 = 1700$ EUR
Control of passwords	100 EUR	100 EUR
Impact on productivity	$240 \times 100 = 24{,}000$ EUR	$240 \times 2000 = 480{,}000$ EUR
Total solution cost	35,800 EUR	681,800 EUR

Table 6.1: Total estimated cost of the solution

Many remarks can be made about these effective costs. First of all, we can note that if we rely on the assumptions made for our calculation, the cost of such a strategy hugely differs from one size of company to another. In our example, it varies almost linearly depending the size of the company (if we except the fixed costs of controlling the passwords on SCADA devices). Then we decided to choose the same amount of SCADA devices for both companies, but actually this number depends on each company and on its material needs, and making an average of devices used in companies seems difficult. We had to face the same difficulty concerning the average cost of one hour working, which depends on each country. However, we have tried to best represent reality on a European developed-country scale.

6.1.3 ROSI estimation

To calculate the ROSI and estimate the benefits of the strategy followed by our two companies C1 and C2, it's needed to estimate the risk exposure and the percentage of risk mitigated.

In the following section, we will try to be the most accurate possible. To do so, we have decided to assume three different scenarios S1, S2 and S3, depending each of the frequency of attack.

S1 Each year, C1 and C2 suffer 2 default password attacks. C1 estimates that each attack cost approximately 10,000 EUR in loss of data and productivity, whereas C2 estimates this cost at 100,000 EUR. Mitigation costs are those calculated and mentioned above.

S2 Each year, C1 and C2 suffer 6 default password attacks. Others estimations remain, C1 estimates that each attack cost approximately 10,000 EUR in loss of data and productivity, whereas C2 estimates this cost at 100,000 EUR.

S3 Each year, C1 and C2 suffer 12 default password attacks. Other estimations are identical.

As the percentage of risk mitigated is very difficult to estimate, and in order to get different visions depending on the effectiveness of our strategy, we also assume it to be expected to block either 40, 60 or 80% of the attacks, in order to test the reliability of our strategy. Indeed, hacking a system by entering default passwords is only one way to proceed when attacking a system and trying to fill this security issue does not prevent attackers from using other ingenious methods.

Now we have all the figures and different scenarios to calculate the ROSI, as shown in Table 6.2.

	Mitigation ratio = 40%	Mitigation ratio = 60%	Mitigation ratio = 80%
Scenario 1	C1: -77%, C2: -76%	C1: -66%, C2: -65%	C1: -55%, C2: -53%
Scenario 2	C1: -32%, C2: -29%	C1: 0.6%, C2: 6%	C1: 34%, C2: 41%
Scenario 3	C1: 34%, C2: 40%	C1: 101%, C2: 111%	C1: 168%, C2: 182%

Table 6.2: ROSI calculation for different scenarios

To try and compensate for our lack of information regarding the cost of risk exposure, the cost of mitigation and mitigation ratios, we have decided to go further in our assumptions and be as comprehensive as possible. We will consider a distribution of several risk exposures, with a combination of different percentages of risk mitigated. ROSI function of risk exposure for a company of 2000 employees is depicted in Figure 6.1. The assumption of 40%, 60% and 80% risk mitigation for several password attacks in a year, is considered for these plots respectively.

Many conclusions can be drawn regarding the ROSI calculations and the results. First, with the assumptions made to calculate it, it can be noticed that the size of the company does not really matter. This means that, in the case of this particular strategy, the more company employs people and the more money will have to be spent to make them aware of the security issue, and the more financial impact it will have in case of attack as well. Then we also note that this strategy is only valid and efficient if the frequency of hacking password is high, the more attacks occur and the most efficient and relevant the strategy in term of money spent. Moreover, as we could expect, better is the mitigation ratio and better is the return on investment. As a result, we can say that one strategy is only valid in terms of money spent is the risk is high enough and if the solution proposed is efficient enough to mitigate the security issue.

6.2 Tackling DoS

In this second strategy we consider an automotive industry facing DoS attack. This is another example of attack that is very regular nowadays and which can have huge impact on productivity as we will see. This is the most frequently type of vulnerability used for hacking into a system and the number of attacks have reached unprecedented levels for a few couple of years. In the following calculation, we will assume a big company which has several car production lines and which has to face with a DoS attack on a production line, affecting as a consequence all the chain of production and creating a downtime until the attack is repaired.

6.2.1 Estimation of the costs involved in the strategy

First, cost estimation of the repairing has to be done. As mentioned above, cost is divided into direct and indirect cost. The cost of this solution includes the price of hiring or calling up IT employees to detect where the problem happens and go up as much as possible to the source of the attack. Experts also have to stop the attack by redirecting it towards a "black hole" and try to fix the problem so as it does not happen again. Let us assume that one hour costs 25 EUR per employees, and that 6 experts are required to face the attack. Moreover, on average, 6 hours is good ratio of time to solve a DoS attack and stopping a production costs, again on average, 20,000 EUR for a company per minute in the automotive sector. This downtime number especially includes the losses in term of equipment production, cost of delay and costs of hiring employees who have no tasks to do [3]. This is no indirect cost here (impact on productivity for example), because the solution found (fixing the problem) has no impact on employees.

As a result, solving this attack problem costs $25 \times 6 \times 6 = 900$ EUR. As mentioned above, the losses for a company per minute of downtime is 20,000 EUR. In a period of 6 hours, the deficit can reach $20{,}000 \times 60 \times 6 = 7{,}200{,}000$ EUR in losses.

6.2.2 ROSI estimation

We can now calculate the ROSI. If we assume that 50% of the risk has been mitigated by the solution, we get a ROSI of 399,900%. With a ratio of 60% of risk mitigated, ROSI reaches 479,000%.

	Mitigation ratio = 50%	Mitigation ratio = 60%
Scenario	399%	479%

Table 6.3: ROSI calculation for DoS scenario

Thus, this calculation shows us that sometimes breaches have very huge impact on a company in terms of economic losses and mitigating attacks. At this level, we wonder whether it is still relevant or not to use the ROSI estimation, due to the enormous discrepancy between solution cost and estimation of risk.

6.3 Limitations of the ROSI model

Estimating the amount of money saved from losses that may never happen is a hard task that as we have seen. In the real world, it requires more than straightforward application of

simple formulas. Indeed, our ROSI calculation is the result of many approximations. The cost of a security incident and the annual rate of occurrence are very hard to estimate and the resulting numbers can vary highly from one firm to another. Moreover, in our calculation we have decided to take the same amount of SCADA devices for both companies. However, the bigger a company is and the more likely it uses SCADA devices to monitor processes.

As a matter of fact, the ROSI calculation is essential for us to be able to give insight into an estimated cost of a strategy, and to be able to know whether a strategy can be put in place or not.

7 Conclusion

What it boils down to is that, security problems involve different actors. Depending on the perspective taken for the analysis, the problem owner can be different, but without any doubt, the immediate user is the number one problem owner. In this report, we went through numerous actors and their parts. Depending on how deep we would like to analyse the problem domain, we need to consider these actors and the strategies to be taken by them.

Actors can tackle the problem using several risk management strategies. Indeed, vendors and manufacturers of the device need to develop their patch management workflow, as we could see with the *"time between the current the newest versions of firmware"* metric. Concerning the IT department of the targeted companies, password and remote access management is very important to mitigate attacks against SCADA devices. A number of proactive methods can be established by the company such as, TARA method concerning the threat agents, CRAC strategy for the confidentiality, FAIR method to calculate the threat event frequency and the magnitude of losses, and Game Theory to understand the attacker's behaviour to minimise the impact of the attack. Finally, over time, these strategies will evolve in a way that reduces risks.

DoS and DDoS attacks against SCADA systems and routers are so effective that it can disrupt services and pave the way for their misuse in attacks against other victims. The attack becomes more devastating when large numbers of vulnerable devices are put in to work to attack SCADA systems. Although it is almost impossible to eradicate these attacks, but there are ways to make it harder for the attacker to carry on the task.

As we saw, from a defender's point of view, several strategies can be put in place to try to measure the actual risk and mitigate security breaches. Depending on the situation, some strategies are more efficient than others. Decision-makers, who need to know the financial impact of a security issue on infrastructure, need practical economic tools before investing in a strategy. Very often a compromise has to be reached between costs and efficiency. We believe that the ROSI calculation presented previously, can help decision-makers in taking measures. However, to be as accurate as possible, a set of tools must be utilised, including for example, the *ALE (Annualised Loss Expectancy)*, or the *"net present value"* model.

References

[1] Eric Byres, John Karsch, and Joel Carter. *Firewall Deployment for SCADA and Process Control Networks*. CPNI. 2005. URL: http://energy.gov/sites/prod/files/Good%20Practices%20Guide%20for%20Firewall%20Deployment.pdf (visited on 10/11/2015).

[2] Mike Chapple. *How to prevent a denial-of-service (DoS) attack*. ITBusinessEdge. URL: http://searchsecurity.techtarget.com/answer/How-to-prevent-a-denial-of-service-DoS-attack (visited on 10/11/2015).

[3] *Costs of Downtime in the Manufacturing Industry*. eMaint. URL: http://www.emaint.com/manufacturing_downtime_infographic/ (visited on 10/11/2015).

[4] Louis Anthony (Tony) Cox Jr. "Game Theory and Risk Analysis". In: *Risk Analysis* 29.8 (2009), pp. 1062–1068. ISSN: 1539-6924. DOI: 10.1111/j.1539-6924.2009.01247.x. URL: http://dx.doi.org/10.1111/j.1539-6924.2009.01247.x.

[5] Lawrence A. Gordon and Martin P. Loeb. "The Economics of Information Security Investment". In: *ACM Trans. Inf. Syst. Secur.* 5.4 (Nov. 2002), pp. 438–457. ISSN: 1094-9224. DOI: 10.1145/581271.581274. URL: http://doi.acm.org/10.1145/581271.581274.

[6] Jack A. Jones. *An Introduction to Factor Analysis of Information Risk (FAIR)*. Risk Management Insight. 2005. URL: http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf (visited on 10/11/2015).

[7] Ayse Morali et al. "CRAC: Confidentiality Risk Assessment and IT-Architecture Comparison". In: *Proceedings of the 6th International Conference on Network and Service Management (CNSM 2010)*. Los Alamitos: IEEE Computer Society Press, Aug. 2010. URL: http://doc.utwente.nl/72631/.

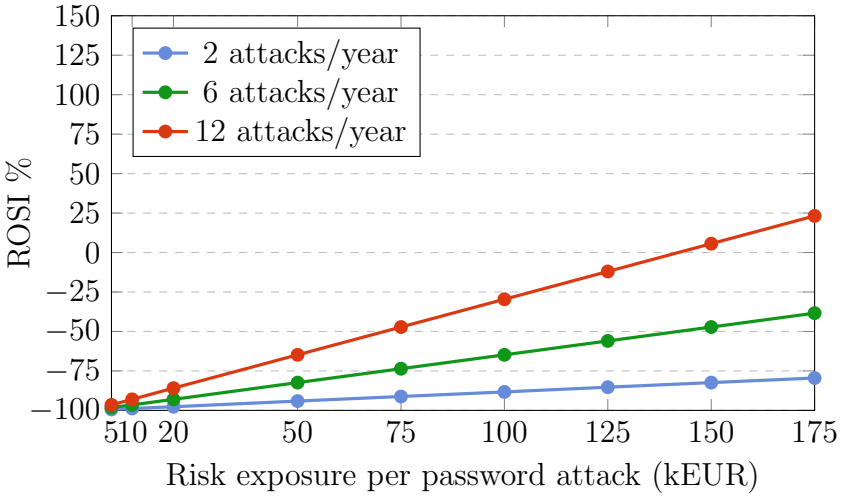
[8] Jonathan Pollet. *patriotSCADA Distributed Firewall for SCADA and Industrial Networks*. PlantData Technologies. URL: http://www.controlglobal.com/assets/whitepapers/wp_001_SCADApollet.pdf (visited on 10/11/2015).

[9] Matthew Rosenquist. *Prioritizing Information Security Risks with Threat Agent Risk Assessment*. Intel. 2009. URL: https://communities.intel.com/community/itpeernetwork/blog/2010/01/05/whitepaper-prioritizing-information-security-risks-with-threat-agent-risk-assessment (visited on 10/11/2015).

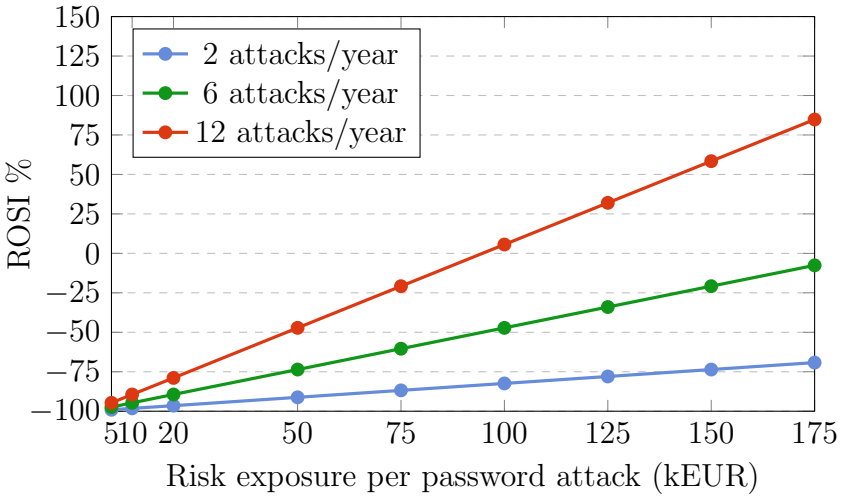
[10] Wes Sonnenreich, Jason Albanese, and Bruce Stout. "Return On Security Investment (ROSI): A practical quantitative model". In: *Journal of Research and Practice in Information Technology*. INSTICC Press, 2005, pp. 239–252.

[11] Aaron Weiss. *How to Prevent DoS Attacks*. eSecurity Planet. 2012. URL: http://www.esecurityplanet.com/network-security/how-to-prevent-dos-attacks.html (visited on 10/11/2015).

ROSI function of risk exposure with 40% of risk mitigated



ROSI function of risk exposure with 60% of risk mitigated



ROSI function of risk exposure with 80% of risk mitigated

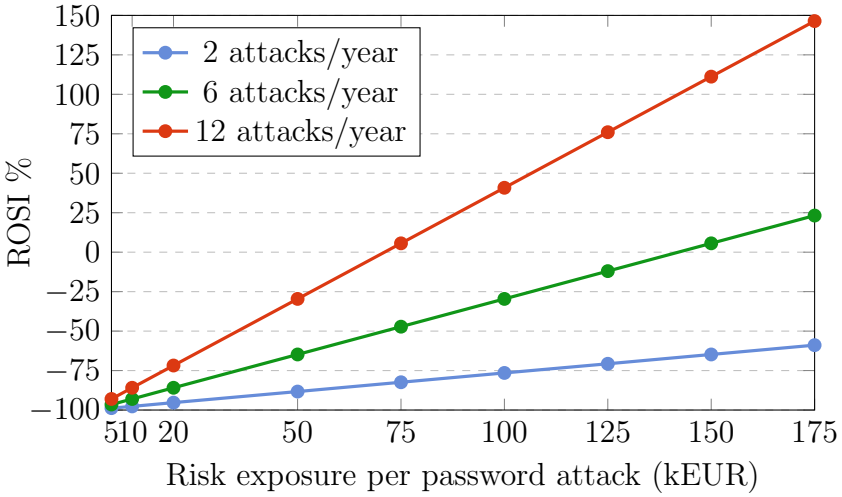


Figure 6.1: Different possibilities for the ROSI function