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 5, 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

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

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.

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 Devices under scrutiny

3.1 Residential routers

3.2 SCADA ICS systems

3.3 Data gathering techniques

4 Metrics to measure the situation

4.1 Ideal metrics

4.2 Limitations

4.3 Practical metrics

4.4 Observable results

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.

There's 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.[5]. 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.

5.1.1 For SCADA systems

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.

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 modeling the network traffic. So by analyzing 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.

5.1.2 For routers

The strategy that the problem owner can use to reduce the risk might be avoid using outdated protocols like CHARGEN and add additional patches to some protocols like SNMP.

Vulnerabilities in protocols used by the routers, make the routers vulnerable to DDoS attacks. Protocols like Simple Network management protocol (SNMP) and Character Generator protocol (CHARGEN) make the router 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.

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

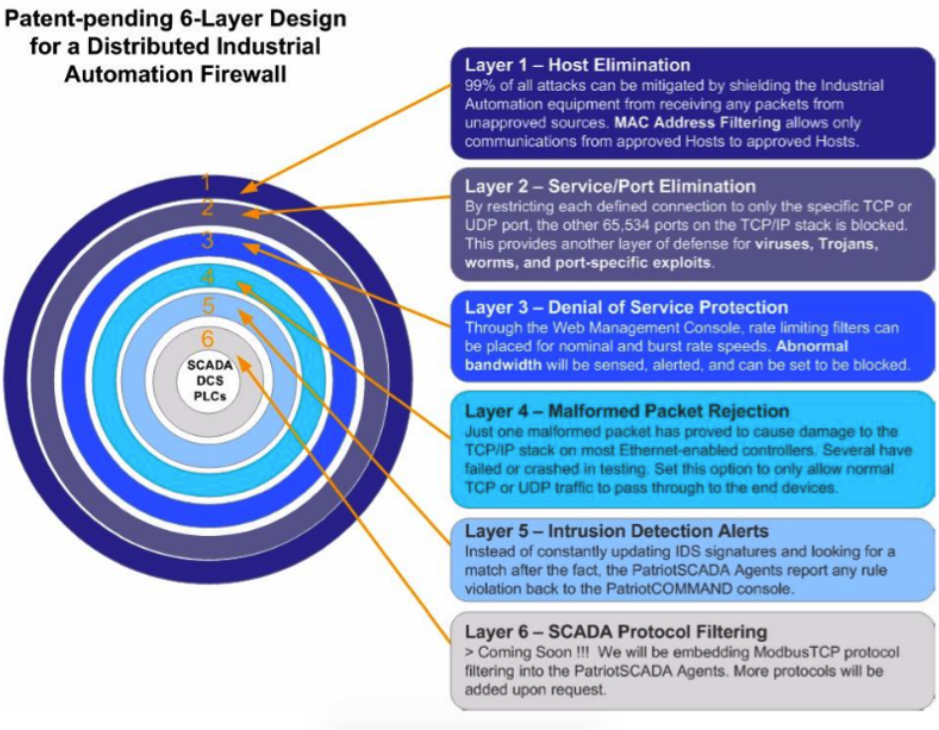

Figure 5.1: 6-layer defence design for distributed firewall agents

- 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.

5.2 Risk strategies for the actors

To tackle the problem, actors such as the vendor of the device and the IT service of the targeted company can use several strategies. 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.

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). 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), 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), 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.

Finally, adversarial risk assessment in Game Theory 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 more fast than in 2008.

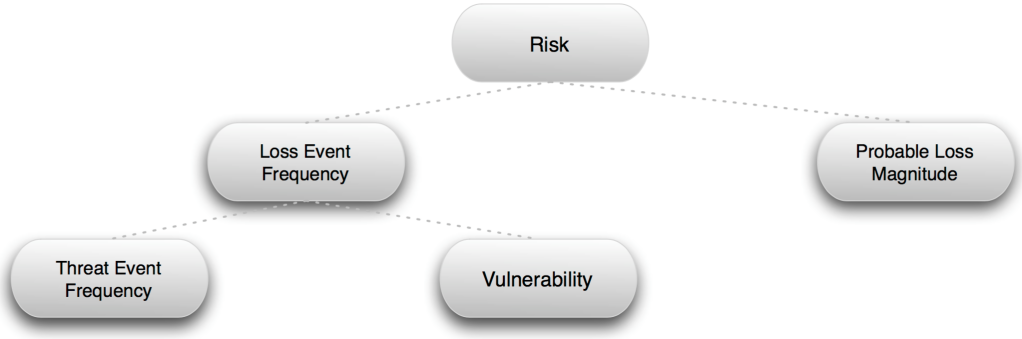

Figure 5.3: FAIR method standard graph

5.3 Exempli gratia

5.3.1 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 he risks that a company's computer system faces can differ from one week to one other, 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.

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.

5.3.2 Estimation of the costs involved in our 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.

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 5.1.

	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 5.1: 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.

5.3.3 ROSI estimation and limits of the model

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 5.2.

	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 5.2: ROSI calculation for different scenarios

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 : 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.

5.3.4 Limitations of the 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.

6 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. I this report, we went through numerous actors and their part. Depending on how deep we would like to analyse the problem domain, we need 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.