

Security Taxonomy Pattern Language

Ben Elsinga, Aaldert Hofman
Technology Consulting
Cap Gemini Ernst & Young Nederland B.V.

Ben.Elsinga@cgev.nl
Aaldert.Hofman@cgev.nl

1 INTRODUCTION

1.1 Intent

The intent of this pattern is to give you guidance and support in establishing a consistent and coherent set of security aspects that have to be addressed in enterprise security.

1.2 Motivation

In day-to-day life we experience that people address information security only in a limited way. That might be because they do not oversee the broadness of the information security field or because they just focus on products or techniques.

You could argue if setting terminology is a pattern at all. The authors discussed this issue and from our point of view it is a pattern.

- Every pattern uses specific terminology. Yet there is no section on terminology in the pattern template. Hence, terminology used in a pattern is hardly ever defined properly. A pattern setting terminology provides a common basis and reusable solution to this.
- It is a comprehensive way of setting terminology; it saves you all the hassle in reading standards or books. But it's more than that: we combine several sources and pick the terminology that we know to be good, based on our experience in the field.

1.3 Patterns introduced in this paper

This paper introduces a few patterns that contribute in solving this problem by providing a consistent framework of terminology along a few distinct dimensions:

- The Goal of security: why do you want to provide security?
- The Nature of safeguards: safeguards can be physical, but also within IT, etc.
- The Effect of safeguards: preventing incidents, detecting incidents, etc.

1.4 Acknowledgements

We would like to thank our EuroPLoP2003 shepherd Markus Schumacher, Darmstadt University of Technology, who guided us through several iterations of our submission and provided many constructive comments. All in all he's a nice guy.

2 THE GOAL OF SECURITY

Alias: Security Services Pattern

2.1 Context

In everyday life it is difficult to perceive the collection of security safeguards in an organisation as a complete, coherent and consistent set of security safeguards. This pattern provides a complete set of security aspects that can be used in a structured approach to information security.

This pattern is applicable in any situation where information security is addressed. However, this does not mean that all security aspects are applicable in every situation. The pattern aims at introducing security to novices; security professionals will need much more material.

2.2 Example

The apt of the monastery in Irsee wants to protect the recipe of the beer. However, since securing information is not his prime task, he can't think of anything else than just putting a lock on the door or perhaps even burying the recipe.

Since the apt is a wise man, he assumes that it's probably not that easy. So he invites some fans of the beer that happen to be experts in the field of information security. The apt asks them how he should address all relevant security aspects.

2.3 Problem

How can we structure the complex world of information security in such a way that we can assure to address all regular goals of information security?

2.4 Forces

People focus on technique, on the security safeguards to be implemented. Thereby they tend to forget to ask what the goal of the safeguard is. The safeguard in itself might be perfect, however it serves another goal than you need.

The approach to security is usually either strategic or operational. Strategists are concerned about risk analysis and risk management; they talk about confidentiality, integrity and availability. Operational people are concerned about flaws in the operational safeguards and maintaining them; they talk about firewall, viruses and hackers. Each group thinking about it's own business, they lack a set of security goals to bridge the communication gap.

Due to time pressure people are eager to implement security safeguards, without asking or concerning about why they need this specific safeguard.

A fragmented approach, usually for years, result in a patchwork quilt of security safeguards of very different age, quality, effectiveness or cost. People do not care or do not know why a certain safeguard is in place and they're not interested in the security goal of this safeguard.

A lot of people regard the Code of Practice (ISO17799, also known as British Standard 7799) as the one and only truth about security. However, since ISO17799 focuses on what to do and pays hardly any attention to why to do so, people are not questioning the goal.

It is difficult to find a good and comprehensive overview of the goal of security. It's not that there is no material on the subject; there are lots of books and international standards. However, this material is definitely not for free and consists of hundreds of pages reading.

2.5 Solution

The solution is to provide a comprehensive structure to the complex world of information security along international standards ISO13335 and ISO7498, that both have proven to address all regular goals of information security.

The ISO Technical Report 13335, part 1 provides a clear definition of IT Security:

IT Security is related to all aspects related to defining, achieving and maintaining:

- Confidentiality
- Integrity
- Availability
- Accountability
- Authenticity
- Reliability

Each of these security aspects is defined as well, largely based on ISO7498:

Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities or processes [7498].
Integrity	Consisting of data integrity and system integrity: <ul style="list-style-type: none">• Data integrity is the property that data has not been altered or destroyed in an unauthorized manner [7498].• System integrity is the property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system.
Availability	The property of being accessible and usable upon demand by an authorized entity [7498].
Accountability	The property that ensures that the action of an entity may be traced uniquely to the entity [7498].
Authenticity	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.
Reliability	The property of consistent intended behaviour and results.

2.6 Resolved example

So the experts provided the apt with a comprehensive paper addressing all relevant aspects of IT security, based on international standards ISO13335 and ISO7498. They also provided the apt with some examples to think about.

The apt knows that he addresses all aspects of security, when considering:

- Confidentiality, e.g. to ensure that the recipe is not made available or disclosed to unauthorized people.
- Integrity, e.g. to ensure that no one messes with or destroys the recipe, but also that no one messes with or destroys the brewery machinery.
- Availability, e.g. to ensure that the recipe and the brewery are accessible and usable when the monastery wants.
- Accountability, e.g. perhaps less important for the apt, although he still likes to be sure that he can address the monks on certain actions they did or did not perform.
- Authenticity, e.g. to ensure that the recipe indeed is the right one. But also that suppliers or buyers are the ones they claim to be.
- Reliability, e.g. to ensure that the brewery works as it is supposed to do.

From now on the apt knows what he's talking about as far as security aspects are concerned.

2.7 Consequences

Benefits:

- This paper sets terminology on the goal of IT security.
- The paper provides a comprehensive overview based on extensive knowledge of and experience with international standards.
- The security aspects can be understood, remembered and addressed very well.
- It's easy to refer to and it's free 😊

Pitfalls:

- Since IT security knows a lot of terminology, with synonyms and homonyms, it is quite easy to frustrate communication by using an extensive vocabulary.
- A comprehensive overview does not and cannot replace books and standards. Do not assume that you know all there is to now after reading this paper.

2.8 Implementation Issues

Two other ISO standards related to IT Security are very well known as well: ISO 17799 (also known as British Standard 7799) and ISO 7498.

ISO 17799 regards Confidentiality, Integrity and Availability in 10 separate chapters. Although not named explicitly, ISO 17799 also addresses Accountability, Authenticity and Reliability, but this is less clear than ISO 13335.

ISO 7498 regards Security Architecture and has a lot of resemblances with ISO 13335. The main disadvantage of ISO 7498 is the use of the word "Security Service". In the Internet era with web services etcetera, this leads to a lot of miscommunication.

Be aware these issues only regard the provision of a complete set of security goals. The goal and use of the named standards is much broader than just provisioning security goals.

2.9 Related Patterns

All patterns in the Taxonomy Pattern Language are strongly related to each other:

- This pattern assures that we address all security goals.
- The pattern “The Nature of Safeguards” assures that we are aware of the different natures of safeguard and shows how these support each other.
- The pattern “The Effect of Safeguards” assures that we are aware of the different effects of safeguards and shows how these add to each other.

The discussion paper [Schumacher] introduced the idea to extract patterns from standards.

2.10 Known Uses

The authors used this pattern in several security architecture projects, e.g. in the IBB-project. In that project we used this material to explain to others (from project manager to designer) the essence of IT security within 5 minutes.

2.11 References

- [7498] ISO 7498-2:1989, Information processing system – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.
- [13335] ISO/IEC TR 13335-1:1996, Information Technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security.
- [17799] ISO/IEC 17799-1:2000, Information Technology – Code of Practice for Information Security Management – Part 1.
- [Schumacher] Security Patterns and Security Standards by Markus Schumacher, Darmstadt University of Technology; 11 June 2002.

3 THE NATURE OF SAFEGUARDS

Alias: Security is more than just technique

3.1 Context

We assume that by now you do have a clear picture of all security goals; otherwise you'd better read the previous pattern "The Goal of Security" first.

In everyday life there are always alternative ways to achieve the goal of security. These alternatives might not only differ in complexity or effect, but also in nature. This pattern provides a comprehensive and complete set of these natures that can be used in a structured approach to information security.

This pattern is applicable in any situation where information security is addressed. However, this does not mean that safeguards of all natures are applicable in every situation. The pattern aims at introducing security to novices; security professionals will need much more material.

3.2 Example

The apt of the monastery in Irsee wants to protect the recipe of the beer. However, since securing information is not his prime task, he can't think of anything else than just putting a lock on the door or perhaps even burying the recipe.

Since the apt is a wise man, he assumes that it's probably not that easy. So he invites some fans of the beer that happen to be experts in the field of information security. The apt asks them if there is any alternative to physical precautions.

3.3 Problem

How can we structure the complex world of information security in such a way that we can assure to regard all different natures of information security safeguards?

3.4 Forces

In general people find it difficult to think "out of bounds": if you're working in IT, you might forget that a physical lock might do the trick as well.

People tend to underestimate the complexity in applying safeguards of another nature; they think they can do it themselves, without involving appropriate expertise. Have you ever compared the challenges in managing physical keys to cryptographic key management?

In a lot of situations safeguards of different natures complement each other; only combining these will provide a sound solution. People often do not think about this dependency, since they are happy that at least one safeguard is in place.

It is difficult to find a good and comprehensive overview of the nature of security. It's not that there is no material on the subject; there are lots of books and international standards. However, this material is definitely not for free and consists of hundreds of pages reading.

3.5 Solution

The solution is to provide a comprehensive structure to the complex world of information security along international standard ISO13335 that has proven to address all different natures of information security safeguards.

The ISO Technical Report 13335, part 1 addresses the nature of safeguards:

Physical	Safeguards in the physical environment.
Technical	Safeguards in the technical environment (in hardware, software or communications).
Personnel	Safeguards in the personnel environment.
Administration	Safeguards in the administrative environment.

3.6 Resolved example

So the experts provide the apt with a comprehensive overview of all different natures of safeguards.

The apt recognizes that all these natures can be applied.

- Technical, since safeguards in the hardware, software and communications of the brewery are necessary to protect the recipe.
- Physical, since safeguards in the physical environment (like a lock on the door) prevent people just walking in.
- Personnel, since safeguards in the personnel environment (like a guard) will help in case there are some intruders who broke physical or technical safeguards.
- Administration, since safeguards in administrative environment (like regulations or procedures) will ensure that the people in the monastery know what to do or not to do

From now on the apt knows that he can address safeguards of all these natures to have a consistent and complete set of safeguards.

3.7 Consequences

Benefits:

- These different natures are supplementary to each other.
- Alternatives can be judged on ease of use, costs, effectiveness, etc.
- This paper sets terminology on the nature of IT security.
- The paper provides a comprehensive overview based on extensive knowledge of and experience with international standards.
- It's easy to refer to and it's free 😊

Pitfalls:

- Don't think you're an expert on all safeguards in all these environments.
- A comprehensive overview does not and cannot replace books and standards. Do not assume that you know all there is to now after reading this paper.

3.8 Implementation Issues

Although ISO13335 provides a good solution, you have to be aware that it is all about regarding safeguards of alternative natures. So if you find another source for alternative natures, that's no problem at all. Just verify that you find at least the natures listed above.

Synonyms to the terminology used in ISO13335 are widely available. Again, remember that it is all about regarding safeguards of alternative natures. Exact terminology is less important.

3.9 Related Patterns

All patterns in the Taxonomy Pattern Language are strongly related to each other:

- The pattern "The Goal of Security" assures that we are aware of the complete set of security goals and what definitions come along.
- This pattern assures that we address all different natures of safeguards.
- The pattern "The Effect of Safeguards" assures that we are aware of the different effects of safeguards and shows how these add to each other.

The discussion paper [Schumacher] introduced the idea to extract patterns from standards.

3.10 Known Uses

One of the most common known uses is in passwords:

- The use of passwords is a technical safeguard available in operating systems.
- An administrative safeguard (specifying the minimum requirements of a good password) is necessary in addition.
- A personnel safeguard (checking keyboards for post its or providing a helpdesk) is also necessary in addition.
- And finally, a physical safeguard (a lock on the computer room) complements it all.

Besides this, the authors used this pattern in several security architecture projects. In these projects we used this material to explain to others (from project manager to designer) the essence of IT security within 5 minutes.

3.11 References

- [7498] ISO 7498-2:1989, Information processing system – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.
- [13335] ISO/IEC TR 13335-1:1996, Information Technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security.
- [17799] ISO/IEC 17799-1:2000, Information Technology – Code of Practice for Information Security Management – Part 1.
- [Schumacher] Security Patterns and Security Standards by Markus Schumacher, Darmstadt University of Technology; 11 June 2002.

4 THE EFFECT OF SAFEGUARDS

4.1 Context

We assume that by now you do have a clear picture of all security goals and all alternative natures of security safeguards; otherwise you'd better read the previous patterns "The Goal of Security" and "The Nature of Safeguards" first.

In everyday life people usually only think about implementing security safeguards, without paying attention to the effect of the safeguard. Besides that, there are always alternative ways to achieve the goal of security. These alternatives might not only differ in complexity or nature, but also in effect. Since these effects are quite different, this is an important thing to consider. This pattern provides a comprehensive and complete set of these effects that can be used in a structured approach to information security.

This pattern is applicable in any situation where information security is addressed. However, this does not mean that safeguards of all effects are applicable in every situation. The pattern aims at introducing security to novices; security professionals will need much more material.

4.2 Example

The apt of the monastery in Irsee wants to protect the recipe of the beer. However, since securing information is not his prime task, he can't think of anything else than just putting a lock on the door or perhaps even burying the recipe.

Since the apt is a wise man, he realises that just a lock on the door is not sufficient. At least there has to be someone to call the police when an intruder forces the lock. The apt wonders if the same is true for IT security.

4.3 Problem

How can we structure the complex world of information security in such a way that we can assure to regard all different effects of information security safeguards?

4.4 Forces

People often think that it's sufficient to do something to prevent any incident. That's the easiest step in providing security and at least you can tell your boss that you did something.

Bosses don't like to hear that you need more money, more time and more people, just because you want to apply multiple safeguards of different effect. They think only one safeguard should do.

It is difficult to find a good and comprehensive overview of the effect of security. It's not that there is no material on the subject; there are lots of books and international standards. However, this material is definitely not for free and consists of hundreds of pages reading.

4.5 Solution

The solution is to provide a comprehensive structure to the complex world of information security along international standard ISO13335 that has proven to address all different effects of information security safeguards.

The ISO Technical Report 13335, part 1 provides a clear statement of the function, the effect of the safeguards in IT Security:

Detection	Safeguards used to detect that another safeguard is compromised.
Deterrence	Safeguards used to scare or frighten potential intruders.
Prevention	Safeguards used to prevent intrusion or compromising safeguards.
Limitation	Safeguards used to limit the damage an intruder can cause.
Correction	Safeguards used to correct the damage that has been done.
Recovery	Safeguards used to recover from serious damage that has been done.
Monitoring	Safeguards used to monitor other safeguards or the environment.
Awareness	Safeguards used to create a secure mindset in people.

4.6 Resolved example

So the experts advised the apt to the effect of the safeguards according to the above.

The apt thinks again about the lock on the door and how he could apply different safeguards with different effect.

- Prevention. The lock on the door is just prevention.
- Detection. He needs some kind of burglar alarm or a guard to check the lock.
- Deterrence. As a deterrence safeguard, the apt puts a sign on the outer wall of the monastery stating that the monastery is safeguarded by locks, dogs and guards.
- Limitation. By using several different locks the consequences of breaking one lock are limited.
- Correction. The guards are provided with the keys as well, so they can lock the door as well in case someone forgot.
- Recovery. The apt agrees with the local blacksmith that he can provide the monastery either with a new lock (if the old one is broken) or with new keys upon request.
- Monitoring. The guards will check every lock every hour.
- Awareness. All monks are trained to lock the door when they leave the monastery.

From now on the apt knows what he's talking about regarding the effect of safeguards.

4.7 Consequences

Benefits:

- It is easy to remind anyone that you not only need prevention.
- This paper sets terminology on the effect of IT security.
- The paper provides a comprehensive overview based on extensive knowledge of and experience with international standards.
- The security aspects can be understood, remembered and addressed very well.
- It's easy to refer to and it's free 😊

Pitfalls:

- The better your prevention safeguards are, the lesser work there is to do for the rest. This might lead to decreasing attention or even to abolishing of the safeguards, since there is nothing to do.
- Since IT security knows a lot of terminology, with synonyms and homonyms, it is quite easy to frustrate communication by using an extensive vocabulary.
- A comprehensive overview does not and cannot replace books and standards. Do not assume that you know all there is to now after reading this paper.

4.8 Implementation Issues

Prevention is most effective: prevention is better than cure. In practice about 90 % of all safeguards is in the category of prevention.

Especially on correction and recovery there is a lot of alignment necessary with regular incident management. Since these colleagues are not always as security minded as we are, miscommunication and lack of correction or recovery is a risk.

ISO1335 states 8 different effects of safeguards. In practice, it is not easy to explain or work with such a large set. We usually prefer a smaller set, although we still know the complete set if necessary. The smaller set is: Prevention, Detection, Limitation and Recovery.

4.9 Related Patterns

All patterns in the Taxonomy Pattern Language are strongly related to each other:

- The pattern “The Goal of Security” assures that we are aware of the complete set of security goals and what definitions come along.
- The pattern “The Nature of Safeguards” assures that we are aware of the different natures of safeguard and shows how these support each other.
- This pattern assures that we are aware of the different effects of safeguards and shows how these add to each other.

The discussion paper [Schumacher] introduced the idea to extract patterns from standards.

4.10 Known Uses

The authors used this pattern in several security architecture projects. In these projects we used this material to explain to others (from project manager to designer) the essence of IT security within 5 minutes.

4.11 References

- | | |
|---------|--|
| [7498] | ISO 7498-2:1989, Information processing system – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture. |
| [13335] | ISO/IEC TR 13335-1:1996, Information Technology – Guidelines |

for the management of IT Security – Part 1: Concepts and models
for IT Security.

[17799] ISO/IEC 17799-1:2000, Information Technology – Code of
Practice for Information Security Management – Part 1.

[Schumacher] Security Patterns and Security Standards by Markus Schumacher,
Darmstadt University of Technology; 11 June 2002.