INTEGRATING SECURITY INTO SYSTEMS DEVELOPMENT

Ulrika Evertsson, Urban Örthberg, and Louise Yngström
Department of Computer and Systems Sciences
Stockholm University/Royal Institute of Technology
Sweden

Abstract: There are suggestions that security may be an integrated part of any systems development method. One way to do this is to use a meta-methodology. With this theory as a leading star, a model, called the Pentagon Model is built as a bridge between The Systems Lifecycle (SLC) method and a company's security tools. The model describes what to do in order to develop more secure information systems, rather than a detailed description on how to do to succeed in this work. The level of security in the systems is determined by the context and will differ from case to case. This demands a flexible tool for integrating appropriate security solutions for each system. The Pentagon Model is designed to work together with the SLC, an approach used by most developers today. This way we eliminate the re-engineering of the model to fit in different projects, which might be necessary with a fixed and static model.

Key words: secure information system development, security awareness in development processes

1. INTRODUCTION

This paper is part of an action-oriented research carried out in a local division of a global IT-company mainly dealing with information systems development. Our mission was to improve the security awareness among the staff and to integrate this awareness in the whole system development process. The full report [Evertsson&Örthberg, 2002] includes organizational considerations and introduces a communication role to link the development and security departments. Our work was mainly influenced by researchers suggesting security aspects need to be taken account of already in the

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35691-4_52
D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

process of developing IS-systems [Baskerville, 1988, 92, 94, 2001, Siponen, 2001a-d, Siponen&Baskerville, 2001], and the facts that security needs to take account of business needs, stakeholder interests, and system contexts in a holistic approach [Magnusson, 1999, Yngström,1996, Fillery-James, 1999]. Our model, the Pentagon Model, can be deduced in particular from the IDEAL Approach within the SSE-CMM [SSE-CMM, 1999] and Fillery-James' Orion Strategy [Fillery-James, 1999] with some sub steps influenced by the local System Life Cycle, SLC, method. Even if Orion and IDEAL do not concern systems development in particular, they contribute essential steps in the process of creating secure systems. Together they complement each other in the Pentagon Model, as can be seen from table 1.

Table 1: The steps of the Pentagon Model derived from the Orion Strategy and the IDEAL Approach. Input and Output illustrates different areas to apply each method.

Systems Project/ Changes IN	Input concerning Information Security IN	Stimulus for change IN
The Pentagon Model	**The Orion Strategy**	**The IDEAL Approach**
0 – Reconnaissance	1 – Possible Security Vulnerability	1 – Initiating
1 – Current State	2 – Analyze Current Security Situation	2 – Diagnosing *Characterize Current and desired states*
2 – Ideal Solution	4 – Model Ideal Information Security Solution	
3 – Establish Solution	3 – Analyze Information Classes and sensitivity 5 – Compare Ideal Solution with Current Security 6 – Identify & Analyze Measures to Fill Gaps	2- Diagnosing *Develop Recommendations* 3 – Establishing
4 – Design & Produce	7 – Establish and implement Security Plan	4 – Acting
5 – Evaluate		5 – Learning
OUT Secure Information Systems	OUT Secure Information in Organizations	OUT Systems Security Engineering

The Pentagon Model is a compact model compared to the forerunners. This way we believe it to be easy to grasp and more user friendly. This approach was chosen since our sponsor required a tool to be used on a daily basis, not one that will be ignored due to its' complexity.

Simplifying the predecessors' outline may be understood as we are trying to take shortcuts, which may damage the scope of the models. This also implies a deteriorated quality of the Pentagon Model. We have considered

this and feel that we incorporate all essential parts in a way suited for systems development. From table 1 it is also obvious that we have not left anything out, all steps of the Orion Strategy and the IDEAL Approach are included and influence the Pentagon.

2. VISUAL DESIGN

The visual design of the Pentagon Model as seen in Figure 1 is strongly influenced by the Orion Strategy. Some of the differences are that we have chosen a more symmetric shape and turned the steps around in a clockwise direction. The steps of The Pentagon Model are also fewer than in the Orion Strategy, which is an intellectual, rather than visual, influence from the IDEAL approach.

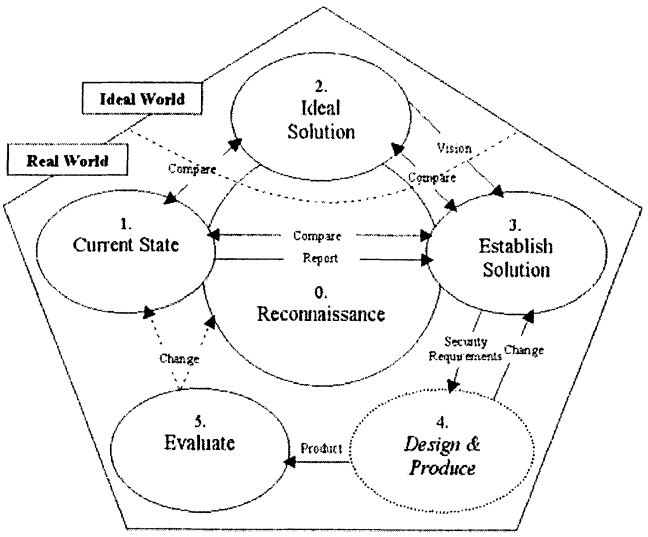

Figure 1. The Pentagon Model

One strong influence from the Orion Strategy is the concepts of an Ideal and a Real World, the visions produced in the Ideal world are essential to generate a well thought out security solution [cf. Fillery-James, 1999 p.138f]. Fillery-James also illustrates the iteration between the Real World and the Ideal World in her model. In the Pentagon we have tried to clarify this iteration by double pointed arrows between the steps 1,2 and 3. The rest of the arrows illustrate the output from each step as the input for the next. Steps 1,2 and 3 are also directly influenced by the findings in step 0, Reconnaissance, which is shown by the overlap of these steps. The fourth step *Design & Produce* is an inactive step, which consists of support for the designers and developers. A dashed border illustrates this.

3. THE STEPS OF THE PENTAGON MODEL

Below, each step of the Pentagon Model will be presented in detail. We use a systems approach where the inputs, processes and outputs of each step are described. This way we capture all the sub steps in each step and visualize the building blocks of the Pentagon Model and the connections between them.

As indicated in Figure 1, an indispensable approach is to iterate the model in general and the steps 1 through 3 in particular. We recommend that the steps 2 and 3 be completed at least twice, but ideally three times. This since it may be hard to grasp all important information in a single session [Modeling Specialist, 2001]. While performing this iteration, an on going comparison to the results of step 1 is essential in order not to loose focus on the current state and its' potential restrictions. There may also occur some iteration between the inactive step 4 and the previous steps and also between step 5 and the steps 0 and 1, in these cases the iteration will always be due to changes. Another general issue of importance is that the steps of the Pentagon Model have to be fixed at some point, in order to continue with the process. When this fixation occurs is dependant of the situation, but the iteration may generate a sense of when this should be done.

3.1 Step 0 - Reconnaissance

The thought behind this naming is that by reconnoitering the customers *Business Needs* and the *Systems Context* and conducting a *Risk Analysis* based on a *Security Policy*, a *Security Base* will be outlined. The security base must be anchored with the project management and the customers by

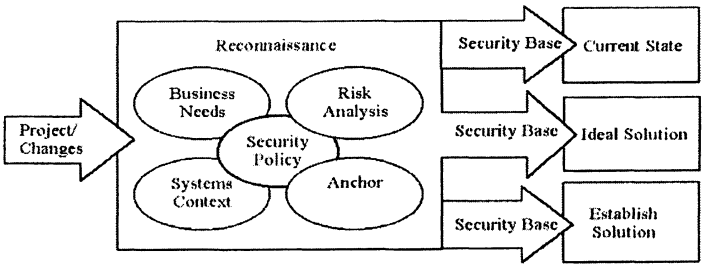

Figure 2. The Reconnaissance Step

convincing them of the severity of the risks in the thought system. The Reconnaissance step, see figure 2, is the minimum security work that has to be done in every systems development project.

The result, the Security Base, is the foundation for the rest of the process of using the Pentagon Model. It directly influences the steps *Current State*, *Ideal Solution* and *Establish Solution*. These steps formulate the *Security Requirements* that is the input to the *Design* step, which determines how the secure system will be built.

This reasoning is illustrated in Figure 3, where the Reconnaissance step is the foundation on which the Pentagon steps are built and the Security Base is the beam that holds it.

Figure 3. The Stairway to Security

By introducing this step in the initiation of a systems development process the developing company can highlight the risks of information systems in general and the thought system in particular. It is then up to the customers to decide whether to live with the risks and the potential damage or to take measures to prevent them from occurring. *Business Needs*: This step is inherited from the studied company's SLC and has the aim to determine the actual needs to be filled within the scope of the commission. A Business Need is a problem or opportunity within the business, which consists of one or more needs. These determine the type of system needed to fulfil the needs. The identification of the Business Needs will also aid in understanding the impact of the thought system on these needs. The focus in this step should be on security implications of the business needs. The step is carried out in cooperation with an analyst responsible for the overall business needs analysis.

Systems Context: The main goal of this step is to describe the information within the system. This description includes the different types of information, how it is communicated and who has access to it. The results define a high level description of the existing system and its environment along with their mutual influences on each other. To succeed with the reconnoitring of the systems context, a systemic approach may be useful.

Security Policy: In order to succeed in the work of developing secure IS it is imperative that the customer has a sufficient Security Policy, which is also the foundation of the next sub step Risk Analysis. The security policy

determines the levels of the information security to be implemented in the information system. The step identifies if there is an existing security policy that is sufficient. If there is no security policy or if the existing is insufficient, a new policy has to be created.

Risk Analysis: The input to this step is the findings of the previous steps Business Needs, Systems Context and especially the Security Policy. The aim of the step is to identify the threats to and the risks of the thought IS. This is best performed with a scenario method for risk analysis, such as the SBA-Scenario [DFS, 2000, Lundqvist 2001]. The result of the risk analysis is one of the main characteristics of the Security Base, but also the basis for the Anchor step. Both Orion and IDEAL introduces the risk analysis in their second steps. Since the results of the risk analysis influence every later step in the Pentagon, we have chosen to incorporate it in the Reconnaissance step.

Anchor: This is where the results of the previous steps will be mediated to the customer for decisions on further action. It is essential that the results are presented in a well formed, categorized and realistic way to convince the audience. This activity is defined as its own sub step since it is of great importance that the customer is aware of the importance of IS security [cf. Fillery-James, 1999, p.146]. The customer is also the one who decides whether or not to proceed with the Pentagon Model.

3.2 Step 1 – Current State

In this step, see figure 4, an exploration of the existing IS security is performed. Every entity of the IS, such as hardware, software and roles, are explored. The result of the exploration is analyzed and compared to the Security Base in order to locate deficiencies.

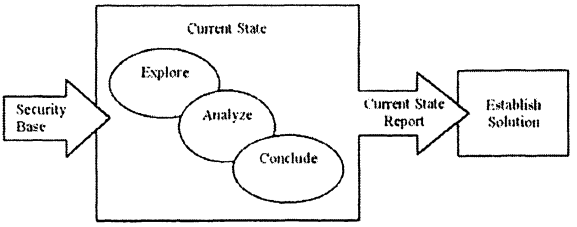

Figure 4. The Current State Step

The conclusions, regarding both sufficient and insufficient security in the existing IS, are then compiled into a Current State Report. This report is an important document, which must be considered throughout the following steps, Ideal Solution and Establish Solution. Current State may be performed with a tool for current state analysis, like the SBA-Check [DFS 2000,

Lundqvist 2001], where the Security Base is one of the parameters. The importance and rigidity of this step may vary. In new systems, where there is no previous IT, the process of this step is minimal. On the other hand, when the commission is to integrate existing and/or new systems with one another the process will be more rigid and of greater importance.

3.3 Step 2 – Ideal Solution

The input into this step, see figure 5, is the Security Base. The aim of this step is to generate a vision of an ideal security solution, without limit or constraints. The Ideal solution step should be viewed as a puzzle where all parts are needed to form a whole, which implies that no parts can stand-alone. All information derived and used should always be considered in light of how the demands for integrity, availability and confidentiality along with accountability, legitimate use and non-repudiation will affect it as required by the puzzle piece *C.I.A.* Furthermore, applying the piece *System Thinking* implies a holistic view of the situation, which is important in order to improve the solution.

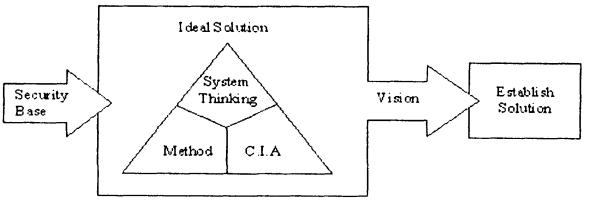

Figure 5. The Ideal Solution Step

Along with the pieces of this puzzle there are two other main ingredients that must be considered, user participation and creativity. The users hold the information on how the company in question is organized, how the work is performed, and what information should be protected within the company and, most importantly, users perceive a fixed situation differently. The users are not always aware that they possess this information and in order to retrieve as accurate and diversified information as possible, a high degree of creativity is needed by the analysts responsible for this step.

The third piece of the puzzle is *Method.* In order to complete this step it is essential to have a method that stimulates creative thinking. There are a number of different approaches of which we have chosen to suggest using *brainstorming, futuristic workshop,* or *functionality analysis* [Löfgren et al]. A common feature of these methods is that they all demand a high level of user involvement. As the step is completed, one or several visions of the ideal system solution are produced. The vision includes both the

functionality of the thought system and its security solutions. The system is described in each vision through for example, use cases that handle the different parts of the system and their subsequent functionality.

3.4 Step 3 – Establish Solution

In this step, see figure 6, four sub steps are to be performed to generate the requirements specification for an optimized solution. This involves all requirements of the thought system, including those regarding security. The order of the steps is not fixed but using the recommended order is thought to be the most appropriate.

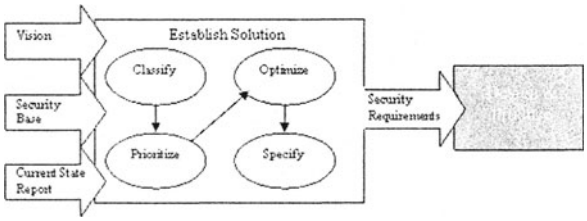

Figure 6. The Establish Solution Step

Classify: The sensitivity of information varies, which implies that different types of information need to be protected on different security levels. In order to be able to protect the information at an appropriate level, it is essential to classify each type of information.

Prioritize: In order to structure the results of the former steps of the development process it is essential to prioritize the cluster of sub-solutions generated in Ideal Solution. How this is done depends on the context. The business needs determine what solutions are the most significant. The Current State also affects prioritizing, regarding both guidance and constrains, but not to the same extent. In addition, there are a number of other constrains which have to be considered during this step. Examples of such constrains may be economical, technical and constrains of competence. These components are used to attain a reasonable ranking of the solutions.

Optimize: Optimizing the requirements involves finding the best possible solution to meet the business needs within the boundaries of the commission. To obtain this, the Security Base, the Current State Report and the Visions must be regarded and compared to each other to assure that the requirements will work together in a cooperative way. It is important to be aware of the risk that some requirements will be left out in this sub-step due to conflicts with the system. In such a case, it is crucial to have in mind that the main functions of the thought system must be fulfilled, which also includes the protection of the most important information of the IS.

Specify: In this sub-step the requirement specification is specified. This may be done in any appropriate way. Some recommendations are that the specification is clear enough to avoid misunderstandings, that the requirements are grouped in an orderly fashion and that the specification is complete.

3.5 Step 4 – Design & Produce

At this stage, the requirements of the product are defined and guide the rest of the process. In the ideal case this will be an inactive step of the Pentagon Model, a black box. On the other hand, an Information Security Analyst must be available to meet questions from designers and developers and changes to the product.

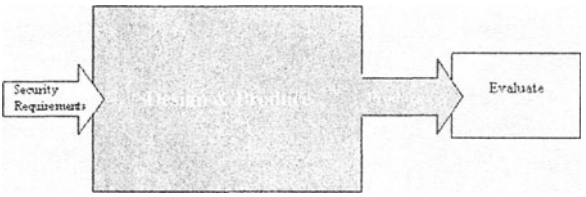

Figure 7. The Design & Produce Step

3.6 Step 5 – Evaluate

The Evaluation step may seem to be a bit misplaced, since it does not follow immediately from the other steps in the model. This is an illusion though, as the previous steps are the foundation of the products to be evaluated. It is necessary to perform evaluations throughout the systems lifecycle. The Evaluate step is applicable during or after the produce, optimize, implement, as well as the operations and maintenance, and termination-phases of the lifecycle. The sub-steps of the Evaluate step are to be executed in the order illustrated in Figure 8.

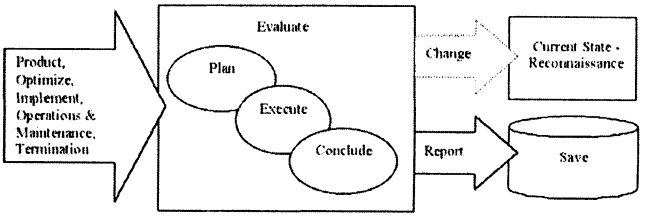

Figure 8. The Evaluate Step

In the sub-step *Plan* it needs to be determined what should be evaluated and also how this evaluation will be performed. The base for what is to be evaluated is the documentation of the preceding steps. How to perform the

evaluation may be inspired by using an evaluation method available on the market, such as the Common Criteria [CC].

During the *Execute* sub-step the evaluation is performed according to the guidelines acquired in the sub-step *Plan.* Finally, during the *Conclude* step, the results of the evaluation should be compared to the initial requirements of the system. If the results concur with the requirements then the evaluated segment is ready for release to the next phase of the system life cycle. However, if the results and requirements are not in accordance with each other, then the segment needs to be re-iterated through the Pentagon Model, either starting at step 0 or at step 1.

4. PENTAGON IN SYSTEMS LIFECYCLE

The Pentagon Model is designed to fit into the entire systems lifecycle. In this case this means the Systems Lifecycle (SLC) and the other methods in our sponsor's Framework for Global Systems Solutions, FGSS. However, since the SLC is more or less compatible with the standard Life Cycle Model, the Pentagon Model is thought to fit with any such lifecycle model.

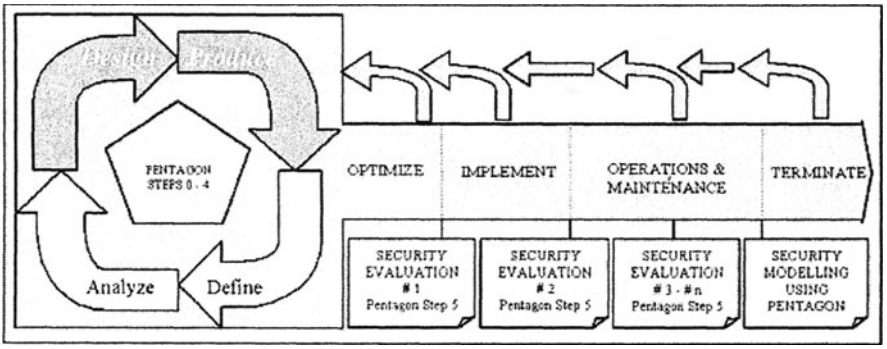

Figure 9. The Pentagon Model incorporated in the entire Systems Lifecycle

Figure 9 illustrates how the steps of the model fit with the framework and any other systems lifecycle. This figure shows the first five steps of the model are parts of the SLC that contains the steps Define, Analyze, Design and Produce. The emphasis of the Pentagon Model first four steps is to use them in the first two steps of the SLC, while step five of the model is connected to the rest of the lifecycle. The fifth step of the Pentagon Model, Evaluate, has the aim to detect insufficiencies in the security controls of the system, to report deficiencies and to evaluate corrections. This work must be done throughout the lifecycle to assure that the right level of security is applied. There are four checkpoints where this step must be performed. After the Produce step the first mandatory evaluation should be conducted to find

out if the general security requirements are met. Connected to the optimization of the system is an evaluation of the entire security solution. So far, the system and its security solutions have been tested in a developmental environment.

Now it is time to implement the system into its real environment, which may cause unforeseen problems. The third evaluation is therefore performed to investigate this. The fourth mandatory checkpoint consists of a complete session with the Pentagon Model and is performed in connection with the termination of the system. This has to be done to assure that all assets of the system are treated in a secure manner during and after the termination of the system. During the operations and maintenance phase of a systems lifecycle, evaluations should be performed with regularity. What this means exactly is dependant of the complexity of the system and available budget, its environment and the confidentiality of the handled information. Any evaluation may call for changes in the system, which is illustrated with the left-pointing arrows in Figure 9. However, every change does not imply a full session with the Pentagon Model. Small problems in the system might be corrected with minor interference. When major or medium changes are called for, we recommend entering the Pentagon Model. The stage of the lifecycle decides in what part of the model to enter.

5. CONCLUSIONS

The Pentagon Model is a meta-model derived from several predecessors designed to work with a general systems lifecycle model. Our model combines the use of the aforementioned tools with a high level of user participation, to ensure that the security requirements of the system are in accordance with the security needs. The Pentagon Model also features an evaluation step to be used, not only during the development of a system, but throughout the entire systems lifecycle. However, the emphasis is on that the model is activated in the beginning of the developmental process. This ensures that the security requirements are incorporated into the entire system and also that the duality in systems development is reduced.

References

[Baskerville 2001] – Baskerville, R.: E-mail interview. 2001/10/04

[Baskerville, 1988] – Baskerville, R.: Designing Information Systems Security, John Wiley & Sons, Chichester, 1988

[Baskerville, 1992] – Baskerville, R.: "The Developmental Duality of Information Systems Security", J of Mgm Systems 4 (1) 1992, pp. 1-12

[Baskerville,1994] – Baskerville, R.: "Information Systems Security Design: *Implications for Information Systems Development*", Computing Surveys 25 (4), December 1994 pp. 375-414

[CC] – Common Criteria, http://www.commoncriteria.org, 2001/10/23

[DFS 2000] SBA Scenario 4.0, SCS 2000

[Evertsson&Örthberg, 2002] – Evertsson, U& Örthberg, U: "Bringing Security to Software. Introducing the Pentagon Model", DSV, 2002

[Fillery-James, 1999] – Fillery-James, H: "A Soft Approach To Management of IS", PhD, School of Public Health, Curtin University of Technology, Perth, 1999

[Lundquist 2001] – Lundquist, Mats: Interview and demonstration of SBA Scenario, Dataföreningen, 2001/10/31

[Magnusson 1999] – Magnusson, C: Hedging Shareholder Value in an IT-dependent Business Society – *the Framework BRITS*, PhD, DSV, 1999

[Modelling Specialist 2001] – In dept interview regarding the Pentagon Model, the FGSS and the methods used in modeling, 2001/09/28

[Siponen 2001a] – Siponen, M.: "On the Scientific Background of Information Security Management Standard: a Critique and an Agenda for Further Development", 2nd Annual Int. SSE Conference, 28 Feb – 2 March 2001, Orlando, Florida, USA

[Siponen & Baskerville 2001] – Siponen, M&Baskerville, R: "A New Paradigm For Adding Security Into IS Development" in Advances in Information Security Management & small Systems Security. Eloff, J., Labuschange, L., von Solms, R., and Dillon, G. (Eds), Kluwer Academic Publishers, 2001

[Siponen 2001b] – Siponen, Mikko T.: "A Paradigmatic Analysis of Conventional Approaches for Developing and Managing Secure IS – *Implications for Research and Practice*", 6th International Conference on Information Security, 11-13 June 2001, Paris, France

[Siponen 2001c] – Siponen, Mikko T.: "An Analysis of the Recent IS Security Development Approaches, In G. Dhillon: IS Mgt – Global Challenges in the Next Millennium, Idea Group Publishing, 2001

[Siponen 2001d] – Siponen, M: E-mail interview, 2001/10/04

[SSE-CMM 1999] – "*SSE-CMM – Model Description Document, Version 2.0*", CMU/SEI, Carnegie Mellon University – Software Engineering Institute, Pittsburgh, 1999

[Yngström 1996] – Yngström, L: "A Systemic-Holistic Approach to Academic Programmes in IT Security", PhD, DSV, Kista, 1996