Refining the pattern-based reference model for electronic invoices by incorporating threats

Michael Netter*, Eduardo B. Fernandez†, Günther Pernul*
*Department of Information Systems
University of Regensburg
93040 Regensburg, Germany
Email: {michael.netter, guenther.pernul}@wiwi.uni-regensburg.de
†Department of Computer Science and Engineering
Florida Atlantic University
Boca Raton, FL, USA
Email: ed@cse.fau.edu

***Abstract*—Almost every company needs to process invoices to either claim money from their customers or to pay for products or services. Although companies are allowed to electronically process their invoices, most of them still rely on the paper-based invoice process. Within this paper we built upon existing work to develop a methodology for defining a reference model for the electronic invoice based on security patterns. This paper identifies threats of the e-invoice process in order to create a context for the security problem, which allows us to refine our methodology.**

***Keywords*-electronic invoice; misuse activities; threat identification; security patterns**

I. Introduction

A recent study [1] of electronic invoices indicates a potential for savings up to 70 percent compared to paper-based invoices. Yet, implementing a valid and particularly secure electronic invoice process is a complex task and thus the majority of companies and especially small and medium-sized enterprises (SMEs) still rely on paper-based invoice processes. In earlier work [2] we have identified the main obstacles that hamper the comprehensive adoption of e-invoices.

To address this problem it is necessary to develop a reference model for the electronic invoice process. A reference model for the electronic invoice should provide guidance for implementing valid e-invoice solutions. Up to now and to the best of our knowledge no such reference model exists. In order to arrive at a reference model our approach aims to use security patterns, as they embody expert knowledge to address the security related aspects of such a reference model. The goal is to find a consistent set of security patterns, known as a pattern system which help to create a secure model for e-invoices.

In [2] we have proposed a methodology to discover a set of known patterns and thereby support the development of a reference model for the electronic invoice process. In this paper we try now to improve our methodology. The refinement consists of two parts. First, the security aspects of the electronic invoice process are approached from the view of an attacker. Therefore, each activity is analyzed to find security vulnerabilities which might be exploited. Second, the threat model is used to refine our work towards an electronic invoice reference model. In the following we use the definitions of threat and misuse activity interchangeably.

The remainder of this paper is structured as follows. In Section II we discuss related work. A detailed threat analysis for the electronic invoice process is presented in section III. Within section IV we introduce the concept of context information, that describes the environment of the security problem. Section V presents our approach to refine our existing e-invoice classification. Section VI concludes the paper with an outlook on future work.

II. Related Work

Security patterns were first introduced by Yoder et al. [3]. However up to now only few papers exist that consider them for improving the electronic invoice process exist ([4][2]). Fernandez et al. proposed a semantic analysis pattern to capture the fundamental aspects of invoice processing. Several approaches exist for threat-modelling in order to elicit, classify and stop threats (for example [5][6]). The contents of invoices can be found in [7], [8], and [9]. Neither of them describes security aspects.

III. E-INVOICE THREAT IDENTIFICATION

Creating a reference model for the electronic invoice requires analyzing the problem domain from different perspectives. Within our previous work we took on the white-hat role, i.e. we approached the problem by regarding the affected security objectives. However, such a single-view based model is not sufficient as it leaves out the view of an attacker. Therefore, in this paper we take the position of an attacker trying to circumvent the security mechanisms.

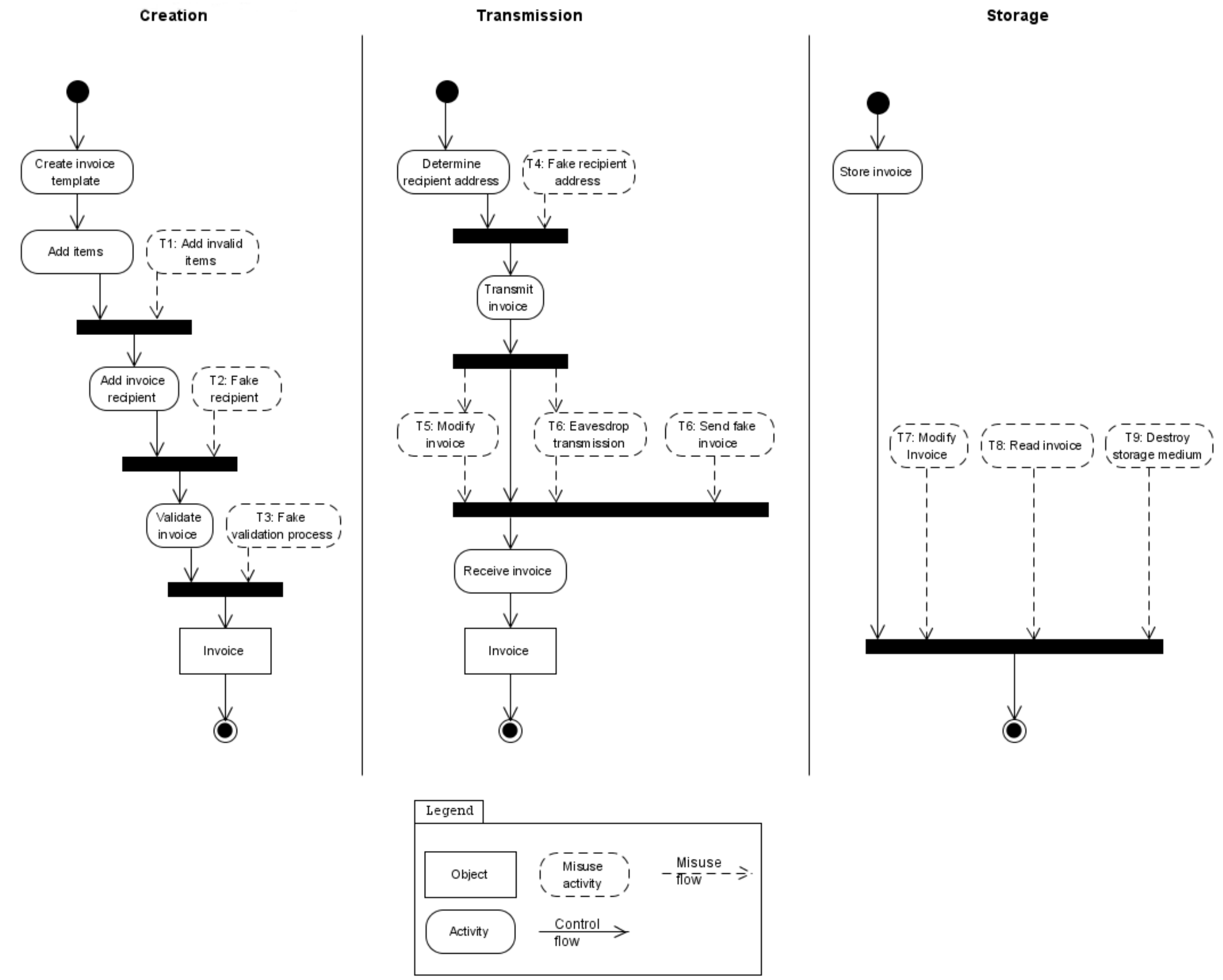


Figure 1. Extended activity diagram for the partitioned electronic invoice process

In order to find all threats a systematic approach is necessary. We apply the misuse activities approach proposed in [10] which uses UML activity diagrams to represent the data and control flow. The activity diagrams are extended with further elements which allow for the representation of misuse activities.

To ease the identification of threats for the electronic invoice process we split the process into three parts:

- **Creation**: Refers to the process of creating a valid e-invoice. This includes measures to ensure a secure, auditable creation process as well as the protection of the integrity of an e-invoice.
- **Exchange**: Refers to the process of sending, transmitting and receiving e-invoices.
- **Storage**: Refers to the process of persistently storing an e-invoice and all attachments that are required to verify the integrity of an e-invoice.

Partitioning the electronic invoice into process steps allows for a detailed investigation of each flow of activities in order to discover all possible ways to subvert an activity. The misuse activities in Figure 1 are denoted by dashed rounded rectangles while dashed connecting lines represent misuse flows that indicate how the flow of control may be modified. Figure 1 shows three UML activity diagrams, each for one part of the e-invoice process steps. Furthermore for each control and data flow, the possible misuse activities are depicted illustrating unambiguously the threats for the specific activity.

Focusing on the creation process, adding items to the electronic invoice template may be subverted by an attacker changing the total sum of the invoice the customer has to pay and thus compromising the integrity of the invoice. Furthermore, an attacker that is able to modify the creation process can additionally alter the recipient, which compromises both the confidentiality and the integrity of the invoice. In order to detect such modifications, Fernandez et al. [4] propose to add an invoice validation activity before the invoice is finalized. However if the attacker is an insider he might be able to fake or even circumvent this validation process, but this is out of scope of our attacker model.

The threat analysis is also performed for the transmission process. It reveals several activities within the control and data flow that are vulnerable. First, the attacker might be able to change the address of the invoice recipient. If, for instance, the invoice is sent by e-mail, the attacker might be able to alter the e-mail address of the recipient if no security mechanisms are in place. Furthermore the transmission itself is vulnerable to several attacks, since it is usually carried out using some insecure channel like the internet. An attacker can eavesdrop the communication by performing a man-in-the-middle attack, which allows him to obtain knowledge of the content of the invoice and thus violate confidentiality. With no protection mechanisms in place, an attacker can furthermore modify the content of the invoice, which corrupts the invoice's integrity. Additionally, the invoice might be intercepted and a fake invoice is sent to the recipient.

The storage part is the third part of the partitioned electronic invoice process and its security is of major importance mostly due to legal requirements. There are three main misuse activities an attacker can perform. First, the invoice can be modified and thus the integrity of the invoice is corrupted which endangers the VAT (value-added tax) refund for this invoice. The second threat concerns confidentiality. An attacker may be able to obtain the content of the invoice which may lead to a competitive disadvantage. Furthermore the invoice may be deleted and is therefore no longer available which also endangers the VAT refund.

IV. Threat context definition

Once the threats for all parts of the electronic invoice process are discovered, policies must be defined to stop those threats [1]. Having both the identified threats and the corresponding policies, this allows to define the context of the security problem. While the threats can be related to the problem section of a security pattern the policies provide a solution. Thus the context of a security problem can be denoted as

$$< context >= (< threat >, < policy >) \tag{1}$$

The context of a security pattern is defined as the environment where the pattern can be applied. Context information can be extracted from both the problem and the solution of a security pattern. Thus we define the context of a security pattern as

$$< context >= (< problem >, < solution >) \tag{2}$$

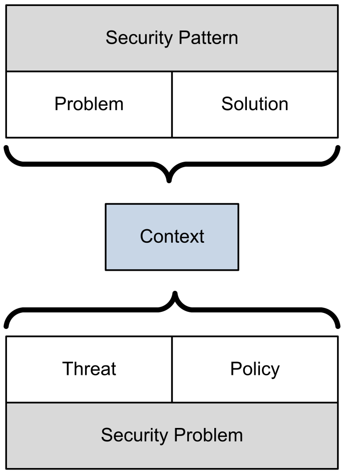


Figure 2. Context definition

Figure 2 depicts the relation between a security problem, described by threats and policies and security patterns, represented by the problem and the solution section. Both concepts create an identical context.

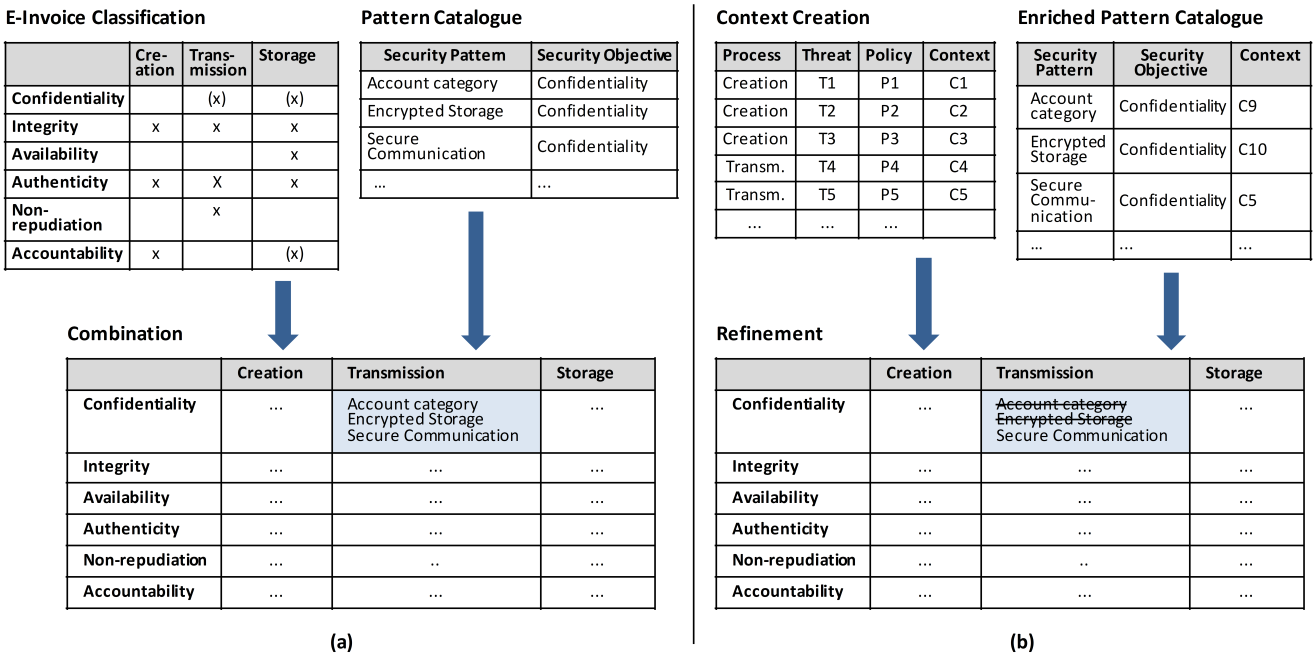
V. Reference model refinement

In our previous work [2], we analyzed the security aspects of the electronic invoice process, focusing on the affected security objectives. There we proposed an approach to relate security objectives to security patterns, leading to a set of patterns that can be used to realize a solution for the security problem. However, using security objectives as the only classification criterion leads to a large set of possible security patterns. In order to refine this set of security patterns, we consider the threats for the electronic invoice, i.e. taking the view of an attacker. We have identified the important threats for the electronic invoice process and defined policies to prevent possible attacks. This information enables us to create a context for each security problem.

In the following we use this context information to refine our existing set of security patterns for the electronic invoice.

Figure 3 (a) shows an extract of our classification scheme, presented in [2]. Therein security objectives are used to map appropriate security patterns to the e-invoice processes. It can be seen, that for a single security objective and a single part of the e-invoice process there are several security patterns, that might be helpful to fulfill the objective. However some patterns a provide similar solution and in other situations, a combination of several patterns is required. Furthermore some patterns admittedly fulfill the security objective but the context is different and thus the patterns are not applicable for the electronic invoice.

In order to refine the selection of security patterns and thus improving the development of a reference model we conduct a threat analysis of the e-invoice process. The approach ist depicted in Figure 3 (b).



E-Invoice Classification

	Cre-ation	Trans-mission	Storage
Confidentiality		(x)	(x)
Integrity	x	x	x
Availability			x
Authenticity	x	X	x
Non-repudiation		x	
Accountability	x		(x)

Pattern Catalogue

Security Pattern	Security Objective
Account category	Confidentiality
Encrypted Storage	Confidentiality
Secure Communication	Confidentiality
...	...

Combination

	Creation	Transmission	Storage
Confidentiality	...	Account category Encrypted Storage Secure Communication	...
Integrity	...	...	...
Availability	...	...	...
Authenticity	...	...	...
Non-repudiation	...	..	...
Accountability	...	...	...

(a)

Context Creation

Process	Threat	Policy	Context
Creation	T1	P1	C1
Creation	T2	P2	C2
Creation	T3	P3	C3
Transm.	T4	P4	C4
Transm.	T5	P5	C5
...	...	...	

Enriched Pattern Catalogue

Security Pattern	Security Objective	Context
Account category	Confidentiality	C9
Encrypted Storage	Confidentiality	C10
Secure Commu-nication	Confidentiality	C5
...	...	...

Refinement

	Creation	Transmission	Storage
Confidentiality	...	~~Account category~~ ~~Encrypted Storage~~ Secure Communication	...
Integrity	...	...	...
Availability	...	...	...
Authenticity	...	...	...
Non-repudiation	...	..	...
Accountability	...	...	...

(b)

Figure 3. Refinement

First, for each threat an appropriate policy must be defined that stops the threat. The combination of a threat $T1$ and a policy $P1$ defines a context $C1$. For instance, in order to stop the threat *T6: Eavesdrop transmission* an appropriate policy might state that *...every communication must be encrypted using a secure algorithm.* Since threats can be related to the problem section and policies to the solution section of security patterns it is possible to determine a context for each security pattern. Thus in order to refine the selection of security patterns shown in Figure 3 (a), the context C is determined for each security pattern of the pattern catalogue. For example, the security pattern *Secure Communication* [11] has the context $C5$ which is identical with the context of the threat/policy combination $T5/P5$ derived from the threat analysis. Thus the pattern is likely to be appropriate to solve the security problem described by threat $T5$.

The refinement step aims to improve the classification scheme developed in [2]. This requires to analyse the set of security patterns for each part of the the e-invoice process. This step is depicted in Figure 3 (b). Due to space constraints only the refinement of the set of security patterns for the transmission process concering the security objective confidentiality is shown. The result of the selection step executed in [2] shows a set of three security patterns. While all security patterns address the security objective confidentiality, the context of two patterns is not suitable. The *Account category* pattern [12] is focused on the length of passwords and the *Encrypted storage* pattern [13] provides a solution to store confidential information on a storage medium. Thus those two security patterns can be removed from the set leaving the pattern *Secure Communication*. As described in the previous paragraph, the context of *Secure Communication* is suitable to stop threat $T5$.

The refinement step is repeated for every field of the classification matrix, i.e. for every set of patterns. As a result, the number of security patterns that are suitable for solving the security challenges of the electronic invoice process is reduced. Using the refined classification scheme shown in 3 (b) the complexity for deriving a pattern system is reduced, which is due to future work.

VI. Conclusion

In this paper we have identified the threats of the electronic invoice process by extending the UML activity diagram with misuse activities. We use the threats to introduce the concept of the context of a security problem and show how to define the context for security patterns. The context information enables us to refine our classification scheme for the electronic invoice developed in [2] and thus improve our methodology to develop a reference model.

However the approach relies on an existing catalogue of security patterns that is enriched with context information, which must be generated manually. Therefore our future work includes the analysis of methods to automatically derive the context information of our security pattern catalogue. Furthermore it is required to derive a pattern system from our classification scheme depicted in Figure 3 in order to derive a reference model for the security related aspects of the electronic invoice process.

Acknowledgment

This work is partly funded by the Bavarian Ministry for Economic Affairs, Infrastructure, Transport and Technology and carried out within the SecPat project (Contract No. IUK292/002).

References

[1] PricewaterhouseCoopers, "Study on the requirements imposed by the member states, for the purpose of charging taxes, for invoices produced by electronic or other means," 1999.

[2] M. Netter and G. Pernul, "Integrating security patterns into the electronic invoicing process," in *Proceedings of the 3rd International Workshop on Secure systems methodologies using patterns*, 2009.

[3] J. Yoder and J. Barcalow, "Architectural patterns for enabling application security," in *Proceedings of the Pattern Languages of Programs Conference*, 1997.

[4] E. B. Fernandez and X. Yuan, "An analysis pattern for invoice processing," in *Proceedings of the 16th Conference on Pattern Languages of Programs*, 2009.

[5] Microsoft Corperation, "Microsoft threat analysis and modeling tool," 2006.

[6] E. B. Fernandez, M. VanHilst, M. M. Larrondo-Petrie, and S. Huang, "Defining security requirements through misuse actions," in *IFIP Workshop on Advanced Software Engineering*, pp. 123–137, 2006.

[7] M. Fowler, *Analysis Patterns: Reusable Object Models*. Addison-Wesley Professional, October 1996.

[8] D. C. Hay, *Data Model Patterns: Conventions of Thought*. New York, NY, USA: Dorset House Publishing Co., Inc., 1996.

[9] L. Silverston, W. H. Inmon, and K. Graziano, *The data model resource book: a library of logical data models and data warehouse designs*. New York, NY, USA: John Wiley & Sons, Inc., 1997.

[10] F. A. Braz, E. B. Fernandez, and M. VanHilst, "Eliciting security requirements through misuse activities," in *Proceedings of the Second Workshop on Secure Systems Methodologies using Patterns*, 2008.

[11] B. Blakley, C. Heath, and Etc, "Security design patterns," tech. rep., The Open Group Security Forum, 2004.

[12] D. Riehle and J. Bergin, "Password patterns," in *Proceedings of the 17th European Conference on Pattern Languages of Programs*, 2002.

[13] D. M. Kienzle, M. C. Elder, D. Tyree, and J. Edwards-Hewitt, "Security patterns repository version 1.0," 2002.