Security Requirements—A Field Study of Current Practice*

John Wilander and Jens Gustavsson
Dept. of Computer and Information Science, Linköpings universitet
{johwi, jengu}@ida.liu.se

Abstract

The number of security flaws in software is a costly problem. In 2004 more than ten new security vulnerabilities were found in commercial and open source software every day. More accurate and consistent security requirements could be a driving force towards more secure software. In a field study of eleven software projects including e-business, health care and military applications we have documented current practice in security requirements. The overall conclusion is that security requirements are poorly specified due to three things: inconsistency in the selection of requirements, inconsistency in level of detail, and almost no requirements on standard security solutions. We show how the requirements could have been enhanced by using the ISO/IEC standard for security management.

Keywords: security requirements, non-functional requirements

1 Introduction

According to statistics from CERT Coordination Center, CERT/CC, in year 2004 more than ten new security vulnerabilities were reported per day in commercial and open source software [2]. In addition, the 2004 E-Crime Watch Survey respondents say that e-crime cost their organizations approximately $666 million in 2003 [5].

For consumers of software the security of the products they use relies heavily on the security requirements specified for the products. If these requirements are poorly specified there is nothing saying that the producers will strive for security. Instead, costs and time will be focused on meeting the other requirements, and security issues may be left for maintenance in the infamous *penetrate and patch* manner [16].

To build more secure software, accurate and consistent security requirements must be specified. We have investigated current practice by doing a field study of eleven requirement specifications on IT systems being built 2003 through 2005. To evaluate the outcome we have looked into documentation of security requirements from the requirements engineering community as well as from the security community. Requirements found in the specifications have been categorized into security areas and divided into functional, non-functional, and assurance requirements. The ISO/IEC standard for security management has been used as an example of how a standard could help to specify better security requirements.

The rest of this paper is organized as follows. In Section 2 we look at how security requirements have been defined within the requirements engineering community and the security community. Next, Section 3 discusses security testing to verify that security requirements have been met. Section 4 presents and discusses our field study of eleven requirements specifications and what they specify in terms of security. Finally, Section 5 concludes our work.

2 Security Requirements

A subgroup of software requirements is security requirements. A lot of work and research has been done to define and standardize security requirements, especially by military organizations. Here we look at (examples of) how security requirements are defined within the requirements engineering (RE) community and the security community.

2.1 From a RE Point of View

Within requirements engineering security is often conceived as a non-functional requirement along with such aspects as performance and reliability, and is generally considered hard to manage [1, 3, 4, 6].

There are several (partially overlapping) definitions of functional and non-functional requirements. The one used in this paper is based on the IEEE definition [8], Thayer and Thayer's glossary [14], extended by Burge and Brown [1].

*This work has been supported by the national computer graduate school in computer science (CUGS) commissioned by the Swedish government and the board of education, Vinnova 2GAP (Second Generation Application Provisioning), and EU EASYCOMP (Easy Composition in Future Generation Component Systems).

Functional Requirement. A functional requirement (*FR*) defines something the system must do, capturing the nature of the interaction between the component and its environment. A FR must be *testable*, which means it is possible to demonstrate that the requirement has been met by a test case resulting in pass or fail [1, 8].

Non-Functional Requirement. A non-functional requirement (*NFR*) is a software requirement that describes not what the software will do, but how the software will do it. NFRs restrict the manner in which the system should accomplish its function. NFRs tend to be general and concern the whole system, not just some parts [1, 14].

In their paper on the future of software engineering Premkumar Devanbu and Stuart Stubblebine discuss security requirements. They define them as:

Security Requirement. A security requirement is a manifestation of a high-level organizational policy into the detailed requirements of a specific system [6].

2.2 From a Security Point of View

One of the seminal documents on security requirements is the *Common Criteria*, or *CC*. The CC is a standard and is meant to be used as the basis for *evaluation* of security properties of IT systems [12].

> "The CC will permit comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation."

Following the CC standard, consumers of software produce a *Protection Profile* that identifies desired security properties of a product. The Protection Profile is a list of security requirements. Producers on the other hand create a *Security Target* that identifies the security-relevant properties of the software. A Security Target can meet one or more Protection Profiles. CC distinguishes between two types of security requirements—functional and assurance:

Security Functional Requirement (CC). Security functional components express security requirements intended to counter threats in the assumed operating environment. These requirements describe security properties that users can detect by direct interaction with the system (i.e. inputs, outputs) or by the system's response to stimulus.

Security Assurance Requirement (CC). Requiring assurance means requiring active investigation which is a process requirement. Active investigation is an evaluation of the IT system in order to determine its security properties. Common Criteria lists what can be done in terms of assurance through evaluation. We highlight a few things here to give an example of what these requirements can look like:

- Analysis and checking of process(es) and procedure(s);
- checking that process(es) and procedure(s) are being applied;
- analysis of functional tests developed and the results provided;
- independent functional testing; and
- penetration testing.

Another relevant standard is the *ISO/IEC 17799 Information technology—Code of practice for information security management* [9]. The section on "Systems development and maintenance" includes ten pages specifying requirements and explaining considerations for techniques such as input validation, encryption, and security of system files.

The ISO/IEC standard does not discuss functional, nonfunctional, or assurance requirements as such.

3 Security Testing

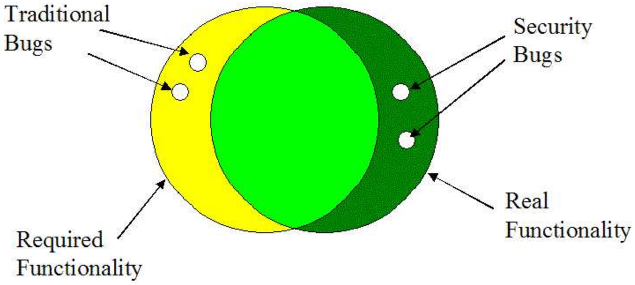

Figure 1. Finding security bugs through testing often means testing for side-effects and functionality outside the requirement specification.

Closely related to requirements is testing. If something is considered a requirement there needs to be some way to verify that it has been met. This can be done with testing where the outcome is pass or fail.

"Traditional" bugs are deviations from the requirement specification, either by doing B when supposed to do A, or by only doing B when supposed to do A and B.

Thompson and Whittaker write about running test cases to find security bugs [15]. Such bugs often differ from traditional bugs by being hidden in side effects. Finding security bugs means finding out what the system *also* does, apart from the specified functionality. Thompson and Whittaker's Venn diagram shows this (see Figure 1).

Requirements on absence of side effects are typically non-functional. Specifying what the system must not do clearly restricts in what way the functional requirements can be fulfilled. Moreover, requirements on *testing* of side effects are not only non-functional but also a kind of security assurance requirement.

This stresses that we need non-functional requirements, and specifically security assurance requirements to specify more secure systems. As we will see later such requirements are rare in current practice (see Section 4).

4 Field Study of Eleven Requirements Specifications

We have studied eleven requirements specifications of IT systems being built 2003 through 2005. In this section we first present an overview of security areas found in the specifications, and an overview of the systems and organizations that have written the specifications. Next, we present both a summarized and a detailed categorization of all security requirements found. The categorization is done into security areas and into functional, non-functional, and assurance requirements. Finally, we discuss the outcome and reflect on potential shortcomings in the material.

On an abstract level we have categorized the security requirements into well-known security areas. A full description along with examples for each category can be found in Internet security glossaries [11, 13].

4.1 Systems in the Field Study

In our study we have taken advantage of the fact that all requirement specifications used for public procurement by Swedish Government or local authorities are public documents. The authorities are also required by law to publish their requests for tenders, and all such requests are categorized depending on the type of products or services bought. The categorization is called Common Procurement Vocabulary (CPV), which is a European standard [7].

We used a commercial database to find "Computer and related services" purchases made by Swedish Government or local authorities from January 2003 to June 2004 [10]. In Table 1 you find a summary of all security requirements found. Here is a brief description of the systems studied:

Billing (City of Jönköping). A billing system for drinking water, sewage, and garbage collection.

Accounting (Cities of Dalsland). System for handling ledgers, accounting, and budgets for five cities in the province of Dalsland.

Salary/Staff 1 (The cities of Kinda, Ödeshög, Boxholm, and Ydre). System for administration of salaries and staff within the cities.

Salary/Staff 2 (The cities of Stenungsund and Tjörn) System for administration of salaries and staff within the cities.

E-Business (The cities of Skövde, Falköping, Karlsborg, Mariestad, Tibro, Tidaholm, and Hjo). System for electronic trade and business including billing.

Defense Materiel (Swedish Defence Materiel Administration). Web-based marketplace for consulting services to the Swedish Armed Forces.

Medical Advice (The Federation of County Councils). System for managing medical advice by phone on a national level. Redirection of calls, queue management, work-flow management, medical documentation, and statistics.

Health Care 1 (Stockholm County Council). Integration platform to support personal medical information following patients between various health care organizations.

Health Care 2 (The city of Lomma). System for event handling in health care including personal medical records.

Highway Tolls (The City of Stockholm's Executive Office). Equipment, systems and services for handling environmental fees for all vehicles entering the city of Stockholm.

Hazmat (Swedish Maritime Administration). Ship reporting system managing mandatory reporting of hazardous goods, arrival, departure, and generated waste in accordance with EU directives.

4.2 Detailed Categorization of Security Requirements

In tables 2, 3, and 4 we present the complete list of security requirements found in the specifications. The list is divided into security areas and every requirement is categorized as functional, non-functional, or security assurance (subcategory of non-functional). The numbers in the table are the number of requirements found for each subcategory. For instance the "E-Business" system has four specific requirements on access control per person (see Table 2).

The security areas are conventional but the categorization relies on the fact that the authors of the specifications know how the various terms differ, for instance the difference between access control, authorization and login where we have found similar requirements in all categories.

It is important to note that these are the requirements found in the specifications, thus *not* a complete list of possible security requirements. For a complete list we refer to published standards such as Common Criteria [12] and ISO/IEC standard for security management [9].

	Billing	Accounting	Salary/Staff 1	Salary/Staff 2	E-Business	Defense Materiel	Medical Advice	Health Care 1	Health Care 2	Highway Tolls	Hazmat
Access Control/Roles	1	11	6	5	8	5	4	5	3		3
Attack Detection							2	4		3	
Backup		5	9	2			2	2			
Digital Signatures			1		1	1	1	2			1
Encryption							4	1			1
Integration							2	1			
Logging		9	3	1	11	1	5	8	1		
Login		5	3	3	8	2		2	1		2
Privacy			2							1	
Authentication							2	4	2		1
Availability	1		3			1	6	4		3	1
Design/Implementation					1			6			1
Physical Security								6			
Risk Analysis										1	
Security Management								2		2	
Security Testing								1			

Table 1. Overview of security requirements on eleven IT systems being built during 2003-2005. The double horizontal line divides the requirement categories into mostly functional (above) and mostly non-functional (below). Figures tell how many requirements were found in each category.

4.3 Discussion

Data from the field study show that—(1) Security requirements are poorly specified, and (2) The security requirements specified are mostly functional.

4.3.1 Security Requirements are Poorly Specified

To support the conclusion that the security requirements are poorly specified we highlight three things:

1. Inconsistent selection of security requirements
2. Inconsistent level of detail
3. Security standards are not required

Inconsistent Selection of Security Requirements. In several of the specifications studied we note that some relevant security areas are fairly well specified whereas other are completely left out. Typically, a need for security has been expressed with detailed functional security requirements whereas non-functional requirements are left out. This may lead to security problems (see Section 3).

Examples of such inconsistencies can be seen in access control/roles where all systems have requirements (two referring to standard) which indicates that restricted access is important. At the same time only three specifications require some kind of encryption of data communication and only two specifications require physical security including restricted physical access.

Inconsistent Level of Detail. Some security requirements have a high level of detail whereas others in the same specification are only specified on a general level. This might indicate that the organizations specifying the security requirements rely heavily on local competence and not standards.

We call this phenomenon *local heroes*—for instance, there might be someone who knows very much about backup systems and thus the specifications on backup become detailed and fairly complete. But in other security areas the organization does not have an expert, which leads to under-specified requirements in that area.

This phenomenon can be seen in for instance the "E-Business" system where the requirements on logging are very detailed (eight requirements on what info to be logged) and at the same time digital signatures are specified as "The system should be able to handle the use of electronic signatures" with no further details.

In the specification of "Salary/Staff 1" we find detailed requirements on backup (automation, durability, and runtime backup), while in the same specification the lone requirement on digital signatures is "The system should handle electronic signatures and interfaces to PKI cards etc".

	Billing	Accounting	Salary/Staff 1	Salary/Staff 2	E-Business	Defense Materiel	Medical Advice	Health Care 1	Health Care 2	Highway Tolls	Hazmat
Access Control/Roles											
- per person (FR)	1	4	3	2	4	3	2		1		1
- per group (FR)		1	1	1	2	2	1	1			1
- one person many roles (FR)				1	1		1				
- file access r/w/x (FR)		6	2	1				4	2		1
- role-based GUI (FR)					1						
Attack Detection											
- intrusion detection (FR)							1	2		1	
- fraud detection (FR)										2	
- antivirus (FR)							1	2			
Backup											
- in general (FR)		1	4				1				
- automatic (FR)		3	2	1			1				
- time interval (FR)		1		1							
- durability (NFR)			2								
- data versioning (FR)								2			
- done run-time (FR)			1								
Digital Signatures											
- in general (FR)					1	1		1			
- use of standard (NFR)								1			1
- use of PKI (FR)			1								
- for data origin (FR)							1				
Encryption											
- use of standard (NFR)							1				1
- during login (FR)							1				
- filesystem (FR)							1	1			
- network traffic (FR)							1				

Table 2. Detailed categorization of mostly functional security requirements on eleven IT systems being built during 2003-2005. (FR) means functional, (NFR) means non-functional.

Security Standards are Not Required. Many security areas have well-known and rigorously reviewed standards such as encryption and access control policies. The specifications studied very seldom require these standards to be followed. Instead the requirements specified leaves to designers and implementers to choose or even invent the technology to be used. Such an ad-hoc approach to security is known to lead to problems [16].

None of the specifications explicitly requires a standard policy for access control. In the case of digital signatures two out of six specifications explicitly require a standard solution. And for the area attack detection no publicly known system is required which means the producer can implement his/her own anti-virus software etc.

4.3.2 Security Requirements are Mostly Functional

As mentioned in Section 2.1, security is often conceived as a non-functional requirement, and as such it is known to be hard to manage. However, our study shows that in more than 75% (164 out of 216) of the cases, security requirements boil down to functional requirements. This transformation of abstract non-functional requirements into concrete functional requirements is known and resembles Chung *et al's* technique of "refining initial high-level goals to detailed concrete goals" [3].

However, the kind of non-functional security assurance requirements discussed in Section 3 are left out in almost all cases—we identified 6 such requirements out of 216. The security areas risk analysis, standardized security man-

	Billing	Accounting	Salary/Staff 1	Salary/Staff 2	E-Business	Defense Materiel	Medical Advice	Health Care 1	Health Care 2	Highway Tolls	Hazmat
Integration											
- with firewall (FR)							1				
- with anti-virus (FR)							1				
- with external PKI (FR)								1			
Logging											
- in general (FR)		6	1	1	1	1		1			
- automatic (FR)							3	3			
- what info to be logged (FR)		3	2		8			2			
- log not changeable (FR)					1		2	2	1		
- tool for log analysis (FR)					1						
Login											
- username, password (FR)		2		1		1					1
- password change (FR)		2	1	1	2						1
- smart card (FR)								1			
- Single Sign-On (FR)			1	1	1			1	1		
- automatic logout (FR)		1	1		1	1					
- non-guessable passwords (FR)					1						
- resticted login attempts (FR)					1						
- inactivate old accounts (FR)					1						
- password re-use (FR)					1						
Privacy											
- anonymity (FR)										1	
- classification (FR)											

Table 3. (Continued) Detailed categorization of mostly functional security requirements on eleven IT systems being built during 2003-2005. (FR) means functional, (NFR) means non-functional.

agement, and security testing were categorized as security assurance. The overall distribution of requirements is; CC's security functional requirements divided into functional (76%) and non-functional (21%), and last CC's security assurance requirements as non-functional (3%).

4.3.3 Security Requirements Absent

A natural question is—what security requirements are left out in the specifications studied? Since we decided to list only the requirements present in at least one specification, a comparison with a more complete list would indicate what could be gained. A fair comparison can be made in terms of level of detail. If a security requirement is specified it is unlikely that it has been deliberately under-specified.

To make such a comparison we have chosen two security areas, digital signatures and logging, and listed what the ISO/IEC standard for security management specifies. The reason for choosing this standard was that "Health Care 1" and "Highway Tolls" require that standard to be used.

In the case of the "E-Business" system the requirement on digital signatures was formulated as: "The system should be able to handle the use of electronic signatures". Reading the ISO/IEC standard we find detailed information on what to consider when requiring digital signatures:

- Protection of confidentiality of signature keys
- Protection of integrity of public key
- Quality of signature algorithm
- Bit-length of keys
- Signature keys should differ from keys for encryption
- Assure proper legal binding of the signatures

Logging is specified without standards in seven of the studied projects and specified by referral to standards in two of the projects. If we look at the seven projects with no referral to external documents, the ISO/IEC standard again provides requirements left out in the specifications:

	Billing	Accounting	Salary/Staff 1	Salary/Staff 2	E-Business	Defense Materiel	Medical Advice	Health Care 1	Health Care 2	Highway Tolls	Hazmat
Authentication											
- use of standard (NFR)								3			1
- per person (NFR)							1				
- per system/entity (NFR)							1	1			
- smart card (FR)									1		
- biometrics (FR)									1		
Availability											
- 24h/day, 7 days/week (NFR)	1					1		1			1
- precentage uptime (NFR)			1					1		2	
- redundant power and network (NFR)			2				3	1			
- redundant data (NFR)							3			1	
- automatic restart (FR)								1			
Design/Implementation											
- compartmentalize (NFR)								1			
- input validation (NFR)								1			
- output validation (NFR)								1			
- referential integrity (NFR)					1			1			
- file integrity (NFR)								2			
- fault tolerant interfaces (NFR)											1
Physical Security											
- in general (NFR)								1			
- fire (NFR)								2			
- water/moist (NFR)								1			
- physical intrusion (NFR)								2			
Risk Analysis											
- fraud risk (SAR)										1	
Security Management											
- use of ISO/IEC standard (SAR)								2		2	
Security Testing											
- availability, stress test (SAR)								1			

Table 4. Detailed categorization of mostly non-functional security requirements on eleven IT systems being built during 2003-2005. (FR) means functional, (NFR) means non-functional, and (SAR) means security assurance (subcategory of non-functional).

- Separation of users logged and reviewers of the log
- Protection against de-activation
- Policy for who can change what to be logged
- Protection against logging media being exhausted

The subcategory “what info to be logged” can be further broken down into specific pieces of information. Three out of the seven projects above have specific requirements in what information to be logged. From the ISO/IEC standard we get the following list of left out requirements:

- User IDs
- Date and time of log-on and log-off
- Terminal ID and location
- Successful and rejected system access attempts and data access attempts
- Archiving of logs

4.4 Possible Shortcomings

There are possible shortcomings to our study. First, we want to stress that we do not have access to any kind of risk analysis documents underlying the security requirements specified. Therefore we cannot know if certain security areas have been left out because of deliberate decisions or because of lack of information or knowledge. As a consequence we do not judge the requirements as good or bad, but rather analyze the consistency and the use of standards.

Some of the requirements found in the specifications studied were hard to categorize in a clear way, mostly due to the diversity in definitions of non-functional requirements. Therefore the categorization should not in all cases be interpreted as a given fact.

Using requirement specifications made for public procurement in Sweden for our field study is a decision made primarily because of the availability of them. Commercial entities tend to have little interest in making their requirement specifications available for research. This limited scope affects the validity of the study.

5 Conclusions

We conclude that current practice in security requirements is poor. Our field study shows that security is mainly treated as a functional aspect composed of security features such as login, backup, and access control. Requirements on how to secure systems through assurance measures are left out. Nonetheless, all systems studied have some form of security requirements and most of them have detailed requirements at least in certain security areas. This shows that security is not neglected as such.

The RE community often conceives security as a non-functional requirement and thus generally hard to manage. Our study shows that security requirements are both functional and non-functional. In the functional case they represent abstract security features broken down into concrete functional requirements. In the non-functional case they are either restrictions on design and implementation, or requirements on assurance measures such as security testing.

Following standards and not relying on local competence would make management of security functional requirements no harder than other functional requirements. Thus security requirements being hard to manage mainly holds for security assurance requirements.

6 Acknowledgments

We would like to sincerely thank the reviewers in the SREIS program committee, and our previewers—David Byers and Kristian Sandahl.

References

[1] J. Burge and D. Brown. NFRs: Fact or fiction? Computer Science Technical Report, Worcester Polytechnic Institute, WPI-CS-TR-02-01 ftp://ftp.cs.wpi.edu/pub/techreports/pdf/02-01.pdf, November 2002.

[2] CERT Coordination Center. CERT/CC statistics 1988-2004. http://www.cert.org/stats/cert_stats.html, January 2005.

[3] L. Chung, B. A. Nixon, and E. Yu. Using quality requirements to systematically develop quality software. In *Proceedings of the Fourth International Conference on Software Quality*, McLean, VA, USA, October 1994.

[4] L. Chung, B. A. Nixon, E. Yu, and J. Mylopoulos. *Non-Functional Requirements in Software Engineering*. Kluwer Academic Publishers, 2000.

[5] CSO magazine, U.S. Secret Service, and CERT Coordination Center. 2004 e-crime watch survey. http://www.csoonline.com/releases/052004129_release.html, May 2004.

[6] P. T. Devanbu and S. Stubblebine. Security and software engineering: A roadmap. In *Proceedings of the Twenty-second International Conference on Software Engineering, ICSE*, Limerick, Ireland, June 2000.

[7] European Union. Common procurement vocabulary. http://europa.eu.int/scadplus/leg/en/lvb/l22008.htm, 2004.

[8] IEEE. IEEE-STD 610.12-1990, ieee standard glossary of software engineering terminology, May 1990.

[9] International Organization for Standardization. ISO/IEC 17799:2000 information technology – code of practice for information security management. http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.ht%ml.

[10] Mercell AB Sweden. Database of all purchases in the category '72 - computer and related services' made by swedish government or local authorities from January 2003 to June 2004. http://www.mercell.com, 2004.

[11] Microsoft. Microsoft security glossary. http://www.microsoft.com/security/glossary.mspx, November 2004.

[12] National Institute of Standards and Technology. Common criteria for information technology security evaluation (CC 2.1). http://csrc.nist.gov/cc/CC-v2.1.html.

[13] R. W. Shirey. Request for comments number 2828, Internet security glossary. http://www.faqs.org/rfcs/rfc2828.html, May 2000.

[14] R. H. Thayer and M. Dorfman. *Software Requirements Engineering, Second Edition*. IEEE Computer Society Press and John Wiley & Sons, Inc., 1999.

[15] H. H. Thompson and J. A. Whittaker. Testing for software security. *Dr. Dobb's Journal*, 27(11):24–32, November 2002.

[16] J. Viega and G. McGraw. *Building Secure Software : How to Avoid Security Problems the Right Way*. Addison–Wesley, 2001.