A Risk-Based Approach to Formalise Information Security Requirements for Software Development

Lynn Futcher, Rossouw Solms

A Risk-Based Approach to Formalise Information Security Requirements for Software Development

Lynn Futcher[1] **and Rossouw von Solms**[2]

[1] Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, Lynn.Futcher@nmmu.ac.za
[2] Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, Rossouw.vonSolms@nmmu.ac.za

Abstract: A primary source of information security problems is often an excessively complex software design that cannot be easily or correctly implemented, maintained nor audited. It is therefore important to establish risk-based information security requirements that can be converted into information security specifications that can be used by programmers to develop security-relevant code. This paper presents a risk-based approach to formalise information security requirements for software development. Based on a formal, structured risk management model, it focuses on *how* to establish information security requirements to ensure the protection of the information assets implicated. In this way it hopes to provide some educational guidelines on how risk assessment can be incorporated in the education of software developers.

Keywords: Information security, security requirements, risk analysis, risk assessment, risk treatment, risk-based approach

1. Introduction

Determining the requirements of a software development project is arguably the most important stage of the lifecycle. Inaccurate, incomplete or vague requirements will result in project failure. In the past, attention was predominantly given to understanding and defining the functional requirements of software development projects – what the system was intended to do, together with its inputs and outputs. Although these functional requirements are still essential for successful software development, developers have recently come to realize the importance of non-functional requirements [1].

Non-functional requirements can be defined as the attributes of the system as it performs its job, including the required usability, performance, reliability and security of the system. Although numerous sources agree that security is a non-functional requirement that needs to be considered when defining the requirements of a system, very few have been able to provide a formal, usable approach to doing this methodically. Various software development methods are typically followed in educating software developers. However, none of these methods provide explicit guidelines on how to establish security requirements. This paper argues that in order to establish these requirements, a risk-based analysis should be performed to determine the risks to the information to be captured, stored, processed and communicated by the software being developed.

The following section describes some important risk concepts, while Section 3 presents a risk-based approach to formalise the information security requirements for a software system. This work is an extension of that published in [2]. Where the focus of that paper was on integrating security into the software development life cycle (SDLC), this paper focuses on *how* to establish information security requirements to ensure the protection of the information assets implicated.

2. Risk Concepts

The various terms relating to risk and risk management are used in many disciplines. This paper supports the formal, structured risk management approach as described in [3] and depicted in Figure 1.

<table>
<tr><td rowspan="8">RISK MANAGEMENT</td><td rowspan="7">Risk Assessment</td><td rowspan="5">Risk Analysis</td><td rowspan="5">“Risk”</td><td rowspan="2">Assets</td><td>Asset identification</td></tr>
<tr><td>Asset valuation</td></tr>
<tr><td rowspan="2">Threats</td><td>Threat identification</td></tr>
<tr><td>Threat assessment</td></tr>
<tr><td>Vulnerabilities</td><td>Vulnerability assessment</td></tr>
<tr><td rowspan="2">Risk Evaluation</td><td colspan="3">Determine risk value or size</td></tr>
<tr><td colspan="3">Prioritise risks</td></tr>
<tr><td rowspan="2">Risk Treatment</td><td colspan="4">Identify suitable controls</td></tr>
<tr><td colspan="4">Implement identified controls</td></tr>
</table>

Figure 1 Risk Management – a formalized, structured approach (adapted from [3]).

From Figure 1 it is clear that risk management comprises two key processes, namely risk assessment and risk treatment. While risk assessment refers to the overall process of risk analysis and risk evaluation, risk treatment is concerned with the process of identifying and implementing suitable controls to mitigate risks.

The main objective of a risk analysis is to identify the risks to which the information systems and its associated information assets are exposed. This can be achieved both formally and informally. Performing a formal risk analysis is a structured process by which the individual information assets, threats and vulnerabilities are identified. However, in order to identify specific risks, the identified information assets need to be related to relevant threats. Having identified all risks by means of a risk analysis exercise, a risk evaluation is required to determine the potential 'size' of each risk and for each risk to be prioritized accordingly.

The entire risk assessment process leads to the selection and implementation of appropriate and justified security controls and safeguards in the risk treatment process. It is unwise to implement controls or safeguards simply because they seem to be the right thing to do, since such implementation may result in serious performance issues [4]. These controls and safeguards should be relative to the information security requirements of the software system in question.

This paper suggests that by following a formal, structured risk assessment, the information security requirements of a software system can be established. The following section briefly describes a risk-based approach to determining these information security requirements.

3. The Proposed Risk-Based Approach

The proposed risk-based approach as described in this section requires that a detailed risk analysis is performed to identify the potential adverse business impacts of unwanted events, and the likelihood of their occurrence. The likelihood of occurrence is dependent on how attractive the information asset is to a potential attacker, the level of frequency or probability of the threats occurring, and the ease with which the vulnerabilities can be exploited. The results of a detailed risk analysis can lead to the identification, assessment and prioritisation of risk that are used to identify and select appropriate controls and safeguards. This can then be used to reduce the identified risks to an acceptable level [5].

3.1 The identification and valuation of information assets

In order to perform a risk analysis, the key information assets involved need to be identified. These information assets may include, for example, personal information, employee salary information, customer contact information or financial information. The listing of assets, according to [4], based on checklists and judgment, yields an adequate identification of the most important information assets to be considered. This can also be achieved by identifying the information assets that pertain to relevant data gathering questions. These questions could, for

instance, refer to those information assets which are the most critical to a company's success, its profitability or its reputation. The aim of this stage is to ensure that the most important information assets that require protection from potentially harmful threats are identified. It is normally sufficient to identify between five and eight key information assets that relate to the software system under development.

The next step in the process is to assign impact values to each of the key information assets identified in Section 3.1. These impact values represent the business importance of the information assets. For simplicity it is recommended that a 5-point Lickert scale, as recommended by [4], be used to establish this impact value. This approach requires that an asset impact value between 0 and 4 (where 0=negligible and 4=critical) is assigned to each of the key information assets, based on its financial value or worth to the organisation. Table 1 illustrates a simple way to map the most critical information assets (rows) against their envisaged asset impact values (columns).

Table 1. Information Asset Valuation

Information Assets	Asset Impact Value				
	0 Negligible	1 Low	2 Medium	3 High	4 Critical
Asset A					*X*
Asset B					*X*
Asset C				*X*	
Asset D				*X*	
Asset E			*X*		

The purpose of this stage of the process is to determine the asset impact value and sensitivity of the information assets in use, being captured, stored, processed or communicated. The next stage requires the identification and assessment of the various threats that may cause harm to these information assets.

3.2 The identification and assessment of threats

[6] defines a threat as an undesirable event that could have an impact on the organisation. Software developers therefore need to identify and assess those threats which could negatively impact the information assets associated with their software systems. In order to simplify this process, a checklist of the most common threats is recommended, based on those referred to in [5]. However, since threats are continually changing, software developers are encouraged to add any additional threats to the standard list provided in Table 2. As part of the threat assessment process, it is necessary to determine the level of frequency or probability that a specific threat may exploit some vulnerability thereby negatively impacting the associated information assets.

Table 2. Threat Identification and Assessment

Common Threats (ISO/IEC TR 13335-3:1998)	Level of Frequency/Probability			
	LOW	MED	HIGH	N/A
Theft of information			*X*	
Use of system by unauthorised users		*X*		
Use of system in an unauthorised manner		*X*		
Masquerading of user identity			*X*	
Malicious software attacks			*X*	
User errors			*X*	
Repudiation		*X*		
Technical software failures or errors			*X*	
Other				

This may be performed, as illustrated in Table 2, by assigning each of the threats listed to one of the frequency/probability levels provided, namely low, medium or high.

3.3 The identification of risk

Risk can be described as a threat that exploits some vulnerability thereby causing harm to an asset. Risk identification therefore requires that the most critical asset/threat relationships are identified to ascertain which risks are most likely to have a negative impact. This is done by simply considering the most important information assets, as identified in Section 3.1., and the most common threats identified in Section 3.2. Those information assets with high or critical asset impact values (i.e., 3 or 4) and those threats recognised to have a potentially medium or high level of frequency or probability, will contribute significantly to the criticality of the risk.

Table 3. Risk Identification

Common Threats (ISO/IEC TR 13335-3:1998)	Information Assets				
	Asset A	Asset B	Asset C	Asset D	Asset E
Theft of information	*Risk 1*	*Risk2*			*Risk 5*
Use of system by unauthorised users			*Risk 6*		
Use of system in an unauthorised manner					*Risk 7*
Masquerading of user identity	*Risk 3*				
Malicious software attacks	*Risk 4*				
User errors		*Risk 8*			
Repudiation					
Technical software failures or errors					
Other ……					
Other ……					

Table 3 provides a way to map the most probable threats (rows) against the most important information assets (columns), i.e. identify the specific risks to the

software system. Using this table, software developers are required to determine the most critical risks (i.e., asset/threat relationships). It is normally sufficient to identify approximately eight key risks. The risk analysis process, however, is only complete having carried out a vulnerability assessment, since without a vulnerability there would be no risk.

3.4 The vulnerability assessment

The purpose of a vulnerability assessment is to determine the degree of weakness that could be exploited. [7] states that in practice, security is not compromised by breaking the dedicated security mechanisms, but by exploiting the weaknesses or vulnerabilities in the way they are used. Therefore, as part of the risk analysis process, it is important to be able to determine the level of vulnerability for each risk (asset/threat relationship) as identified in Section 3.3.

The level of weakness or vulnerability for each risk can be determined by taking the current situation and existing controls into account. This should provide some indication of whether the risk could materialize. Table 4 provides a simple way to map each risk (rows) against the appropriate level of vulnerability (columns), namely low, medium or high. This completes the risk analysis process, as referred to in Figure 1. Section 3.4 describes the risk evaluation process required to complete the risk assessment process.

Table 4. Vulnerability Assessment

Risks (refer to Table 3)	**Level of Vulnerability**		
	LOW	**MEDIUM**	**HIGH**
Risk 1	*X*		
Risk 2		*X*	
Risk 3	*X*		
Risk 4	*X*		
Risk 5		*X*	
Risk 6			*X*
Risk 7			*X*
Risk 8		*X*	

3.5 The risk evaluation

According to [3], the purpose of the risk evaluation process is two-fold. Firstly, it is to determine the value or size of risk and secondly to prioritise risks according to their risk value.

In order to determine the risk value of each risk, the asset impact value of the associated information asset, the level of frequency or probability of the associated

threat and the related level of vulnerability must be considered for each risk identified. These relationships can be matched in a table to determine the specific measure of risk on a scale of 1 (low) to 8 (high). These values are placed in a matrix as illustrated in Table 5, according to those recommended by [5]. The appropriate row in the table is identified by the asset impact value of the associated information asset (0 to 4), as identified in Section 3.1. Similarly, the appropriate column is determined by the level of frequency or probability of each associated threat (low, medium or high) and the corresponding level of vulnerability (low, medium or high). The matching cell in the matrix will determine the risk value of the particular risk identified.

Table 5. Risk Evaluation

RISK 1 (as per Asset/Threat Relationship in Table 3)										
		Level of Frequency/Probability of Threat								
		LOW			MEDIUM			HIGH		
		Level of Vulnerability			Level of Vulnerability			Level of Vulnerability		
		LOW	MED	HIGH	LOW	MED	HIGH	LOW	MED	HIGH
Asset impact value	Negligible 0	0	1	2	1	2	3	2	3	4
	Low 1	1	2	3	2	3	4	3	4	5
	Medium 2	2	3	4	3	4	5	4	5	6
	High 3	3	4	5	4	5	6	5	6	7
	Critical 4	4	5	6	5	6	7	6	7	8

The specific risk values, as determined for each risk, are valuable in assessing and prioritising those risks that require individual attention throughout the rest of the software development lifecycle. Furthermore, having followed a formal, structured risk assessment one is able to document appropriate risk-based information security requirements through which these risks may be reduced to an acceptable level.

4. Risk-based Information Security Requirements

According to [8], information security requirements are generally defined in terms of specific technological mechanisms and tools. However, these can rarely be traced back to a recognised risk. In order to arrive at appropriate information security requirements, this approach proposes a more formalised process whereby a risk assessment is carried out followed by the identification of appropriate security services, as referred to by [9], for each risk. For each key risk, multiple security services can be identified, namely: identification and authentication, access control, data confidentiality, data integrity and non-repudiation. These security services could then be translated into security mechanisms as referred to by [9]. These eight security mechanisms include encryption, digital signatures,

access control mechanisms, data integrity mechanism, authentication exchange mechanisms, traffic padding, routing control and notarization mechanisms. This approach should therefore lead to an improved risk treatment process whereby the correct controls are selected and implemented.

5. Conclusion and Future Work

Risk management is an essential tool for the systematic management of information security. It helps identify possible security holes in information systems and assists in providing appropriate countermeasures. For software under development, it is important to have a clear understanding of the information assets that need to be protected, the threats against which those information assets must be protected, the vulnerabilities associated with the information assets, and the overall risk to the information assets from those threats and vulnerabilities.

By following a risk-based approach as proposed in this paper, the controls that are implemented can easily be traced back to specific risks to the information assets implicated in the software under development. It can also assist in motivating which controls, and the strength of the controls to be implemented.

References

1. Britton, C., Doake, J.: Software System Development. A Gentle Introduction. 4th Ed, pp. 21-35. McGraw-Hill, Berkshire (2006).
2. Futcher, L. von Solms, R.: SecSDM: A Model for Integrating Security into the Software Development Life Cycle. IFIP International Federation for Information Processing. Fifth World Conference on Information Security Education. Volume 237. pp. 41-48. Springer, Boston (2007).
3. von Solms, S.H., von Solms, R.: Information Security Governance, pp.87-100, Springer, New York (2009).
4. Landoll, D. J. The security risk assessment handbook : A complete guide for performing security risk assessments. New York : United States of America: Auerbach Publications (2006).
5. ISO. ISO/IEC TR 13335-3 : Information Technology – Guidelines for the Management of IT Security. Part 3 : Techniques for the management of IT security (1998).
6. Peltier, T. R. *Information security risk analysis*. New York : United States of America: Auerbach Publications (2005).
7. Jurjens, J. Using UMLSec and goal trees for secure systems development. *Communications of the ACM*, *48* (5), pp.1026-1030. (2002).
8. Tirado, I. Business Oriented Information Security Requirements Development, Ivan Tirado, CISSP-ISSAP, Kennesaw State University, 1000 Chastain Road, Kennesaw, GA 30144, itirado@students.kennesaw.edu. (2006).
9. ISO. ISO 7498-2: Information Processing Systems - Open System Interconnection - Basic Reference Model - Part 2: Security Architecture. (1989).