2008

Organisational security requirements: An agile approach to Ubiquitous Information Security

A B. Ruighaver
Deakin University

DOI: 10.4225/75/57b563f7b8770
Originally published in the Proceedings of the 6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 1st to 3rd December 2006.

Organisational security requirements: An agile approach to Ubiquitous Information Security.

Dr. A.B. Ruighaver
Business Security Research and Privacy Group
Deakin University
tobias@deakin.edu.au

Abstract

This paper proposes to address the need for more innovation in organisational information security by adding a security requirement engineering focus. Based on the belief that any heavyweight security requirements process in organisational security will be doomed to fail, we developed a security requirement approach with three dimensions. The use of a simple security requirements process in the first dimension has been augmented by an agile security approach. However, introducing this second dimension of agile security does provide support for, but does not necessarily stimulate, innovation. A third dimension is, therefore, needed to ensure there is a proper focus in the organisation's efforts to identify potential new innovations in their security. To create this focus three common shortcomings in organisational information security have been identified. The resulting security approach that addresses these shortcomings is called Ubiquitous Information Security. This paper will demonstrate the potential of this new approach by briefly discussing its possible application in two areas: Ubiquitous Identity Management and Ubiquitous Wireless Security.

Keywords

Security requirement engineering, agile security, ubiquitous security, ubiquitous identity management, wireless intrusion detection

INTRODUCTION

At present, organisations are often ill-prepared to cope with the increased risks in their IT environment whilst their reliance on computers and computerised communication devices continues to grow (Ngo et. al. 2005). Over the past decades the number of reported security incidents and the resulting losses has been rising steadily. While security technology and security management are rapidly becoming more complex, they have not been able to keep up with the rapid adoption of new IT technologies and new business practices.

Deciding which security strategies, architectures and applications to deploy is still a major issue for most organisations. In this paper, we suggest that one of the major problems in organisational information security is that current security management lacks innovation and is still mainly based on now inadequate 20th century risk management (Shedden et. al. 2006) and security standards/applications (Tan & Ruighaver 2005). While previous papers have identified other common shortcomings in security governance and security culture (Ruighaver et. al. 2007), this paper will propose the use of security requirement engineering at the organisational security level to address the lack of innovation.

While security requirement engineering in software engineering is a rapidly growing research area (Crook et. al. 2002), the use of security requirement engineering at the organisational level is currently almost non-existent. According to Maiden and Robertson (2005) “Requirements Engineering is a creative process in which stake-holders and designers work together to create ideas for new systems that are eventually expressed as requirements”. Hence, an obvious approach to address the lack of innovation in organisational security will be to introduce a proper requirement engineering process in security management.

The main decision making process currently used in information security is the Plan-Do-Check-Act cycle as documented in the current security standards. This PDCA model, however, is less suitable for “situations that are invariably uncertain, dynamic and confusing” (Grant & Kooter 2005). Our research in security culture (Ruighaver & Maynard 2006) also indicates that organisations using PDCA often do not actively pursue understanding of the current security situation in their organisation anymore. This, we believe, will severely complicate any attempts to improve security in a cost-effective manner. Hence, any new approach in security management will need to emphasise security failures instead of just concentrating on security successes.

Further more, the current approach to information security is based on a heavyweight process which starts with an extensive risk analysis, followed by the development of a security policy and the implementation of that policy. While this process looks akin to the waterfall approach in software engineering, in practice there are a number of common deficiencies found in the way organizations develop their information security.

The growing complexity of ICT has increased the cost of a systematic risk analysis. This cost has become so high that organizations can no longer afford to perform this risk analysis at a low enough level of granularity needed to accurately identify the controls that might mitigate these risks (Shedden et.al. 2006). Unfortunately, the shortcuts that organizations take to simplify the risk identification and analysis have a detrimental effect on the quality of the risk analysis, a fact seldom recognized by the organization.

These and similar experiences has lead to our decision to adapt a lightweight requirement engineering process. Keeping the requirement engineering process lightweight, however, means that we can not extend the requirement process itself to improve creativity (Nguyen et.al. 2000). While this issue will undoubtedly be explored in future research, the rest of this paper will explore two other dimensions of the requirements engineering approach needed to support and stimulate innovation.

In a section on Agile Information Security we discuss how the adoption of security requirements engineering introduces several new challenges. These challenges, as well as the lack of prioritisation guidelines in the current standards (Tan & Ruighaver. 2005) and the increasingly dynamic nature of the security environment in organizations (Peterson et.al. 2002, Pye et.al. 2005) suggest that there is a need to develop a more agile approach to information security.

On its own, however, agile security does not address the need for more innovation. While, for now, we declined to enhance the requirement process itself to stimulate creativity, we would like to ensure that the requirement process receives some direction. Creativity is simply not useful if the resulting solutions are not relevant and effective (Bruner 1962). In our final section on Ubiquitous Information Security, we identify three common shortcomings in organisational security to provide a focus in the requirement engineering process.

While this paper can not, and will not, attempt to describe the ultimate Ubiquitous Information Security approach or solution, it tries to demonstrate the potential of this new approach by discussing its possible application in two main areas: Ubiquitous Identity Management and Ubiquitous Wireless Security.

ORGANISATIONAL SECURITY ENGINEERING

While organisations are, in general, willing to invest more in their information security, they are still struggling coming to a decision where to best increase their security effort and which security strategies, architectures and applications they need to deploy to achieve the most cost-effective solution. Unfortunately, while there are standards such as ISO27002 and Cobit that provide lists of what controls should be implemented, they provide little guidance on when these controls are relevant, what alternatives are available, or what requirements these controls really fulfil.

Investigating the literature on requirement engineering for security applications and systems did not deliver any immediately usable insights either. Few papers have been found on (explicit) requirements for information security or security applications or on the need to re-use requirements. While it would be possible to investigate the literature on particular security systems and extract the implicit requirements for those systems from the design discussions, we were not convinced that the results would be helpful in our effort to increase creativity at the organisational security level. Further more, little evidence could be found that the requirement processes used in application security encourage creativity.

The only area of systems security where requirements and requirement engineering is taken more seriously is in cryptography. However, while there is a standard on (functional) security requirements for cryptographic modules, no proper guidelines are available for general applications using cryptography. Realisation has been growing that applications of cryptography normally break because of human factors and implementation problems but, while a similar problem occurs in organisational security, it is not clear what lessons can be learned from cryptography that are relevant for organisational security.

Probably more relevant for this research is the literature on security requirement solicitation in information systems design. Although there seems to be a growing interest in the use of misuse cases in security requirement solicitation, we feel that the development of misuse cases as part of the requirement solicitation process itself might not work in organisational security requirements engineering. We are currently investigating its use in incident reporting and expect that a repository of misuse cases borrowed from information systems design will be useful in organisational security as well.

The largest body of work in this area that is relevant for organisational security is the research on reuse of security requirements and artefacts (Firesmith 2004). We need new research that identifies re-usable artefacts that are useful at the security architecture and security applications level, but again we believe it may be necessary to develop separate processes, for instance through a feedback process based on incident reporting, to ensure that the development and maintenance of repositories for those artefacts takes place independent from the actual security requirement elicitation process.

As discussed before, our starting point is that the actual security requirement engineering process needs to be a lightweight process. Unfortunately, many current security requirement engineering methodologies proposed for use in software engineering such as TROPOS and SQUARE (Mead et.al. 2005) are complex and may therefore not be cost-effective in an organisational security context. More importantly, the organisational security architect or other security expert that becomes responsible is likely to lack any experience in these software engineering methodologies and a simple to understand methodology is therefore preferred.

Although we aim to start with a lightweight process, we have no objection against making the process slightly more extensive in future. However, our experience with decision making processes such as the previously mentioned PDCA is that organisations always tend to simplify the process. So we would like to ensure that the top level structure of the requirement process still produces good requirements, before we add more structure underneath each step of the process.

Our current approach, therefore is to adopt a simple process borrowed from User Requirement Specification in Software Engineering

- Elicitation/Identification
- Analysis
- Specification
- Communication

As the above process is extensively described in many software engineering papers and books we will not further elaborate on each of the four steps in this paper, but instead will discuss some of the issues related to the use of this process in organisational security.

Firstly, organisational security requirement engineering can and should be used at many levels of the security strategic context (Tan & Ruighaver 2005), in particular at the strategic level, the security infrastructure level and the security application level. In this paper we will demonstrate the proposed concepts at the application level. It is important to understand that security requirement engineering at the application level does not necessarily identify requirements of a particular security application but instead aims to identify which applications are needed to satisfy the organisation's security needs.

It should also be obvious that before the security requirement process starts, the organisation first needs to identify which area of its organisational information security it would like to improve. This is similar to when you start developing a software application: You will need some idea what kind of application it is. In the examples used in this paper, the author has chosen two areas that are common problem areas in organisational security. Fortunately, the ubiquitous approach introduced in this paper will also ensure that, in time, a better understanding of the organisation's security will develop.

In the proposed requirement specification process, it will be the task of an Organisational Security Architect to interview the stake-holders as part of the Elicitation stage. As we do not expect any initial domain knowledge from most of the stake-holders, this first step will need the architect to be the expert, brief the stake-holders, and provide direction. The quality of the requirements will therefore depend largely on the domain knowledge of the architect and his willingness to encourage creativity. One of the aims of the rest of this paper is therefore to provide this organisational security architect with at least one potentially effective direction that he might find useful to explore.

Finally, there is still an open issue of how we will evaluate the quality of the resulting requirements. Future research in this area is needed as well. Whatever framework the organisation eventually will decide to adopt, however, it will need to address at least the following issues:

- Simplicity and Cost-effectiveness
- Balance and coverage (as in any security approach)
- Innovation

AGILE INFORMATION SECURITY

As mentioned before, there seems to be a reluctance in most organisations to employ heavyweight processes in the management of information security although most standards still encourage an approach akin to the waterfall approach in software engineering. Life cycle models proposed for security policy implementation are normally also based on waterfall like approach.

A major problem faced by organisations is that the dynamic security environment is forcing them to reduce the time frame of their security implementation. Hence, organisations both use shortcuts in their risk assessment

phase and in their implementation phase. While as a result, the process followed is no longer a real waterfall approach, it still suffers from the main disadvantage of this approach that ignited the software engineering revolution: The heavy cost of maintenance. Some of the organisations that we have studied in the past have even decided that it would be more cost-effective to just start from scratch again.

Another major reason why the current development process in information security is not really a proper waterfall approach is the general lack of documentation on the policy development process (Maynard & Ruighaver 2003). Heavyweight software development processes rely on documentation (Khan & Balbo 2004), but our experience is that organisations seldom have a proper documentation of the risk analysis process, or of the link between the risks that the organisation wants to control and the actual controls in their policy. This will therefore severely hamper any further development of their information security.

At the same time, the lack of domain knowledge within organisations on security requirements at both the security infrastructure and security application level will make any initial attempt at organisational security engineering less effective and indicates that an agile approach to organisational security might be in order. Further more, adding a security requirement focus to organisational security will, on its own, not solve the above mentioned problems unless we attempt to be innovative and look outside the current set of traditional controls. Identifying, developing, and assessing the cost-effectiveness of new controls will, however, be a process of trial and error. Hence, it is important that we change the current mind set in both organisations and in information security research that information security is based on a waterfall approach.

One important aspect of agile security is that organisations will need to gain better knowledge of internal security to assist in the prioritisation of agile security projects. Hence, organisations might want to consider starting with some agile projects related to the monitoring of security. The particular approach to agile security proposed in this paper, as described in the next section on Ubiquitous Information Security, aims to improve the balance between preventive controls and detection and response. So each agile project based on this approach will automatically provide data that can be used to prioritise further agile projects.

Finally, like always, it is important in information security that your security covers all potential risks. Fortunately, there is less need in agile security to accept risks. By evaluating the balance between continued improvement of existing agile projects and starting new projects, the organisation has more opportunities to increase its coverage. Agile security encourages the organisation to keep thinking about *what* instead of *how*. Hence, choosing an agile security approach is an opportunity to be innovative in your security coverage as well.

UBIQUITOUS INFORMATION SECURITY

Agile Security is a necessity in today's security environment, but adopting an agile security approach is only a start. The aim of agile security should be continuous innovation. Applying an agile security approach to traditional information security will only offer limited improvement.

To give direction to the requirements engineering process at the application level, we would expect the organisation to have both a strategic direction as well as a preferred security infrastructure. While we believe good security governance needs to follow a top down approach, we also realise that most organisations still follow a bottom up approach as they are used to do in IT governance. As a result, mission statements in organisations are often general statements about information security and the strategy communicated to IT and security staff is normally restricted to “follow this standard”.

This lack of strategic direction in organisations will make it difficult for those organisations to be creative in their organisational security requirement engineering. Too provide some general direction to this creative process, we have therefore identified three basic security principles/strategies that we would like to see in an organisation:

- Current security is too preventive; we need a better balance between prevention and detection/response. For each preventive control we really should also have detection and response planned for when that control fails. One good example of this obsession with preventive controls is the current state of the art in authentication and access control: I have found no organisations that even consider detecting masquerading attacks or monitoring their user's file access patterns. Another example is Defence in Depth, which was originally a reactive strategy but is now actively promoted as a pure preventive strategy.
- Security should be based on multiple overlapping controls instead of one single complex control. Currently many security controls are just too complex. It is a well known principle of asymmetric warfare that complexity in defence favours the attacker. Furthermore, this escalation in preventive controls often hinders detection of attackers bypassing the control.

- We need to better integrate security with every day activities and in every day devices. Nowadays users have USB sticks, PDA's, mobile phones, etc, that may endanger your security but might also be used to improve your security. And, while many organisations now have strict physical access control in their buildings, most keep these physical access control systems separated from their authentication and access control of IT systems.

Ubiquitous Information Security is an approach that utilises these principles to build a security architecture that can be tailored to the organisation's security needs. The aim is not to make security perfect, but to find a way to optimise security for each organisation. Of course, this is not necessarily the ultimate set of security strategies that an organisation can use to direct its security efforts. These three have been chosen to demonstrate the power of a strategic approach to direct innovation at the application level. Research is continuing to identify more strategies that fit with this original set.

Some other requirements for an ubiquitous security infrastructure/architecture are:

- An ubiquitous security architecture should be based on multiple small security mechanisms or applications that work together to create a practical and robust approach to security. At least one of those mechanisms or applications will need to be detective/reactive.
- Mechanisms and applications designed for one ubiquitous security architecture should be designed for reuse in other ubiquitous security architectures.
- Similar to ubiquitous computing, an obvious trend in ubiquitous security will be the use of location information. This could include access control based on location of user and authentication based on location of personal devices.

Evaluating potential requirements for an ubiquitous security infrastructure has brought up some new issues that we consider important enough that they may also have some relevance outside ubiquitous security. Although we are hesitant at this moment to elevate them to the strategic level, we may decide do so in future. These issues are:

- Ubiquitous security should not be invisible. Users should be continuously aware of the potential impact of their activities and decisions on the organisation's information security.
- While users should be aware of the security surrounding them, ubiquitous information security should not inhibit the user's normal activities.
- An ubiquitous security approach is likely to utilise new technologies that may have an increased impact on the user's privacy. Hence, it will be necessary to balance the need for security with the user's need for privacy.

TWO EXAMPLES OF UBIQUITOUS INFORMATION SECURITY PROJECTS

As stated before, it is up to the organisation to prioritise which agile security projects will be most beneficial for that organisation's security. To illustrate the ubiquitous security approach we have selected two projects that should provide some value for most organisations: Ubiquitous Identity Management and Ubiquitous Wireless Security. Obviously, it is not the aim of this paper to completely describe ubiquitous security in these areas: There is only room for a brief discussion and we will not be able to discuss potential responses to a detected security breach.

As most organisations still rely on simple password based authentication, they obviously are unaware of the increased risk of masquerading attacks. Passwords are easily compromised through the use of cameras in phones and other devices, while the potential reuse of company passwords on the Internet may increase this risk even further.

One approach to Ubiquitous Identity Management starts with a simple notification application that sends an SMS to the user's phone when that user logs in. Notice that the user does not need have the phone when logging in, something that has prevented banks from introducing SMS for the communication of one time passwords. Still, sending an SMS for every login may not be the optimal solution. Our suggestion is to only send an SMS for an internal login when the physical access control system indicates that the user is not in the building. While this may prevent detection of internal masquerading attacks, it will be considered adequate security in many organisations and is better than using passwords alone. Further more, sending an SMS "You logged in at your desk but have not swiped your access card" will certainly increase security awareness.

If this initial implementation is not secure enough, the organisation might consider a second authentication using the user's USB stick. While there are commercial USB based authentication systems available, a cheap software only solution should be fine for now, and can be kept separate from the original authentication system. As this is a second authentication system, there is no need to implement the ultimate perfect authentication mechanism.

However, a one time password based system is preferable. After the normal login the user will be requested to insert the USB stick and if the second authentication is successful no SMS message will be send. The same system could also be used on the user's home computer by installing the necessary software there. Notice that when users forget their USB stick they can still login.

If even more security is required, the organisation might now consider adding an SMS based authentication system as well. This is more intrusive but, when users forget their phone, access is still possible using the USB based authentication and an automatic SMS alert. If the user can not authenticate using a USB stick either, login with a normal password may still be allowed, as long as a security administrator is alerted.

While these are only the initial steps in the development of a full ubiquitous identity management system, it should be evident that such a system can be tailored for each organisation and that a software only solution will be a cheap alternative to current hardware based authentication systems.

Our second example of an ubiquitous wireless security system is basically an agile but limited version of a new wireless intrusion detection system we have been developing. This system is based on the use of existing nodes in a WI-FI network, such as laptops and PDA's, as network sensors. When their wireless interface is not active, in particular when they are docked and connected to a fixed wire network, they can be used to collect network data. The original wireless intrusion detection system aims to provide an instantaneous response to masquerading attacks, in particular denial of service attacks, by detecting the difference in location between the original node and an attacker for particular frames using the difference in signal strength at each sensor.

A similar approach to detect masquerading attacks can be used in an ubiquitous wireless security approach, by ensuring that access points and other vulnerable nodes listen for network frames with their own MAC address that they obviously did not send themselves. While this currently would need a change in the network cards firmware to really work well for most mobile devices, other devices such as access points sometimes already have a built in sensor. Furthermore, most current denial of service attacks are not very intelligent and can be detected even when the network node only listens occasionally.

To further improve this system, we suggest the configuration of a DIY sensor network by adding several cheap network cards to existing PC's and by creating an application for laptops so they can detect whether they are docked and should register for this sensor network. The more sensors the better the location detection will be. To limit the amount of data that needs to be collected, the system only needs to collect the signal strength for a few types of control frames that are commonly used in attacks. A centralised intrusion detection system can collect this data and use the different signal strengths of a frame to compute the approximate location of origin for that frame. While our experiments have shown it will be difficult to separate an attacker that is in close proximity of the attacked system, attackers that are further away will be easy to detect.

If the sensor network also collects signal strengths of frames during the initial authentication of a node with its access point, other security policies can be implemented to prevent wireless access from outside the building or to discourage wireless access if the node is close to its docking station. More importantly, however, this location information can now be used in the ubiquitous identity management system to decide if an SMS alert should be generated.

CONCLUSION:

In this paper we introduced several new concepts in the area of organisational security requirements engineering. The emphasis of this paper has been to describe some of the challenges that the use of security requirement engineering will face and to demonstrate the value of using this approach in stimulating innovation in organisational security.

Our approach to organisational security requirement engineering is based on the assumption that the use of a heavyweight security requirements process in organisational security will eventually fail because most organisations are likely to take whatever shortcuts they can think of the reduce the cost of the requirements process.

To support and encourage innovation in information security while using a lightweight security requirements process, we developed a requirement engineering approach with two additional dimensions. Adding a dimension based on agile security simply enables innovation. Another dimension, Ubiquitous Information Security, finally aims to stimulate and give direction to the creativity made possible by the agile security approach. Ubiquitous Information Security supports this agile approach by encouraging the use of simple and overlapping controls that can be tailored to an organisation's security needs. As each set of controls also includes at least one control aimed at detection of potential security failures, this approach will give the organisation better insight in its internal security to assist it in prioritising further agile security projects.

REFERENCES:

Bruner, J. S. (1962) The conditions of creativity, in H. Gruber, G. Terrell, & M. Wertheimer, eds., Contemporary approaches to cognition, pp. 1–30, Atherton, NY, USA.

Crook, R., Ince, D., Lin, L., and Nuseibeh, B. (2002) Security requirements engineering: when anti-requirements hit the fan, Proceedings of the 10th anniversary IEEE international requirements engineering conference (RE'02), Essen, Germany

Firesmith, D.G. (2004) Specifying Reusable Security Requirements, *J.Object Technology*, vol. 3, no. 1, pp. 61-75, Jan.-Feb. 2004

Grant, T.J., and Kooter, B.M. (2005) Comparing OODA & Other Models as Operational View C2 Architecture. In Proceedings of the 10th International Command and Control Research Technology Symposium, June 2005, McLean, VA. USA.

Khan A. and Balbo S. (2004) A Tale of two Methodologies: Heavyweight versus Agile. In Proceedings of the tenth Australian World Wide Web Conference (AusWeb), Gold Coast, Australia, 2004.

Maiden N.A.M. and Robertson S. (2005) Integrated Creativity into Requirements Processes: Experiences with an Air Traffic Management System, Proceedings 13th IEEE International Conference on Requirements Engineering, IEEE Computer Society Press, 105-114.

Maynard, S., and Ruighaver, A.B. (2003) Development and Evaluation of Information System Security Policies, *Information Systems: The Challenges of Theory and Practice*, Hunter, M. G. and Dhanda, K. K. (eds), Information Institute, Las Vegas, USA, pages 366 – 393.

Mead N.R., Hough E.D., and Stehney II T.R. (2005) Security Quality Requirements Engineering (SQUARE) Methodology, CMU/SEI, Technical Report CMU/SEI-2005-TR-009, ESC-TR-2005-009, Nov. 2005.

Ngo, L. and Zhou, W. and Warren, M. (2005) Understanding Transition towards Information Security Culture Change, in C. Valli, A. Woodward (eds), Proceedings of the 3rd Australian Information Security Management Conference, pp. 67-73, School of Computer and Information Science, Edith Cowan University, Western Australia, Australia

Nguyen L., Carroll J.M. and Swatman P.A. (2000) Supporting and Monitoring the Creativity of IS Personnel During the Requirements Engineering Process, Proc. Hawaii Int'l Conf. Systems Sciences (HICSS-33), IEEE Computer Society.

Peterson, R.R, Parker, M., and Ribbers P. (2002) Information Technology Governance Processes under environmental dynamism: Investigating competing theories of decision making and knowledge sharing, 23rd Annual International Conference on Information Systems, Barcelona, 15-18th December 2002.

Pye G., Pierce J.D., Warren M.J., and Mackay D.R. (2005) Supply Chain Security: The Need for Continuous Assessment, *Supply Chain Practice* Vol. 7 (1): pp.4–16.

Ruighaver, A.B. and Maynard, S. (2006) Organizational Security Culture: More Than Just an End-User Phenomenon, *Proceedings of the 21st IFIP TC-11 International Information Security Conference (IFIP/SEC 2006)*, May 22, 2006, Karlstad, Sweden, pages 425-430.

Ruighaver, A.B. , Maynard, S., and Chang, S. (2007) Organizational Security Culture: Extending the End-User Perspective, *Computers & Security*, Volume 26, Issue 1, February 2007, Pages 56-62.

Shedden, P. Ahmad, A and Ruighaver, A.B. (2006) Risk Management Standards– The Perception Of Ease Of Use. 5th Annual Security Conference, Las Vegas, Nevada USA, 19-20 April 2006.

Tan C.C.T. & Ruighaver A.B. (2005) Understanding the scope of strategic context in security governance. In B Cusack (ed), *IT Audit: A Strategic Foundation for Corporate Governance* . 65-77. Auckland , New Zealand : School of Computer & Information Science, Auckland University of Technology.

COPYRIGHT