Human Factors in Software Security Risk Management

Shareeful Islam
Institut für Informatik
Technische Universität München
München, Germany
islam@in.tum.de

Wei Dong
School of Computer
National University of Defense Technology
ChangSha, P.R.China
wdong@nudt.edu.cn

ABSTRACT
All kinds of human factors can deeply affect the results and efficiency of software risk management. This paper focuses on our ongoing work of studying human factors in security risk management. The human factors are identified and classified for the categories of individual, team, management and stakeholder, as well as for the activities of security risk identification, analysis and mitigation. Then some considerations and recommendations for mitigating these factors and risks are presented, and the generic framework of evolving them into the secure software architecture is also figured.

Categories and Subject Descriptors
D.2.9 [**Software Engineering**]: Management – *software quality assurance, programming teams*

General Terms
Human Factors, Management, Security

Keywords
Human factors, software security, risks management

1. INTRODUCTION
Nowadays people are more dependent on the software in their daily activities. At the same time, software systems have become more complex and extensible, and distribute their functions and data through high speed networks. But even using the latest security techniques and protocols, most software systems still face a lot of security breaches, and the adopted development methodologies always deliver the software beyond the limit of budget and schedule. One of the major reasons is that human, who are involved in developing, managing and using the software, may make mistakes due to lack of security perceptions, skills and knowledge. These mistakes would bring a great loss if they are not properly handled. Now it has been convinced that the integrated software security risk management should be considered from the early phases in the development, so that the confidentiality, integrity, availability, authenticity, etc. of the software can be ensured, and the products can be delivered on time within budget.

Software risk management needs a holistic approach that should consider four integrant dimensions of the risks. These are: 1) the risks of adopted technologies and products; 2) the risks of software development process and life cycle models; 3) the methodologies of software risk management; and 4) the risks from involved human and organizations. From the last dimension, human and organization factors and their relations to the security risks should be addressed for ensuring the software security. The perceptions for security risks are varying from man to man, and can deeply affect the results of risk management. This paper presents the current status of our work on studying what are the risk factors from the dimension of human and organization, what are the effects of the human perception on software security risk management, and how to use the appropriate security policies, procedures, techniques and tools to mitigate these risks.

2. DIMENSION OF HUMAN AND ORGANIZATION
The roles of human involved in software development fall into four categories, which are individual, team, management and stakeholder/interested party [2]. There are always inter-relations and overlaps among these four categories. Some risk factors of individuals and teams are as follows:

- ✓ Personal competency of employing the development methods, language and tools
- ✓ Experience and leadership of the team leader
- ✓ Team performance
- ✓ Availability of skilled personnel
- ✓ Commitment to the project
- ✓ Personnel loyalty to the organization
- ✓ Skills of identifying and analyzing the factors in risk management, etc.

Management and stakeholders have different views of risks. For example, management focuses on the risks in terms of profit, schedule, quality, fewer personnel with more outputs, etc; the stakeholders such as customers or users concern the investment, security level, software usability, and effectiveness of using the software, etc. Different views about the risks should be considered among numerous human factors based on the scopes and levels of responsibilities, time, cost, goals, skills, knowledge, and expertise etc. The decisions from management have a great impact on software development. Essential management and stakeholder factors to be considered for software security risk management are:

- ✓ Management directions and supports
- ✓ Confidence level of the management team
- ✓ Recruitment of right personnel
- ✓ Collaborations with external organizations
- ✓ Contract between management and service providers
- ✓ Appropriate training resources

- ✓ Periodical review of security policies and procedures
- ✓ Support for effectively applying enhanced methodologies
- ✓ Risk culture
- ✓ Periodical risk assessment and security planning
- ✓ Additional budget, schedule for risk mitigation, etc.

The roles that involved in software risk management should be well organized with good mutual interactions. The organization dimension considers the overall organization infrastructures, which will directly affect the process, cost and schedule of software development and risk management. Organization risk factors may include [6]:

- ✓ Organization structure and its stability
- ✓ Internal and external communications
- ✓ Efficiency
- ✓ Maturity
- ✓ Environment for implementing security policies and procedures
- ✓ Integration of security issues with day-to-day operators
- ✓ Adequate facility for software development
- ✓ Compliance with the legal requirements, etc.

Factors of human and organization dimensions will directly affect the cost, schedule, development process and lifecycle. In addition, the capabilities of the individuals, teams and management that contribute to the development process have great influence on the well-founded risk management process and successful software development. Team leader's experience, communication and guidance ability, motivation can also deeply impact the results [8]. Furthermore, for security risks, the human and organization factors have their own characteristics which are discussed in following sections.

3. SECURITY VULNERABLILITIES

Human factors are underlying reasons for many attacks on information systems. Hackers, intruders, virus writers and all other malicious users may exploit the human factors to penetrate the systems. To improve the security, each layer of the information systems is required to be perfectly secure. Users still think computer as a black box. They don't understand that using the software which contains vulnerability can bring the genuine security risks. Sometimes users may simply ignore following the minimum responsibilities, such as opening email attachments from anonymous users, irregularly updating the antivirus software, etc. This lack of security consciousness helps hackers to complete the successful attacks via malicious activities. Most users are also not aware of how to correctly treat confidential information, such as choosing weak password, writing password in plain paper and laying it on the desk, not following the clean desk policy, sharing ID, etc. All these issues can be helpful for the social engineers to breach the confidential information.

Not only ordinary users, but also the security professional can violate the security policies. These risk factors concern the human rather than technologies, and may cost a lot even using the best technologies. These factors can be concluded as:

- ✓ Deficient security awareness
- ✓ Inadequate considerations of security issues more than virus and worms
- ✓ Ignoring security alerts
- ✓ Lack of security analysis before choosing products
- ✓ Ignoring user's responsibilities
- ✓ Improper system configuration
- ✓ Lack of periodical monitoring and maintenance, or timely update of security devices
- ✓ Underestimating the severity of security threats
- ✓ Low competency level of the security management team
- ✓ Poor relationship with other teams, etc.

Finally, human factors have strong impacts on creating and implementing security policies and procedures aiming for security management. These factors are not only concerning the development of security policies and procedures but also the popularization of these policies among all participants including roles within organization and persons of external parties. For instance, all users should understand and follow the security policies; adopted security policies and standards should be up-to-date and well documented. Only technical considerations cannot obtain the sufficient security in practice, and the human awareness might be the most cost-effective way for security management [5]. Thus, human aspects for managing the security vulnerabilities should be considered as carefully as technical aspects.

4. HUMAN FACTORS FOR SECURITY RISK MANAGEMENT PROCESS

Software security risk management is a process which includes step by step activities, such as asset identification, threat and risk identification, risk measurement, consequence quantification and evaluation, risk reporting and mitigation. The process is time consuming and costly, and should start from the early phases of software development. Successful completion of this process should be able to mitigate maximum risks into the acceptable level, so that the software product finally can be delivered on schedule and within the budget, and would be affected by less security breaches in the future usage. Human involved in the whole process play a significant role for successfully achieving these purposes.

4.1 Risk Identification

It is expected that critical security risks can be identified before they will introduce some problems into the systems. Security risk is a threat that would cause harm to critical assets. Generally, people have different views while conducting the risk identification. Some common variations of the human perception while identifying the security risks include [1]:

- ✓ People generally prefer risks that they know or concern individually
- ✓ Too much attention is paid to identify the hidden, new, unfamiliar or uncertain risks
- ✓ Less attention is paid to the common, anonymous, less discussed risks
- ✓ Overestimating the hidden risks and underestimating the common risks
- ✓ Misunderstanding or neglecting the threat environment
- ✓ Overconfidence of internal systems
- ✓ Considering more on external attacks that can exploit the security breaches
- ✓ Considering less on internal users who can sometimes also exploit severe security vulnerabilities
- ✓ Underestimating the risks from some controlled or trusty external sources, etc.

Due to these factors, actual risks may not be properly or completely identified initially. As a result, it may affect the results of risk management. Therefore, human perception should be considered as an important risk factor for the whole risk management process.

4.2 Risk Analysis and Mitigation

All identified risks need to be analyzed and prioritized so that they can be eliminated or at least be mitigated into an acceptable level. Several specific aspects should be considered while analyzing each individual risk, such as likelihood of occurrence, severity, magnitude of the cost, effectiveness of the countermeasure to mitigate the risk, etc. These aspects are related with each others, and need to be analyzed in detail for effectively mitigating the risks. People always like to use the rules of thumb, rather than considering mathematically [1]. But this trend of perception needs to be corrected to match the reality. For example, if severity of an individual risk is considered higher than it actually is, then there may have a chance to overspend the time and money on mitigating the risk and vice versa. Underestimation or overestimation of each aspect of the potential threats can bring on the wrong evaluation for the trade off.

5. CONSIDERATION AND RECOMMENDATION

In this section, some possible guidelines, procedures and technical aspects that may be needed or helpful for identifying and analyzing the human factors in security risk management are presented.

5.1 Human and Team Work

Competence level of employees can be improved by mandatory training, security awareness program, etc. The training needs to consider not only security protocols, mechanisms and devices, but also the security risk management process and the procedures for developing secure software. Developers should receive the technology-specific security training that may be involved in the phases of software analysis, design, coding, and testing. They should be educated to incorporate security in every phase rather than just considering security as an add-in feature. Appropriate software architecture is very important for improving security, so the techniques of designing secure architectures should be specially focused on in the training. Roles and responsibilities of the team members and leaders in security management should be clearly defined and constantly reviewed. Periodical security awareness program, information security education and using the system with acceptable manner should also be considered for all levels of the personnel.

5.2 Organization and Management

Security policies and procedures approved by the management need to be implemented for the whole organizational environment. It is critical for management commitment that should consider the personnel roles and responsibilities, criteria for acceptable risk levels, and the supports of establishing, implementing, monitoring and reviewing these levels. Parts of the major policies and procedures that may be considered in addressing human and organization risk factors include [9]:

- ✓ Security policies
- ✓ Access control policy
- ✓ User responsibility
- ✓ Risk management methodology
- ✓ Organization structure
- ✓ Asset identification, classification and acceptable usage
- ✓ Input / output validation
- ✓ Cryptographic control
- ✓ Physical and environment security
- ✓ Malicious activity detection and network monitoring
- ✓ Detecting malicious code in software development
- ✓ Security architect, design, coding and testing
- ✓ Training need assessment, plan and feedback
- ✓ Competence / skill level matrix for all employees
- ✓ Security awareness program and security education
- ✓ Checklist for system upgrade and maintenance
- ✓ Response of security incident
- ✓ Compliance with legal requirements, etc.

To improve the human perception for risk identification, we recommend considering the methods such as common sense assessment (based on the historical knowledge), risk taxonomy based questionnaires, analogy based on well known cases (including underestimate and overestimate ones), asset based threat analysis, vulnerability analysis and modeling, expertise with real risks in the specific area, etc [3]. All these methods can be used to identify and analyze the risks which would more closely match the reality for trade off.

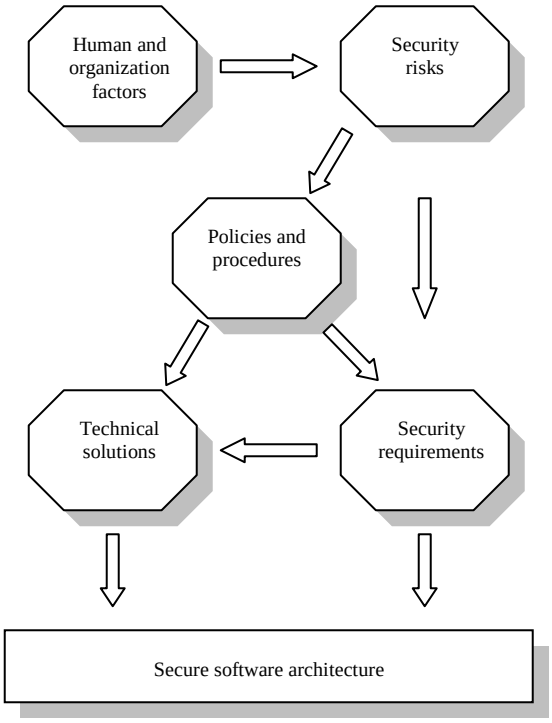

Figure 1. Developing secure software architecture considering human factors.

5.3 Technical Consideration

After identifying and analyzing the security risk factors, the security policies and procedures need to be developed. Security requirements can be constructed through mapping the risks, policies and procedures into the metrics of secure software [7]. Then the security protocols, technologies, tools, policies and procedures can be adopted to mitigate the security risks of human issues. Furthermore, when these technical aspects have been established, the corresponding security infrastructures should be integrated into the software architectures. So in our ongoing work, we should study more about how to establish the links or relations among human and organization factors, security risks, security policies and procedures, security requirements, corresponding technologies and secure software architectures. The generic framework is shown in figure 1.

6. CONCLUSION

Factors of human – those who develop, manage, purchase, use and attack the software – should be tackled in software development and security risk management. Here we identified the human and organization factors in the software development and software security risk management. All these aspects need to be considered from the early stages in software development so that the successful security risk management can be expected. Finally, what are the relations of these issues with the security solutions, technologies and tools, and how the possible mitigation methods can be considered and adopted earlier and throughout the software life cycle will be further studied.

7. ACKNOWLEDGMENTS

The work is partly supported by the German Academic Exchange Service (DAAD), the projects from National Natural Science Foundation of China (No.60673118) and National 863 High Technology Research and Development Program of China (No.2006AA01Z429).

8. REFERENCES

[1] Bruce Schneier. The psychology of Security, http:// www. schneier.com/ eassy-155.html, 2008.

[2] Ronald P. Higuera, Yacov Y. Haimes. Software Risk Management. Technical report, CMU/SEI -96-TR-012, 1996.

[3] Dale Walter Karolak. Software Engineering Risk Management. IEEE Computer Society Press. ISBN 0-8186-7194-7, 1996.

[4] Konstantin Sapronov. The human factor and information security, http://www.viruslist.com/en/analysis?pubid= 176195190, Dec 2005.

[5] Gary Hinson. Human factors in information security, IsecT Ltd. 2003.

[6] C. Woody. Eliciting and Analyzing Quality Requirements: Management Influences on Software Quality Requirements, Networked Systems Survivability, Technical Note, CMU/ SEI-2005-TN-010, 2005.

[7] Shareeful Islam, Wei Dong. Security Requirements Addressing Security Risks for improving Software Quality. Workshop on Software Quality Modelling and Evaluation, Springer-Verlag, 2008.

[8] Matthew R. Mcbride. The Software Architect. Communications of the ACM, Vol.50, No.5, 2007

[9] Thomas R. Peltier. Information Security Risk Analysis, second edition, Auerbach publications, 2005.