
M. Li, M. Tang

Meng’gang Li
China Center for Industrial Security Research,
Beijing Jiaotong University, China
morganli@vip.sina.com

Mincong Tang
International Center for Informatics Research,
Beijing Jiaotong University, China
mincong@bjtu.edu.cn

Abstract: Information security is not a new topic in academics and industry. However, through a comprehensive literature review, we found that most research in information security focus on technical perspectives including evaluation methods and mathematical approaches for securities, risk mitigation algorithms, with some research focus on economic perspective of information security and even a few talked about social engineering of information security. There is not a unique framework to integrate different types of research in information security. We believe that information security research apply the theories and methodologies in systems engineering to investigate the problems, that is, information security engineering. In this paper, we propose a conceptual framework of information security engineering. This framework explicitly illustrates the methodological system, content system, procedures and strategies for information security engineering research and practices.

Keywords: Computer Science, Information Security Engineering (ISE), Systems Engineering, Information Systems.

1 Introduction

Information security problem has been coming along with the development of our society. In the past two decades, information technologies (IT) and Internet have changed our world in an unbelievable speed. They bring to us many conveniences as well as risks and uncertainties. Thus information security problem becomes very prominent under such circumstance and it now plays a decisive position in national securities of a country. Information security mainly involves governments, enterprises, organizations, associations and individuals. It spreads with a very wide time domain and covers all fields of the society including politics, economy, culture, military etc. Compared with the securities of politics, economy and military, information security has the following features: 1) information security is the core of national security in information era; 2) the nature of information security is information resource security; 3) information security relies more and more on the securities of technological systems; 4) attack sources of information security are characterized as spectral and concealed.

Information security nowadays is no longer an isolated and scattered but a very complicated systems engineering problem. Thus we propose that it’s necessary and urgent to conduct in-depth and comprehensive studies to examine information security from the viewpoint of engineering. We define this as information security engineering (ISE): ISE is a kind of systems engineering which is based on information technology and takes information security management as its approach and information security laws and policies as its assurance. As a subset of systems engineering, ISE is the embodiment of information system securities for systems security engineering, systems engineering and system acquisitions. ISE is a product of the integration
of security engineering, information management and information systems development. The 
contents of ISE mainly include: connotations, contents and objectives of ISE; information secur-
ity risk analysis and evaluation procedures, methods and tools; requirement analysis methods, 
security strategies, security architecture, security solutions, security implementation standards, 
security test and operations, emergency measures and methods, security education and training.

The thinking of engineering has been well applied into software development and security 
management, from which two subjects: software engineering and security engineering have been 
formed and developed. Though these two subjects are relatively completed, studies of information 
security have been affected by the knowledge structures of researchers, rapid development of our 
society and other factors, the findings of information security research are scattered and the 
theory lags behind the demand of applications. On the other hand, though the sense of security 
has been strengthen in the past 10 years, from installing anti-virus software to procuring security 
products, the understanding of security still stays at the very stage of ‘treat only where the pain 
is’. The problem of information security cannot be solved by pure technology, nor can it be 
solved by putting security products together. It has to rely on complicated systems engineering— 
information security engineering (ISE). Therefore, there is a need to conduct in-depth research 
in information security from a systems engineering perspective.

We organize this paper in the following ways: in the next section we present a comprehensive 
literature review, which forms the foundations of ISE. Followed by is the processes of ISE in 
section 3. After that we propose a framework of ISE, the framework is used to suggest future 
trends within ISE research and practices in section 4.

2 Foundations of ISE

As developed from software engineering and security engineering, ISE follows the foundations 
of systems engineering but its context is limited to information security and information systems. 
Different from typical systems engineering, ISE research focuses on the development of method-
ology and architecture for information security. It intends to unite the diversities in information 
security research and makes it an interdisciplinary research without limiting the analysis to a 
particular discipline (i.e. computer sciences, information systems etc.). By comprehensively re-
viewing existing information security literature, we mainly found that four issues of information 
security have been well studied. These four issues are:

1) Security Management (SM): SM refers to the ways like information systems planning and 
evaluation, to maintain secure information systems within organizations. Backup, recovery, 
contingency management are included in SM.

2) Communication Security (CS): CS refers to the measures adopted to ensure secure com-
munication achieved between people.

3) Access of Information and Systems (AIS): AIS refers to the measures that control people’s 
access to information and systems.

4) Secure Information Systems Development (SISD): SISD refers to the methods, policies and 
procedures that lead a secured information system to be developed.

According to the differences in research approaches of the literatures we reviewed, we only
incorporate those studies after 2000 for the purpose of most updated knowledge in these areas, we summarized the findings from existing literature as table 1.

Table 1: Summary of Existing Literature in Information Security

<table>
<thead>
<tr>
<th>Issue</th>
<th>Source</th>
<th>Propositions/Findings</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Dhillon &amp; Backhouse (2000)</td>
<td>Responsibility, integrity, trust and ethicality (RITE) principles hold the key for successfully managing information security. In addition to confidentiality, integrity, and availability (CIA).</td>
<td>Conceptual</td>
</tr>
<tr>
<td></td>
<td>Eloff &amp; Eloff (2003)</td>
<td>To successfully secure the information and technology related assets of an organization, management should aim towards establishing an information security management system (ISMS).</td>
<td>Conceptual</td>
</tr>
<tr>
<td></td>
<td>Solms &amp; Solms (2004)</td>
<td>10 essential aspects like not realizing that information security is a corporate governance responsibility and not realizing that information security is a business issue and not a technical issue and so on must be taken into account in an information security governance plan to make it a success</td>
<td>Conceptual</td>
</tr>
<tr>
<td></td>
<td>Solms (2005)</td>
<td>A separate information security compliance management department is needed when talking about information security management</td>
<td>Conceptual</td>
</tr>
<tr>
<td></td>
<td>Saint-Germain (2005)</td>
<td>For organizations to fall into several regulatory realms, they need to establish a comprehensive, flexible framework for implementing cost-effective compliance, deployed via a governing system that maintains security policies and controls</td>
<td>Organizational (Case study)</td>
</tr>
<tr>
<td></td>
<td>Tsoumas &amp; Gritzalis (2006)</td>
<td>The separation of security requirements from their technical implementations facilitates security management</td>
<td>Technological</td>
</tr>
<tr>
<td></td>
<td>Chang &amp; Lin (2007)</td>
<td>Organization culture will significantly influence the effectiveness of implementing information security management</td>
<td>Organizational (Survey)</td>
</tr>
<tr>
<td></td>
<td>Ashenden (2008)</td>
<td>Human challenge of Information Security management has largely been neglected and people need to look at the skills needed to change organizational culture, the identity of the Information Security Manager and effective communication between Information Security Managers, end users and Senior Managers.</td>
<td>Conceptual</td>
</tr>
<tr>
<td></td>
<td>Werlinger et al. (2009)</td>
<td>18 challenges like technical complexity, mobility and so on can affect IT security management within organizations</td>
<td>Organizational (Survey)</td>
</tr>
<tr>
<td></td>
<td>Chaddoud et al. (2001)</td>
<td>Baal protocol as a scalable solution to group key management problems and it can resolve the user’s revocation problem</td>
<td>Technological</td>
</tr>
<tr>
<td></td>
<td>Khadra et al. (2003)</td>
<td>Impulsive synchronization of two chaotic systems is very robust, this robustness is useful in designing chaos based cryptosystems, which is used to ensure secure communication</td>
<td>Technological</td>
</tr>
<tr>
<td>Issue</td>
<td>Source</td>
<td>Propositions/Findings</td>
<td>Approach</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Information Security</td>
<td>Yang (2004)</td>
<td>Impulsive synchronization is more robust than continuous synchronization. Based on a combination of both conventional cryptographic method and impulsive synchronization of chaotic systems, a new chaotic secure communication scheme is proposed, which is to ensure secure communication.</td>
<td>Technological</td>
</tr>
<tr>
<td>Engineering: a Framework</td>
<td>Liang et al. (2008)</td>
<td>Secrecy capacity region of the Gaussian BCC complements the secrecy capacity region of the discrete memoryless BCC. This will enhance secure communication.</td>
<td>Technological</td>
</tr>
<tr>
<td>for Research and Practices</td>
<td>Kiani-B et al. (2009)</td>
<td>The proposed encoding chaotic communication has achieved a satisfactory, typical secure communication scheme. Results show that security is enhanced based on spreading the signal in frequency and encrypting it in time domain in the proposed system.</td>
<td>Technological</td>
</tr>
<tr>
<td></td>
<td>Access of Information and</td>
<td>Trust is added as a new dimension to pervasive computing, allowing greater flexibility in designing policies and providing more control over accessing services and information.</td>
<td>Conceptual</td>
</tr>
<tr>
<td>Systems</td>
<td>Kagal et al. (2001)</td>
<td>An approach for regulating service access and information disclosure on the Web is proposed, which consists of a uniform formal framework to formulate and reason about – both service access and information disclosure constraints. This approach ensures communicating users’ requirement while disclosing no private information.</td>
<td>Technological</td>
</tr>
<tr>
<td></td>
<td>Bonatti, &amp; Samarrati (2002)</td>
<td>'Understanding the enemy' is believed to be an important component of information protection.</td>
<td>Conceptual</td>
</tr>
<tr>
<td></td>
<td>Whitman (2003)</td>
<td>A security architecture based on a role-based access scheme is proposed and found to be effective to identify different users’ access to local sources and other sites.</td>
<td>Conceptual</td>
</tr>
<tr>
<td></td>
<td>Gritzalis &amp; Lambrianoudakis</td>
<td>Contextual factors including organizational culture, management support etc. for the application of IS security policies have been discussed, these factors are to be taken into consideration when implementing information security policies including access to information and systems.</td>
<td>Conceptual</td>
</tr>
<tr>
<td></td>
<td>Karyda et al. (2005)</td>
<td>A new model for risk-based access control is proposed. This model is based on fuzzy multi-level security access control and found to be more effective than traditional Bell–Lapadula model.</td>
<td>Technological</td>
</tr>
<tr>
<td>Secure IS development</td>
<td>Jurjens (2001)</td>
<td>UML is used to express security requirements in system development.</td>
<td>Technological</td>
</tr>
<tr>
<td></td>
<td>Georg et al. (2002)</td>
<td>An aspect-oriented approach to modeling is proposed to allows developers to encapsulate design concerns like security, availability of services, and timeliness so that they can be woven into a design in a systematic and consistent manner.</td>
<td>Technological</td>
</tr>
</tbody>
</table>
Jones & Rastogi (2004) Security has to be “baked in” to the overall systems development life-cycle process.

Villarroel et al. (2005) Eleven secure systems design methodologies have been compared to see how they should be adopted in system development.

Mouratidis et al. (2005) An approach considering security concerns as an integral part of the entire system development process is proposed to be necessary.

Mellado et al. (2007) Security has to be dealt with at all stages of IS development, especially in the establishment of security requirements to achieve a robust IS.

Cheng et al. (2008) A new concept of security engineering environment (SEE) is proposed, SEE concept with high security requirements can provide a base for designers, developers, users, and maintainers with standard, formal, and consistent supports.

Mouratidis & Jurjens (2010) Two prominent approaches, a goal-oriented security requirements engineering approach called Secure Tropos and an MBSE approach called UMLsec have been integrated to help how elicited security requirements can be realized in the design stage and how the developed design can be verified against the security requirements of the system.

Based on the discussion from existing literature, we believe that these four issues of information security above consist of the major contents of ISE (Figure 1) and form the foundations of ISE. Specifically, the four issues in ISE can be elaborated as followings.

![Figure 1: Fours issues in Information Security Studies](image)

While the contents of information security mainly cover the four issues, ISE research issues will include but not limits to: philosophical foundations of information security, definitions
of information security, mathematical foundations of information security, safety rheology and mutation laws, physiological and psychological issues in information security, ISE methods of analysis, forecasting and control, information security risk evaluation and information security management methods, human-computer environment analysis and design etc. These research issues interact with the four issues of information security.

3 Processes of ISE

As a subset of systems engineering, ISE mainly follows the processes of systems engineering, which is illustrated by figure 2.

![Processes of Systems Engineering](image)

The processes described above are usually carried out in the following ways:

1) Discover tasks or requirements;
2) Define functionalities of system;
3) Design system;
4) Implement system;
5) Evaluate effectiveness

For ISE, the processes above are customized to specific information securities. The key is to fulfill the requirements of information protection by implementing systems engineering processes. ISE can facilitate the development of system products and process solutions to satisfy the users’ requirements. Thus, the processes of ISE becomes:

1) Discover requirements of information security: ISE will first investigate users’ requirement, policies, standards, vulnerabilities and threats regarding of information. Then ISE will mark the users of information and systems, their roles and responsibilities in information security.

2) Define information security system: users’ requirements of information protection and description of information system environment are interpreted as the objectives and functionalities of information security system. In this stage, ISE will define what can be done by information protection system and the executions of information security system as well as the internal and external interface of information security system.

3) Design information security system: ISE will design the architecture of information security system and detail the design scheme of information security system.
4) Implement information security system: according to the requirements of information security, this stage aims to development, procure, integrate, test and verify the collections of configuration of information security system. Similar with the corresponding stages in systems engineering, ISE will conduct implementation and testing in this stage.

5) Evaluate effectiveness of information security system: ISE emphasizes the capabilities of providing confidentialities, integrities, availabilities and non-repudiation for information. ISE processes emphasize marking, conceiving and controlling information security risks and optimize these risks to protect potential losses due to various possible threats and attacks.

4 A Framework for ISE Research and Practices

In Oxford Dictionary, framework is defined as a structure upon or into which contents can be put and further relates it to thoughts that are directed for a purpose. The ISE Framework proposed in this study provides academics and practitioners with an understanding of how to conduct an information security research and practices from an engineering point of view so as to align ISE theories with applications.

Figure 3: A Framework for Information Security Engineering Research and Practices
As illustrated in figure 3, there are four levels in the framework: definition, basic theory, methodology and application.

At the definition level, four elements are included. We propose that objectives, definitions, research subjects and relations with other disciplines belong to this level. For ISE research, these four elements must be clearly defined.

At the basic theory level, three elements are included. Philosophical foundations of ISE refer to those philosophical issues like unity and contradiction of security and risks, accuracy and fuzziness of information security etc., these provide the highest level of understanding of ISE. Mathematical foundations of ISE provide theoretical and analytical methods to solve the problems of ISE while physiological and psychological problems of ISE focus on the behavioral perspectives of ISE research.

At the methodology level, different techniques (methods) for analysis and evaluation are included. These do not only include analytical methods (i.e. event tree, fault tree etc.), but also include causal analysis methods which are widely used in behavioral research.

At the application level, two categories are proposed to provide guideline for practitioners in ISE, which include information security management and backbone technologies for information security.

This framework provides guidelines and directions for researchers in information security areas. First, it proposes three elements in the basic theory level. These elements cover a very large section of the existing literature in information security especially for the mathematical foundations. Second, from a conceptual approach point of view, the philosophical foundations cover many discussions in literature. Third, physiological and psychological problems, which are still gaps in literature of information security, they are areas calling for further studies. For practitioners, this framework provides insights for their practices in information security and management. Behaviorally, three managerial perspectives are proposed: standards, processes, policies and regulations. Technologically, three issues of information security have been proposed, they are regarded as backbone technologies through which the objectives of information security could be achieved from a technological view.

5 Concluding Remarks

Information security engineering is a comprehensive and cross-disciplined subject which covers the knowledge in mathematics, physics, telecommunication, computer sciences and management. It is not a simple combination of various tools of security technologies, nor does it equal to a series of managerial regulations and safety standards. It is a complicated system engineering. By conducting a comprehensive literature review, we have a body of knowledge on information security research, which forms the basics and contents of ISE. Establishing information security engineering as an independent subject is critical to assure national information securities and improve the levels of information security training. Moreover, it guides theoretical research and practical applications in this area and make it possible to integrate the critical security technologies and standards and subsequently create a unique and effective system for information securities.

Acknowledgement

This paper is part of the project ‘Research on China Industrial Security Index’ (No. B09C1100020) funded by the Ministry of Education, China. We are grateful for the suggestions and comments from two experts who reviewed this article for us.
Bibliography


