Preface

In the last decade information and computer security is mainly moving from the confines of academia to the enterprise concerns. As populations become more and more comfortable with the extensive use of networks and the Internet, as our reliance on the knowledge-intensive technology grows, and as progress in the computer software and wireless telecommunication increases accessibility, there will be a higher risk of unmanageable failure in enterprise systems.

In fact, today's information systems are widely spread and connected over the networks, but also heterogeneous, which involves more complexity. This situation has a dramatic drawback regarding threats, which are now occurring on such networks. Indeed, the drawback of being open and interconnected is that they are more and more vulnerable as a wide range of threats and attacks. These attacks have appeared during the last few years and are growing continuously with IP emergence and with all new technologies exploiting it (SIP vulnerabilities, phishing attacks, etc.) and also due to the threats exposing operators (DDOS) and end user (phishing attacks, worms, etc.). The Slammer and SoBig attacks are some of the examples that were widely covered in the media and broadcast into the average citizen home.

From the enterprise perspective, information about customers, competitors, products and processes is a key issue for its success. The increasing importance of information technology for production, providing and maintaining consistent security of this information on servers and across networks becomes one of the major enterprise business activities. This means that it requires a high flexibility of the organizational infrastructure and on the introduction of new ways of information usage.

In such a complex world, there is a strong need of security to ensure system protection in order to maintain the enterprise activities operational. However, this book gathers some essays that will stimulate a greater awareness of the whole range of security issues facing the modern enterprise. It mainly shows how important to have a strong interaction that is required between enterprise goals and security solutions.

OBJECTIVES

It is the purpose of this book to provide a practical survey of the principals and practice of IT security with respect to enterprise business systems. It also offers a broad working knowledge of all the major security issues affecting today's enterprise IT activities, giving readers the tools to address opportunities in the field. This is mainly because the security factors provide to the enterprise a high potential in order to provide trusted services to their customers. This book shows also to readers how to apply a number of security techniques to the enterprise environment with its complex and various applications. It covers the many domains related to the enterprise security, including: communication networks and

multimedia, applications and operating system software, social engineering and styles of attacks, privacy and authorisation and enterprise security risk management.

This book gathers a best collection of papers written by many authors instead of a book that focuses on a specific approach or methodology.

Intended Audience

Aimed at the information technology practitioner, the book is valuable to CIO's, operations managers, network managers, database managers, software architects, application integrators, programmers, and analysts. The book is also suitable for graduate, master and postgraduate course in computer science as well as for computers in business courses.

STRUCTURE OF THE BOOK

The book chapters are organized in logical groupings that are akin to appropriate levels in an enterprise IT security. Each section of the actual book is devoted to carefully chosen papers, some of which reflect individual authors' experience. The strength of this approach is that it gives a benefit from a rich diversity of viewpoints and deep subject matter knowledge.

The book is organized into eighteen chapters. A brief description of each of the chapters follows:

Chapter I proposes three different realistic security-level network architectures that may be currently deployed within companies. For more realistic analysis and illustration, two examples of companies with different size and profile are given. A number of advices, explanations and guidelines are provided in this chapter so readers are able to adapt those architectures to their own companies and both security and network needs.

Chapter II is dedicated to the security requirements detailing various secured middleware systems, such as GRID computing, which implies sharing heterogeneous resources, located in different places belonging to different administrative domains over a heterogeneous network. It shows that there is a great similarity between GRID security and classical network security. Moreover, additional requirements specific to grid environments exist. At the end, the chapter gives some examples of companies using such systems.

Chapter III describes in detail the fundamental security requirements of a Symbian based mobile device such as physical protection, device access control, storage protection, network access control, network service access control, and network connection security. Symbian security is also evaluated by discussing its weaknesses and by comparing it to other mobile operating systems.

Chapter IV describes in its first part the security features of IEEE 802.11 wireless local area networks, and shows their weaknesses. A practical guideline for choosing the preferred WLAN configuration is given. The second part of this chapter is dedicated to the wireless radio network by presenting the associated threats with some practical defence strategies.

Chapter V presents first a classification and a brief description of intrusion detection systems, taking into account several issues such as information sources, analysis of intrusion detection systems, response options for intrusion detection systems, analysis timing, control strategy, and architecture of intrusion detection systems. It is then discussed the problem of information exchange among intrusion detection systems, being addressed the intrusion detection exchange protocol and a format for the exchange of information among intrusion detection systems. The lack of a format of the answers or countermeasures

interchanged between the components of intrusion detection systems is also discussed as well as some future trends in this area.

Chapter VI presents security solutions in integrated patient-centric Web based healthcare information systems, also known as electronic healthcare record (EHCR). Security solutions in several projects have been presented and in particular a solution for EHCR integration from scratch. Implementations of

, privilege management infrastructure, role based access control and rule based access control in EHCR have been presented. Regarding EHCR integration from scratch architecture and security have been proposed and discussed.

Chapter VII proposes a novel interactive access control model: servers should be able to interact with clients asking for missing or excessing credentials whereas clients my decided to comply or not with the requested credentials. The process iterates until a final agreement is reached or denied. Further the chapter shows how to model a trust negotiation protocol that allows two entities in a network to automatically negotiate requirements needed to access a service. A practical implementation of the access control model is given using X.509 and SAML standards.

Chapter VIII aims to put into perspective the delegation implications, issues and concepts that are derived from a selected group of authorization schemes which have been proposed during recent years as solutions to the distributed authorization problem. It is also the analysis of some of the most interesting federation solutions that have been developed by different consortiums or companies, representing both educational and enterprise points of view. The final part of this chapter focuses on different formalisms specifically developed to support delegation services and which can be integrated into a multiplicity of applications.

Chapter IX introduces digital rights management (DRM) in the perspective of digital policy management (DPM) focusing on the enterprise and corporate sector. DRM has become a domain in full expansion with many stakes, which are by far not only technological. They also touch legal aspects as well as business and economic. Information is a strategic resource and as such requires a responsible approach of its management almost to the extent of being patrimonial. This chapter mainly focuses on the latter introducing DRM concepts, standards and the underlying technologies from its origins to its most recent developments in order to assess the challenges and opportunities of enterprise digital policy management.

Chapter X describes common attacks on antivirus tools and a few obfuscation techniques applied to recent viruses that were used to thwart commercial grade antivirus tools. Similarities among different malware and their variants are also presented in this chapter. The signature used in this method is the percentage of APIs (application programming interface) appearing in the malware type.

Chapter XI describes the various ways in which phishing can take place. This is followed by a description of key strategies that can be adopted for protection of end users and organizations. The end user protection strategies include desktop protection agents, password management tools, secure email, simple and trusted browser setting, and digital signature. Some of the commercially available and popular antiphishing products are also described in this chapter.

Chapter XII describes the threat of phishing in which attackers generally sent a fraudulent email to their victims in an attempt to trick them into revealing private information. This chapter starts defining the phishing threat and its impact on the financial industry. Next, it reviews different types of hardware and software attacks and their countermeasures. Finally, it discusses policies that can protect an organization against phishing attacks. An understanding of how phishers elicit confidential information along with technology and policy-based countermeasures will empower managers and end-users to better protect their information systems.

Chapter XIII provides a wide spectrum of end users with a complete reference on malicious code or malware. End users include researchers, students, as well as information technology and security professionals in their daily activities. First, the author provides an overview of malicious code, its past, present, and future. Second, he presents methodologies, guidelines and recommendation on how an organization can enhance its prevention of malicious code, how it should respond to the occurrence of a malware incident, and how it should learn from such an incident to be better prepared in the future. Finally, the author addresses the issue of the current research as well as future trends of malicious code and the new and future means of malware prevention.

Chapter XIV provides a wide spectrum of existing security risk management methodologies. The chapter starts presenting the concept and the objectives of enterprise risk management. Some exiting security risk management methods are then presented by sowing the way to enhance their applications to enterprise needs.

Chapter XV presents a system life cycle and suggests which aspects of security should be covered at which life cycle stage of the system. Based on this it is presented a process framework that due to its iteratively and detailed ness accommodates the needs for life cycle oriented security management.

Chapter XVI presents a study on the classification of software specification languages discussing the current state of the art regarding attack languages. Specification languages are categorized based on their features and their main purposes. A detailed comparison among attack languages is provided. We show the example extensions of the two software specification languages to include some features of the attack languages. We believe that extending certain types of software specification languages to express security aspects like attack descriptions is a major step towards unifying software and security engineering.

Chapter XVII qualifies and treats the security associated with the transfer of the content, as a quality of service parameter. The user is free to select the parameter depending up on the content being transferred. As dictated by the demanding situations, a minimum agreed security would be assured for the data at the expense of the appropriate resources over the network.

Chapter XVIII gives an introduction to the CORAS approach for model-based security risk analysis. It presents a guided walkthrough of the CORAS risk analysis process based on examples from risk analysis of security, trust and legal issues in a collaborative engineering virtual organisation. CORAS makes use of structured brainstorming to identify risks and treatments. To get a good picture of the risks, it is important to involve people with different insight into the target being analysed, such as end users, developers and managers. One challenge in this setting is to bridge the communication gap between the participants, who typically have widely different backgrounds and expertise. The use of graphical models supports communication and understanding between these participants. The CORAS graphical language for threat modelling has been developed especially with this goal in mind.