Detailed Table of Contents

The established legal value of digital signatures and the growing availability of identity-based digital services are progressively extending the use of smart cards to all citizens, opening new challenging scenarios. Among them, motivated by concrete applications, secure and practical delegation of digital signatures and decryptions is becoming more and more critical. Unfortunately, all secure delegation systems proposed so far include various drawbacks with respect to some of the main functional requirements of any practical system. With the purpose of proposing a truly practical solution for signature and decryption delegation, in this chapter the authors put forth the notion of a "Proxy Smart Card System," a distributed system that allows a smart card owner to delegate part of its computations to remote users. They first stress the problematic aspects concerning the use of known proxy-cryptography schemes in synergy with current standard technologies, which in turn motivates the need of proxy smart card systems. Then they formalize the security and functional requirements of a proxy smart card system, identifying the involved parties, the adversary model, and the usability properties. Finally, the authors present the design and analysis of a proxy smart card system, which implements the required functionalities outperforming the current state of the art.

The expansion of electronic commerce (E-commerce) has become an increasing reality due to Internet's rapid growth during the last few years. E-commerce is growing at an exceptional rate with more organizations offering their goods and services online every day. Importantly, this growth is being matched by the number of people gaining access to the Internet in a variety of ways. E-commerce offers opportunities as well as threats. Information is crucial for any organization, especially in the e-market. The lack of an effective and trusted payment system that can be used in combination with online shopping has been limiting factor in the growth of Internet sales. Consumers are hesitant to provide personal information, including credit card details, over the Internet because of high perception of risk and concerns with privacy. Establishment of Information Security System can minimize the threats and risks. Technology can play an important role in intensifying trust in the information society and securing consumer rights. E-commerce will not be successful without protecting the consumers' rights, especially in the area of information security. The research highlights the relevant theories of information security within the e-commerce sectors, including identifying and investigating the problems.

One of the problems highlighted within the area of information security is that international standards are implemented in organisations without adopting them to special organisational settings. In this chapter the authors analyse information security goals found in hospital settings. They found that the CIA-triad fails to cover organisational specific information security goals in hospital settings. They found also that information security goals held by information security managers and business managers are not the same, implying that both these groups should be involved in designing of information security goals, in order to find information security goals relevant for the organisation. Finally, the authors found goal maps used in this study for analysis of empirical data, to be a useful tool for analysis and communication of information security goals in an organisation.

Chapter 6

Authentication is probably one of the main security processes that almost everybody has at one point used. Currently, the most widespread authentication mechanism is based on textual passwords, a well-established approach that, with the growth of users and services, has increasing and serious drawbacks. With the rise of high quality displays and more ergonomic human computer interaction mechanisms such as mice, touch-pads and touch-screens, graphical passwords are credited as a valuable replacement to old-fashioned passwords. In contrast to alphanumerical passwords, graphical authentication mechanisms promise greater memorability and usability. In this chapter, an overview of the state-of-art of this topic is presented, introducing some of the main schemes proposed in current literature. The issues and concerns related to security and usability, which still challenge the researchers in this area, are also discussed.

Chapter 7

Security evaluation is a complex problem. As more and more software systems become available, more diversity and alternatives can be found to accomplish the same tasks. However, there is still a lack of a standard approach that can be used to choose among the available alternatives or evaluate their configuration security. In this chapter, the authors present a methodology to devise security appraisals, which is based on the collection of widespread security knowledge for a specific domain. They demonstrate their methodology by devising two specific appraisals for the domain of transactional systems. The first one can be used to evaluate and assess the configuration of an already deployed database installation, while the target of the second one is to compare the capability of specific database brands concerning security aspects. The authors also present a real demonstration of both appraisals in real scenarios.

Chapter 8

Regulatory compliance in areas such as privacy has become a major challenge for organizations. In large organizations there can be hundreds or thousands of projects that involve personal information. Ensuring that all those projects properly take privacy considerations into account is a complex challenge for accountable privacy management. Accountable privacy management requires that an organization makes sure that all relevant projects are in compliance and that there is evidence and assurance that

this actually is the case. To date, there has been no suitable automated, scalable support for accountable privacy management; it is such a tool that the authors describe in this chapter. Specifically, they describe a privacy risk assessment and compliance tool which they are developing and rolling out within a large, global company – called HP Privacy Advisor (HP PA) – and its generalisation and extension. The authors also bring out those security, privacy, risk, and trust-related aspects they have been researching related to this work in particular.

Secure information splitting is used in many tasks of the intelligent sharing of secrets and key data in business organisations. The significance of information splitting depends on its nature, while the significance of information sharing may depend on its importance and the meaning it has for the organisation or institution concerned. This chapter presents models for multi-level information splitting and information management with the use of the linguistic approach and formal grammars. Such methods constitute a secure enhancement of traditional secret splitting algorithms and introduce an additional stage at which information is coded using the appropriately defined regular or context-free grammar. The many possible applications of such methods include their use for the intelligent management of important or confidential information in government institutions or businesses. Algorithms of multi-level information splitting allow information that is not available to all employees of a given organisation or its environment to be securely split or shared.

Due to the huge growth in the need for using Web applications worldwide, there have been huge efforts from programmers to develop and implement new Web applications to be used by companies. Since a number of these applications lack proper security considerations, malicious users will be able to gain unauthorized access to confidential information of organizations. A concept called SQL Injection Attack (SQLIA) is a prevalent method used by attackers to extract the confidential information from organizations' databases. They work by injecting malicious SQL codes through the web application, and they cause unexpected behavior from the database. There are a number of SQL Injection detection/prevention techniques that must be used in order to prevent unauthorized access to databases.

Though embedded applications were originally built on standalone devices, nowadays these devices require a growing integration with other systems through their interconnection with TCP/IP networks. Web Services, which provide a service oriented distributed architecture for the interconnection of systems through TCP/IP networks, have been widely adopted for the integration of business applications, but this sort of integration is still not widely provided by embedded applications. The present work aims to demonstrate the feasibility of using Web Services for the integration of embedded applications running

on heterogeneous architectures. This is achieved through the provision of a support for the development and deployment of web services for embedded applications. Basic objective of the system developed is to monitor and control Humidity and Temperature through Internet using interactive computer front end. The feasibility of this approach in terms of security and authentications of its Internet users is demonstrated by developing an mail server along with application deployed. Mail server keeps track of authorised users' with login password and email ID in a database table. This information is used to identify authorised users who are allowed to make changes in control parameters of the stated embedded application.

P2P networks have characteristics of decentralization, autonomy, and dynamicity. The security problems caused by these characteristics have seriously affected further development of P2P networks. The authors did research on CL-PKC key management schemes. (1) They propose a certificateless-based key distribution scheme with multiple trusted centers that fits the characteristics of P2P networks, and analyzed its security. (2) They also propose an improved interactive key agreement protocol across multiple domains, and then compare it with some existing key agreement protocol from aspects of security and computational efficiency. (3) The authors have implemented the proposed key management schemes, then verified their correctness and tested their computational efficiency. Combined with master key share management and key management of nodes, this system constructed a complete certificateless-based key management model, which is an exploration to solve security problems in P2P networks.

Privacy for Service-Oriented Architecture (SOA) is required to gain the trust of those who would use the technology. Through the use of an independent Privacy Service (PS), the privacy policies of a service consumer and provider can be compared to create an agreed upon privacy contract. In this chapter, the authors further define a metamodel for privacy policy creation and comparison. A trust element is developed as an additional criterion for a privacy policy. The authors define the PS, outline what operations it must perform to accomplish its goals, and present how the PS operates in different scenarios. They believe the PS, combined with the enhanced metamodel, provides a strong solution for providing privacy in an SOA environment.

Security inspections are increasingly important for bringing security-relevant aspects into software systems, particularly during the early stages of development. Nowadays, such inspections often do not focus

specifically on security. With regard to security, the well-known and approved benefits of inspections are not exploited to their full potential. This book chapter focuses on the Security Goal Indicator Tree application for eliminating existing shortcomings, the training that led to their creation in an industrial project environment, their usage, and their reuse by a team in industry. SGITs are a new approach for modeling and checking security-relevant aspects throughout the entire software development lifecycle. This book chapter describes the modeling of such security goal based trees as part of requirements engineering using the GOAT tool dedicated plug-in and the retrieval of these models during the various phases of the software development lifecycle in a project by means of Software Vulnerability Repository Services (SHIELDS, Software Vulnerability Repository Services) created in the European project SHIELDS (SHIELDS, SHIELDS - Detecting known security vulnerabilities from within design and development tools).

Chapter 15

Today, Peer-to-Peer SIP based communication systems have attracted much attention from both academia and industry. The decentralized nature of P2P might provide the distributed peer-to-peer communication system without help of the traditional SIP server. However, the decentralization features come to the cost of the reduced manageability and create new concerns. Until now, the main focus of research was on the availability of the network and systems, while few attempts were put on protecting privacy. In this chapter, the authors investigate P2PSIP security issues and introduce two enhancement solutions: central based security and distributed trust security, both of which have their own advantages and disadvantages. After that, they study appropriate combination of these two approaches to get optimized protection. Their design is independent of the DHT (Distributed Hash Table) overlay technology. The authors take the Chord overlay as the example, and then analyze the system in several aspects: security & privacy, number-of the hops, message flows, et cetera.

Chapter 16

The role of human behaviour in enterprise security is one of the little studied aspects. The author proposes a reinforcement model of collaborative security employing basic concepts from game theory, socio-psychology, and probabilistic model-checking. The proposed model aims towards solving the problem of inducing positive network effect to enable user centric monitoring of security violations, in particular, against violations related to "semantic manipulation" of context dependent logical resources. Preventing such violations using existing security enforcement mechanisms is neither feasible nor cost effective. The author defines a payoff mechanism to formalize the model by stipulating appropriate payoffs as reward, punishment, and community price according to reporting of genuine or false violations, non-reporting of the detected violations, and proactive reporting of vulnerabilities and threats by the users. Correctness properties of the model are defined in terms of probabilistic robustness property and constraints for economic feasibility of the payoffs. For estimating the payoff parameters, system and user behaviours are further modelled in terms of probabilistic finite state machines (PFSM) and likelihood of the success of the model is specified using probabilistic computation tree logic (PCTL). PRISM model checker based automated quantitative analysis elicits the process of the estimation of various parameters in the model using PFSMs and PCTL formulas.

In this chapter, the authors propose the expression and the modelling of the most important principles of privacy. They deduce the relevant privacy requirements that should be integrated in existing security policy models, such as RBAC models. They suggest the application of a unique model for both access control and privacy requirements. Thus, an access control model is to be enriched with new access constraints and parameters, namely the privacy contexts, which should implement the consent and the notification concepts. For this purpose, the authors introduce the Privacy-aware Organisation role Based Access Control (PrivOrBAC) model.

In this chapter, first the authors discuss the current trends in the usage of formal techniques in the development of e-voting system. They then present their experiences on their usage to specify and verify the behaviors of one of currently deployed e-voting systems using formal techniques and verification against a subset of critical security properties that the system should meet. The authors also specified attacks that have been shown to successfully compromise the system. The attack information is used to extend the original specification of the system and derive what we called the extended model. This work is a step towards fostering open specification and the (partial) verification of a voting machine. The specification and verification was intended as a learning process where they would use formal techniques to improve the current development of e-voting systems.

CAPTCHAs are employed on websites to differentiate between human users and bot programs that indulge in spamming and other fraudulent activities. With the advent and advancement of sophisticated computer programs to break CAPTCHAs, it has become imperative to continuously evolve the CAPTCHA schemes in order to keep the Internet network and website free of congestion and spam-bots. In light of these developments concerning information security, in this chapter, the authors introduce the novel concept of Scrambled CAPTCHA, which is a combination of OCR-based and Picture CAPTCHAs and exploits an inherent characteristic of human vision and perception. They also introduce Hindi CAPTCHA, developed in Hindi language (Devanagari script). This CAPTCHA will typically address spamming on Indian websites. It also contributes to the digitalization of books written in this script. The authors also discuss the features and security aspects of these schemes in detail, which, to the best their knowledge, had not been implemented earlier.

own security rules, which can be shared and improved through exchanges with others devices. With this new approach, called grid of security, a community of devices ensures that a device is trustworthy and that communications between devices progress in respect of the control of the system policies. To support this approach, the authors present a new communication model that helps structuring the distribution of security services among the devices. This can secure both ad-hoc, local-area or enterprise networks in a decentralized manner, preventing the risk of a security breach in the case of a failure.

Fine-grained malware analysis requires various powerful analysis tools. Chief among them is a debugger that enables runtime binary analysis at the instruction level. One of the important services provided by a debugger is the ability to stop execution of code at arbitrary points during runtime, using breakpoints. Software breakpoints change the code being analyzed so that it can be interrupted during runtime. Most, if not all malware are very sensitive to code modification with self-modifying and/or self-checking capabilities, rendering the use of software breakpoints limited in their scope. Hardware breakpoints on the other hand, use a subset of the CPU registers and exception mechanisms to provide breakpoints that do not entail code modification. However, hardware breakpoints support limited breakpoint ability (typically only 2-4 locations) and are susceptible to various anti-debugging techniques employed by malware. This chapter describes a novel breakpoint technique (called stealth breakpoints) that provides unlimited number of breakpoints which are robust to detection and countering mechanisms. Further, stealth breakpoints retain all the features (code, data and I/O breakpoint abilities) of existing hardware and software breakpoint schemes and enables easy integration with existing debuggers.

One cannot develop effective economic models for information security and privacy without having a good understanding of the motivations, disincentives, and other influencing factors affecting the behavior of criminals, victims, defenders, product and service providers, lawmakers, law enforcement, and other interested parties. Predicting stakeholders' actions and reactions will be more effective if one has a realistic representation of how each of the various parties will respond to internal motivators and external stimuli. In this chapter, reactions of involved parties are assumed to be based on "personal utility functions." However, it is not sufficient merely to develop static utility functions, since the net value of security and privacy changes dynamically. External events, such as the announcement of a new threat, also have a significant effect on both subjective and objective net value. Knowing how such value functions vary over time helps determine the overall dynamic impact of security and privacy measures on the behavior of various participants and ultimately on the economic model that describes these behaviors. Also in this chapter, the authors enumerate the many factors that affect all the various parties and examine how these factors affect the responses of all those involved due to the economic impact of particular exploits and situations as they affect different groups.