1

Privacy and Security Issues in a Digital World

Milan Petković[1] and Willem Jonker[2]

[1] Philips Research, The Netherlands
[2] Twente University & Philips Research, The Netherlands

Summary. This chapter reviews the most important security and privacy issues of the modern digital world, emphasizing the issues brought by the concept of ambient intelligence. Furthermore, the chapter explains the organization of the book, describing which issues and related technologies are addressed by which chapters of the book.

1.1 Introduction

This book addresses security, privacy and trust issues in modern data management in a world where several aspects of ubiquitous computing and ambient intelligence visions are emerging. In the sequel, we give a short introduction to these issues and explain how the book is organized. The book consists of five parts. Following this introduction, the first part of the book contains two chapters on security and privacy legislation and ethics in this digital world.

Chapter 2 focuses on the common issues and developments in privacy law in relation to technology. This chapter explains the system of privacy protection in the law and surveys the internationally accepted privacy principles which form the basis of the law in most jurisdictions. Next to that, the most important interpretation rules by the courts are given and their applications to technology are discussed. Finally, the chapter gives an outlook on the future of the privacy law.

Chapter 3 reviews ethical aspects of information and system security and privacy. First it focuses on computer security, addressing topics such as the relation between computer security and national security, and then it concentrates on moral aspects of privacy and the impact of information technology on privacy.

The rest of the book is organized as follows. Part II covers security issues of modern data management. Privacy is addresses in Part III. Part IV deals with digital asset protection technologies while Part V provides a selection of more-specific issues brought about by the concepts of ambient intelligence and ubiquitous computing. The following sections introduce security, privacy and content protection issues, explaining in more detail each part of the book.

1.2 Security Issues

As already mentioned, information pervasiveness, along with all its benefits, brings concerns with respect to security issues. Data is no longer hidden behind the walls of a fortress. It does not reside only on mainframes physically isolated within an organization where all kind of physical security measures are taken to defend the data and the system. Systems are increasingly open and interconnected, which poses new challenges for security technologies. Instead of being a protection mechanism, as it is today, security will in the future serve as an enabler for new value-added services. The trends mentioned in the previous section influence every security mechanism. Therefore, Part II of this book covers fundamental security technologies and introduces advanced techniques.

Large and open distributed systems need flexible and scalable access control mechanisms where user authorization is based on their attributes (e.g. credentials). Consequently, languages and mechanisms for expressing and exchanging policies are indispensable. The basics of access control, including discretionary and mandatory access policies, administrative policies, as well as the aforementioned challenges, are described in Chap. 4.

The concept of role-based access control (RBAC) faces similar challenges. Chapter 5 introduces the basic components of RBAC and gives some guidelines with respect to emerging problems of designing role hierarchies in different environments.

Extensible markup language (XML) security provides an important opportunity to fulfill new requirements posed by the concepts of ubiquitous computing and ambient intelligence. It allows access privileges to be defined directly on the structure and content of the document. Chapter 6 describes the main characteristics of the key XML technologies such as XML signature, XML encryption, key management specification and policy languages.

The rising trend of openness also affects databases. An organization internal database of yesterday is today already open for access by users outside the organization. A number of attacks exists that exploits web applications to inject malicious SQL queries. Databases are facing insider threats as key individuals (often administrators) control all sensitive information and infrastructure. Chapter 7 provides most relevant concepts of database security, discusses their usage in prevalent database management systems, such as Oracle, DB2, and MySQL, and covers a number of challenges including the ones mentioned above.

As already mentioned, advanced security technologies should enable new services in the open environment of the future. Trust management is an important mechanism closely related to security that supports interoperation, exactly in this open environment. Therefore, trust management systems are becoming increasingly important and getting more and attention. In Chap. 8, state-of-the-art systems are described, as well as several research directions, such as trust negotiation strategies and reputation-based systems.

Consequently, the issue of trusting a computing platform to perform a task as expected is rising. There a new initiative on trusted computing plays an important role. It is expected that it will allow computer platforms to offer an increased level of security, making computers safer, less prone to viruses and malware and therefore more reliable. Trusted platform modules as well as the consequences for authentication, secure boot, protected execution, secure I/O and other related technologies are described in Chap. 9.

To further elaborate on the physical aspects of a trusted computing platform, this part of the book is completed with Chap. 10 on physical unclonable functions (PUFs). A PUF is a hardware system that realizes a function that is difficult to model and reproduce. This chapter describes their role in the security of modern data management systems and elaborates on the two main applications of PUFs, namely unclonable and cost-effective way of storing cryptographic key material and strong authentication of objects.

1.3 Privacy Issues

A number of privacy issues also arise with the proliferation of digital technologies. Personalized services, such as reward programs (supermarket cards, frequent flyer/buyer cards, etc.) require collection, (uncontrolled) processing, and often even distribution of personal data and sensitive information. With ubiquitous connectivity, people are increasingly using electronic technologies in business-to-consumer and business-to-business settings. Examples are financial transactions, credit card payments, business transactions, email, document exchange, and even management of personal health records. Furthermore, new technologies are being used for the purpose of monitoring and recording behaviors of individuals who may not even be aware of it. This data typically includes personal information and is essentially privacy sensitive. The flow of this information will almost certainly get out of the individuals' control, thus creating serious privacy concerns. Therefore, there is an obvious need for technologies that support these new services but ensure people's privacy. Part III of this book addresses these concerns and provides an overview of the most important privacy-enhancing technologies.

Thanks to the same trends described above, data mining technologies are becoming increasingly used. Organizations are creating large databases that record information about their customers. This information is analyzed to extract valuable nonobvious information for their businesses. However, these techniques are particularly vulnerable to misuse and revealing of individual data records. Chapter 11 deals with privacy-preserving data mining technologies that have been developed for this problem. It presents multiparty computation and data modification as the two main techniques currently used.

Chapter 12 continues on a similar topic, which is the protection of privacy-sensitive data used for statistical purposes. It presents the model and concepts of a statistical database and surveys two important techniques for privacy preservation: restriction and noise addition.

With increased connectivity data confidentiality becomes increasingly important. Although cryptographic techniques, which consequently gain more attention, solve basic problems, they also introduce new ones such as searching encrypted data. The basic problem is that it is difficult to search in an outsourced database in which the data is encrypted. Chapter 13 reviews and compares several search methods that support searching functionality without any loss of data confidentiality.

Chapter 14 extends on previous chapters and addresses a specific problem in multiparty computation of a server and a resource-limited client. It introduces a framework of secure computation based on threshold homomorphic cryptography and the necessary protocols needed for this specific setting. Then, the chapter describes two applications of this framework for private biometrics and secure electronic elections.

As already mentioned, people nowadays are involved in an increasing number of electronic transactions with a number of parties. These transactions usually include authentication and attribute exchange. To secure them and protect his privacy the user has to maintain a number of user names/passwords with these organizations. This is exactly the problem addressed by federated identity management technologies. Chapter 15 introduces two approaches to solve the aforementioned problems: browser-based federated identity management and private credentials.

The privacy-enhancing technologies presented in this part of the book often require anonymous communication channels and appropriate protocols. Furthermore, an important requirement in many systems is accountability, which is often conflicting with anonymity. Chapter 16 introduces the concept of controlled anonymous communications, presents the main building blocks of an anonymity infrastructure and shows how they can be used to build a large-scale accountable anonymity system.

1.4 Digital Asset Protection Issues

Digital content distribution is one of the fastest emerging activities nowadays. The trend towards digital content distribution gives great opportunities for commercial content providers and consumers, but also poses some threats, as digital content can be very easily illegally copied and distributed. Therefore, commercial content providers need technologies accompanied by legislation which can prevent illegal use of digital content. Digital rights management

(DRM) is a collection of technologies that provides content protection by enforcing the use of digital content according to granted rights. It enables content providers to protect their copyrights and maintain control over distribution of and access to content. Part IV of this book is devoted to these digital rights management technologies.

Chapter 17 gives an introduction to digital rights management. This chapter reviews the early approaches and explains the basic concepts of DRM using the Open Mobile Alliance DRM system as an example.

The fight against piracy started however with copy protection systems. The early methods dealt with audio and video tapes while copy protection is now an integral part of the distribution of all forms of digital content and software on mainly optical media. A historical overview of copy protection techniques is given in Chap. 18, which also describes popular copy protection techniques.

Chapter 19 elaborates on digital watermarking, which allows the addition of hidden verification messages (e.g. copyright) to digital data such as audio/video signals. As opposed to encryption-based DRM systems, watermarking-based systems leave the content in the clear, but insert information that allows usage control or usage tracking. This chapter describes the basic principles of digital watermarking and discuss its application to forensic tracking.

DRM systems are often accused of being against the consumers. In fact, initially, they are built to protect the interest of content owners. Chapter 20 looks at DRM systems from the consumer perspective and introduces two basic concepts relevant for them: authorized domains and person-based DRM. Finally it devotes special attention to the combination of the two, its architecture, user, license, and domain management.

Another big issue in DRM is interoperability. To achieve wide adoption of DRM technology, simple and seamless user experience is indispensable. Finally the dream of many people is that digital content will be available to anyone, anytime, anywhere, on any device. Therefore, DRM technology providers must find ways to make their products interoperable. This topic is addressed in Chap. 21. The chapter defines the interoperability problem and discusses it on three different layers: protected content, licenses, and trust and key management. Then, it describes state-of-the-art solutions to these problems on the level of platform and interfaces. Furthermore, business and user aspects in relation to DRM interoperability are discussed.

In parallel to the introduction of commercial multimedia download services, there is also a clear increase in the production of digital information such as digital photos and home videos by consumers. As a consequence, consumers have to deal with an ever-growing amount of personal digital data, alongside downloaded commercial content. Some of this personal content might be highly confidential and in need of protection. Consequently, the consumer wants to share it in a controlled way so that he can control the use of his content by persons with whom he shares it. Such a DRM system for controlled sharing of personal content is presented in Chap. 22. The chapter starts with scenarios and requirements and continues with the introduction of the DRM approach and the system architecture. Finally, the chapter presents practical solutions for protecting and sharing personal content as well as for ownership management and multiple-user issues.

Chapter 23 addresses privacy issues in DRM systems. The main challenge is how to allow a user to interact with the system in an anonymous/pseudonymous way, while preserving all the security requirements of usual DRM systems. To achieve this goal a set of protocols and methods for managing user identities and interactions with the system during the process of acquiring and consuming digital content is presented. Furthermore, a method that supports anonymous transfer of licenses is discussed. It allows a user to transfer a piece of content to another user without the content provider being able to link the two users.

1.5 Privacy and Security in an Ambient World

The vision of ambient intelligence (AmI) assumes that technology is present everywhere in the form of smart computing devices that respond and adapt to the presence of people. The devices communicate with each other, and are nonintrusive, transparent, and invisible. Moreover, as communication is expected to happen anytime, anywhere, most of the connections are done in a wireless and often ad hoc manner.

The concepts of ambient intelligence and ubiquitous computing that will have a major influence on security and privacy are:

- Ubiquity: smart digital devices will be everywhere and part of the living environment of people. They will be available, for instance, when driving a car or waiting for the train to arrive.
- Sensing: as already mentioned, the environment will be equipped with a large number of sensors. The sensors will gather information about general things like room temperature, but can also register who enters a room, analyze the movement of a person and even sense his/her emotional condition.
- Invisibility: the devices and sensors will not only be everywhere, but will also largely disappear from sight. People will not even be aware that sensors are monitoring them. Moreover, there is a big fear that control over personal information will get out of the hands of users.
- Memory amplification: the information gathered by the sensors will be stored and used for later behavior prediction, improving support of the ambient environment. No matter how sensitive the information is, there is a large chance that it will be stored and used for different purposes.
- Connectivity: smart sensors and devices will not only be everywhere but they will also be connected to each other. Connectivity also implies no control over dissemination of information. Once information has been collected it can end up anywhere.

- Personalization: in addition to connectivity, a chief concept to ambient intelligence is that of personalization. Personalization implies that information about the user must be collected and analyzed by the environment in order for adaptation to that user to happen. The environment will keep track of specific habits and preferences of a person. However, the concept of personalization is, in principle, contradictory to the privacy concepts of anonymity and pseudonymity.

As mentioned above, future ambient environments will integrate a huge amount of sensors (cameras, microphones, biometric detectors, and all kinds of sensors), which means that the ambient will be capable of capturing some of the user's biometrics (face, speech, fingerprints, etc.). Consequently, the ambient environment will be able of cross-referencing the user's profile, activities, location and behavior with his photo, for example. Furthermore, the concept of omnipresent connectivity may make it possible that biometric data could be cross-referenced with some public databases, which will result in the disclosure of the user identity.

It is obvious that security and privacy issues brought by the future ambient world go beyond the threats people are used to nowadays. On the other hand, people are increasingly aware and concerned about their privacy and security. Therefore, it is very important to investigate how the level of privacy and security which people currently have can be kept after the introduction of these new concepts. Furthermore, it is important to develop methods that will build trust in these new concepts.

Part V of this book addresses specific privacy and security topics of the ambient world. It starts with an introduction to ambient intelligence in Chap. 24. This chapter briefly revisits the foundations of ambient intelligence. Then, it introduces notions of compliance and ambient journaling to develop an understanding of the concept of ambient persuasion. Finally, the ethics of ambient intelligence is also addressed.

The following chapters address the privacy concerns mentioned above, beginning with privacy policies. Chapter 25 deals with different stages in the lifecycle of personal data processing, the collection stage, the internal processing stage and the external processing stage, which is typical for ambient intelligence scenarios. It reviews technologies that cover each of these stages, the platform for privacy preferences (P3P) for the collection stage, the platform for enterprise privacy practices (E-P3P) for the processing stage and audit logic for the external processing stage.

The semantic Web goes one step beyond the above mentioned exchange of information. It envisions a distributed environment in which information is machine-understandable and semantically self-describable. This in turn requires semantically enriched processes to automate access to sensitive information. Chapter 26 extends on the previous chapter, describing exchange and interaction of privacy policies on the semantic Web as well as the role of ontologies for conflict detection and validation of policies.

As already mentioned, in the future world of ambient intelligence it is expected that a user will be required to perform identification regularly whenever he changes environment (e.g., in a shop, public transportation, library, hospital). Biometric authentication may be used to make this process more transparent and user friendly. Consequently the reference information (user's biometrics) must be stored everywhere. However this information is about unique characteristics of human beings and is therefore highly privacy sensitive. Furthermore, widespread use of this information drastically increases chances for identity theft, while the quantity of this information is limited (people only have two eyes). In Chap. 27, a novel technology, called biometric template protection, that protects the biometric information stored in biometric systems is introduced.

Radio-frequency identification (RFID) is an automatic identification method that is expected to be prevalently used in the future concepts of ambient intelligence and ubiquitous computing. The number of potential applications is large. However, with its first deployment public fears about its security and privacy exploded. Chapter 28 is devoted to privacy of RFID tags. It introduces the RFID technology, provides an overview of RFID privacy challenges as well as an overview of proposed technical RFID privacy solutions. Furthermore, it considers the problem taking into account applications and policy to evaluate the feasibility of the proposed solutions.

Last but not least, in Chap. 29, the book devotes attention to malicious software and its evolution in the context of ubiquitous computing and ambient intelligence. This chapter brings the reader from current malicious software and defending methods to a projection of the problems of future systems, taking into account the aforementioned aspects of ambient intelligence.