Preface

We are witnessing a rapid growth of technological and business interest towards distributed computing environments, also named Global or Integrated Computing environments. The features of these environments include mobility, open-endedness, heterogeneity of data and applications, mobility of computing entities on a variety of devices, network systems, and logical and physical interconnections channels. In these systems, various resources (applications, data and repositories, as well as user contexts scenarios) demand to be merged under common interoperability paradigms, possibly based on standards and common policies, as well as on enabling technologies for interconnection, such as web Services, internetworking connection technologies, or distributed code and data management. Heterogeneity is a key factor in interconnection: the ability to manage it means the possibility to manage distributed and differently structured and managed resources under unifying paradigms for computing resources and networks.

In this scenario of integrated environments, the ability to create and manage large shared systems in a secure manner is an area that has received attention in various ways, from formal research to practical approaches, methods, and products. A comprehensive, systems approach to security is required if security consolidation is to succeed. This book serves as a forum to describe security threats, technologies, methodologies and deployment in the area of systems integration. The book collects submissions from academia and industry presenting research and development on theoretical and practical aspects related to designing, building and managing secure distributed systems.

The included topics range from Cryptographic Algorithms to Key Management and Public Keys Infrastructures for Security Management, from Authorization Frameworks for Security and Trust management to Models of Security in Federated Systems and Security for Internet Service Oriented Architectures and web-managed data formats.

BOOK AIMS

The basic aim of the volume is to state the point of recent achievements in the field of security related to the interconnection of computers and applications through internetworking. In fact, the Internet is a worldwide collection of networks that are accessible by individual computing hosts in a variety of ways, including gateways, routers, dial-up connections, wireless networks and Internet service providers. In principle, the Internet is easily accessible to any person endowed with a computer and a network connection; individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries or time of day. However, along with the convenience and easy access to information, new risks for security of information and personal data arise. First, the general risk is that valuable information will be lost, stolen, corrupted, or misused and that the computer systems, that is, its valuable data and applications, will be corrupted or damaged. It is well known and accepted that information electronically managed and available on networked computers is vulnerable: intruders do not need to enter an office or a building, and may be located anywhere. They can steal or tamper information without touching a paper or a computing device, creating new or altered files, run their own programs, and, particularly, they can easily hide evidence of their unauthorized activity, practically leaving no trace of their actions.

Concepts

Just to briefly review the basic security concepts, important to *information on internetworking applications*, we remind confidentiality, integrity, and availability. Concepts relating to *information users* are instead authentication, authorization, and non-repudiation.

When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. For some types of information or organizations and companies, confidentiality is a very important attribute. Examples include research data, medical and insurance records, new product specifications, and corporate investment strategies. In some locations, there may be a legal obligation to protect the privacy of individuals. This is particularly true for banks and loan companies; debt collectors; businesses that extend credit to their customers or issue credit cards; hospitals, medical doctors' offices, and medical testing laboratories; individuals or agencies that offer services such as psychological counseling or drug treatment; and agencies that collect taxes.

Besides, information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting.

Information can be erased or become inaccessible, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need.

Availability is often the most important attribute in service-oriented businesses that depend on information (e.g., airline schedules and online inventory systems). Availability of the network itself is important to anyone whose business or education relies on a network connection. When a user cannot get access to the network or specific services provided on the network, they experience a denial of service.

To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Authentication, which is the way to prove that a user is whom he/she claims to be, needs involved parties to provide a "proof." This may involve something the user knows (such as a password), something the user has (such as a "smart card"), or something about the user that proves the person's identity (such as a fingerprint). Authorization is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a remote file or running a program. It is nowadays well accepted that authentication and authorization go hand in hand. Moreover, security is strong when the means of authentication cannot later be refuted — the user cannot later deny that he or she performed the activity. This is known as non-repudiation.

QUESTIONS

The book addresses several questions, such as: What kind of crypto algorithms are being used and are emerging? What kind of certificate and public key infrastructure is the appropriate one for the global Internet? What is the state-of-the-art of certificates in solving authentication problems, and how can authorization problems be solved in a distributed environment? What security problems are emerging in distributed federated databases and document management systems or in distributed code? For example, the information industry is heading rapidly towards adopting Java as the programming language for the Internet. Will the Java Sandbox approach be sufficient to fulfill users' and industrial needs for building the global information infrastructure? For smart cards, industry studies indicate that there could be some 2.5 to 3 billion smart cards in use by the turn of the century. Major users of these joint smart card technologies are forecast to include telecommunications, banks, hotels, airlines and insurance companies, as well as healthcare providers and governments. Smart cards, however, are limited in their processing power and storage capacity, which most security algorithms require. How will the industry solve these shortages and what impact smart cards have on enhancing individuals' security and privacy?

Finally, recent proposals suggest a peer-to-peer relation between the client and the server, where the server will be able to push some content to client(s). Will push technology invade individuals' privacy and create a flooded Internet; or should it be regulated to become subscription based?

Will governments open the national boundaries and stop regulating the encryption technology as well as giving common rules and standards for designing lightweight security algorithms and trusted systems? Will it be possible to build Intranet/Extranets and Virtual Private Networks with full security? Finally, will the Internet and e-commerce rise to the expectation and flourish in the global village? The answers to these questions are yet to be seen.

SECURITY AS A BUSINESS PROBLEM

Information security is today also a business problem, besides a technological problem. With the focus on information security in the media, and in legislatures around the world, organizations are facing complex requirements to comply with security and privacy standards and regulations. This is forcing the discussion of information security into boardrooms, as more executives and boards of directors understand their responsibility and accountability in information security governance. Current topics of discussion in the security field are driven mainly by the following issues:

- *Focus on information security:* The awareness of the challenges and issues to be faced in information security has grown. Through the media, government, cyber-attacks/crimes, and proliferation of vulnerabilities in products, information security continues to receive increased focus.
- *Technology to protect information:* As a result of successful attacks (such as Code Red and Nimda), the organizations have acknowledged that security products are not a complete solution to security problems, but rather security is a business and organizational problem.
- *Standards, regulations and legislation:* Companies and organizations have to face complex standards and regulations. Even within very specific, vertical areas, such as banking services, the complexity to meet security requirements is driven by the presence of different regulations (e.g., the U.S. Gramm-Leach-Biley Act of 1999 (GLBA), Basel Accords, Securities and Exchange Commission (SEC) requirements, U.S. Patriot Act). A complex set of requirements is emerging while organizations cross the international boundaries.
- *Legal liability:* In 2002, legal liability from security has been stated. Organizations and software vendors are being pushed towards a higher degree of accountability for security by their customers.

- *Business partners demanding security:* Organizations have to prove that they are managing data and applications in a secure way, that is, they are applying security to a level that can satisfy their business partners. This goes beyond discussing what security products are installed; this requires that organizations be able to communicate compliance and management practice of security. For example, in the U.S., the National Strategy to Secure Cyberspace released by the White House recommends that organizations disclose their security audit and compliance status.

As a consequence, organizations can expect to see increased regulation, specifically in industry areas that are considered as critical, such as finance, transportation, communication, health care, energy, and utilities. Furthermore, regulatory requirements will come up from governments seeking to boost information security. Luckily, *information security* has turned into a well founded and defined *profession*, and many common security services will continue to be valuable and a real necessity — vulnerability management, secure communications, penetration testing, policy design, intrusion detection — while others may be changing or evolving radically.

Currently, information security is turning from awareness into action in many corporate environments, building on what we have seen in the last decade. Boards of directors and executive management are paying closer attention to their responsibilities in the protection of their information assets. Moreover, we are assisting at an increased focus on certification and accreditation with continuous assessment: as organizations face compliance obligations, or standards and best practices to manage information protection plans, we observe a focus on the certification and accreditation of system security before production implementation. This will be followed by the development of a continuous assessment process to manage risk and compliance with standards and regulations. For example, ISO17799 and BS7799 have become the de facto standards for defining (at a high level) an information security program/architecture. Also, the Common Criteria product certification is more and more widely pursued and recognized: with the mandate that security products be Common Criteria certified in order to be purchased, at least by U.S. Department of Defense Agencies, a significant increase is obtained in the adoption of Common Criteria certification.

INTEGRATION TECHNOLOGIES

In the *integration of different systems* into a distributed global system, issues of data dissemination, access to a variety of applications, disseminated users of various typologies and with heterogeneous needs bring about new security needs. To mention just a few aspects, an integrated system must be able to:

- Authenticate users and applications in a distributed way;
- Selectively grant and revoke access rights to users of the distributed system;
- Encrypt data in an effective and yet efficient way both when data are transmitted and when data are stored;
- Treat in a confidential and privacy respectful way the large amount of structured and unstructured data present in various formats: database data, documents, web pages, links, and so on;
- Manage in a uniform way heterogeneous policies regarding data protection;
- Preserve data from sophisticated attacks that exploit the presence of inter-networked databases and systems, such as Trojan Horses attacks, backdoors, distributed denial of service, or statistical inference.

Current trends in *security technology* go towards the improvement of existing security systems, based on new requirements and customer dissatisfaction. For example, signatures and vulnerability management, or Intrusion Detection Systems (IDS) are being redesigned and improved to decrease the number of "false positives" and improving reliability, while preparing for integration of IDS systems with firewalls, crypto systems, authentication and authorization schemes and models, and security management tools. Also, security models in operating systems, in databases and in web-based systems are being improved by adding standardized ACLs, capability modes, and other security features.

Distributed and peer-to-peer systems, e.g., in service oriented architectures, are starting to gain commercial acceptance; in the meanwhile, architectures for distributed services are emerging with reliable hosting, communication security, backups, secure computation, secure content management, and so on. With trends towards distribution, secure communications are increasingly relevant, since hijacking scenarios, or mis-authenticated agents and servers become possible. A key to securing distributed and cryptography-employing systems will be the strong authentication of any message or data, by employing reliable Public Key exchanges and trusted cryptographic identification. Strong authentication may act as foundation for flexible and availability — assuring accounting and billing systems, such as service management, integrated with Quality of Service Standards on the IP level, in combination with wireless authentication.

Luckily, as long as the technology is evolving, the *legislation on the themes of security* of electronically managed information is becoming stricter and demanding at the national and international levels. Rules and laws are requiring producers and manufacturers, application developers, and service providers to adequate their systems to existing and emerging security levels and standards. As a consequence, companies and Public Administrations are more and more constrained both for business problems and for regulation and legislative prob-

lems to protect their data and application patrimony. Not the last are the problems of industrial espionage, of citizens' personal data discovery and of business and image losses due to attacks and to denial of service or discontinuity of services.

This book wants to put a head forward in the direction of integration of technologies tackling the use of new paradigms, such as web access, (wireless) internetworking, web services, and service oriented computing. These have lead to the urgent need for companies, agencies, and administrations to endow their systems with security measures for physical, logical and organizational security.

BOOK ORGANIZATION

Many research and development efforts worldwide are currently focused on providing stronger and more efficient cryptographic algorithms and infrastructures. **Section I** of this volume is devoted to presenting an overview of recent progresses of cryptography and of its usability, as well as advances in one technological area, the one of smart cards.

Mathematical progresses are presented and crypto applications are illustrated, such as in digital signatures, digital certificates, secure data formats, secure communication protocols, time stamping, insurance of Trust, PKI Servers and Wireless LAN certificates. Aspects of authentication mechanisms based on traditional passwords schemes and on truly complex systems, such as smart card based systems, biometrics authentication, and dedicated software systems are then presented. For networks, the basic of techniques remains cryptography, which is able to ensure a large set of security properties; the problem with cryptography lies in the need to produce more and more sophisticated encryption algorithms and in the need to have manageable systems that reveal to be of treatable complexity in front of encryption/decryption cost and time. Hence the problems are to set up efficient cryptographic systems able to generate and handle crypto keys and certificates and to reach a corporate-level structure of cryptography such as PKI systems, requiring an acceptable effort by managers to operate all the aspects related to the presence of a cryptographic system.

Then, the market orientation of a vendor of security products is inserted, providing an insight on security challenges, on a particular, vertical application, i.e., smart cards, but also providing an interesting overview of the security market perspectives.

Another set of efforts in research and development in the security area are devoted to authorization frameworks, which are aimed at ensuring selective access to information. **Section II** of this volume contains articles devoted to models and systems that allow a precise definition of *access rights*, based on a wide range of paradigms, such as DAC and MAC controls, role based access controls, or credential and reputation based controls. These frameworks

are presented with focus on Internet data and applications, such as Internet-based transactions, workflow systems, federated databases, and information exchange in the semantic web, where machines are regarded as "intelligent agents" able to process and make inferences on a large variety of data.

On federated and distributed system, data distribution and dissemination in the networks resources brings about problems of individual privacy, of selective and dynamic authorization to access portions of the data and to deal with data in various formats, such as web-compliant, XML-based data and images, semantic web oriented information, and voice. **Section III** of this volume contains two articles dealing with confidentially and privacy respectful way the large amount of structured and unstructured data present in various formats: database data, documents, web pages, links, video and voice streams, images, and so on.

Subsequently, the book moves to new applications deployed on internetworked environments, tackling security problems in data and application distribution and web services frameworks based on peer-to-peer environments. Some interesting comparisons among distributed development environments are provided, discussing enabling security technologies. **Section IV** of the book examines distributed application hosting services (DAHSs) and next offers an evaluation of claimed security features in some popular products oriented to web service management.

In more detail, the book sections have the following contents.

Section I: Cryptography and Technology

This first section of the book sets the basis for cryptography with some details on algorithms and on crypto-analysis techniques and tools.

Chapter I by Bertoni et al., "Architectures for Advanced Cryptographic Systems," is intended to give an overview of recent developments in modern cryptography. In the last few years, modern cryptography has been dominated by traditional systems, such as DES and RSA. Such systems have provided a secure way for storing and transmitting information, and are nowadays incorporated in many network protocols and secure storage media. However, more recently, the increasing power of crypto-analysis techniques and tools, and the emergence of new applications, such as wireless communications and mobile computing, service-oriented architectures, and integrated systems have stimulated the research and development of innovative cryptographic algorithms. New integrated systems require a more detailed and sophisticated mathematical formalization of cryptographic techniques. This chapter aims at giving the reader a comprehensive understanding of innovative crypto-systems, of their basic structure, of the alternative hardware architectures to implement them, of the application fields, and of their performance requirements and characterizations. Focus is put, among the others, on Advanced Encryption Standard and Elliptic Curve Cryptosystem.

Chapter II by Berbecaru et al., "Digital Certificates and Public Key Infrastructures," is an exhaustive overview of PKI basics, architectures, and applications. Digital Certificates are signed objects containing a set of data bound together by a digital signature. Currently, Digital Certificates can be divided into three classes, based on the data they are bound to: identity certificates (often referred as public-key certificates, PKC) attribute certificates, and authorization certificates. The chapter explores the various possibilities of certificate structures, standards and usages.

Chapter III by Maradan et al., "Smart Card Applications and Systems: Market Trend and Impact on Other Technological Developments," tackles a theme that is strategic in all fields of security and for all types of organizations. The chapter evidences the new needs and requirements for this important authentication support. The diffusion of new communication technologies has pushed smart cards to a very urgent need of applications, although GSM has been the market driver of this authentication means. In this chapter, our will is to provide ideas and trails to explain what make the strengths of smart cards, exploring both technical security issues and market trends. At the same time, the chapter explores the state-of-the-art of hacking techniques, and reveals some counter measures that could redesign modern security platforms. The chapter illustrated the evolution of smart card platforms and their impact on integrated systems, focusing on content protection, e-commerce, and pay TV systems. It finally presents a case study: the e-content protection and Smartright proposal.

Section II: Authorization Frameworks

Chapter IV by Wijesekera et al., "A Flexible Authorization Framework," gives advances in application areas, such as Internet-based transactions, cooperating coalitions, and workflow systems, which have brought new challenges to access control. In order to meet the diverse needs of emerging applications, it has become necessary to support multiple access control policies in one security domain. This chapter describes an authorization framework, referred to as the Flexible Authorization Framework (FAF) that is capable of doing so. FAF is a logic-based framework in which authorizations are specified in terms of a locally stratified rule base. FAF allows permissions and prohibitions to be included in its specification. FAF specifications can be changed by deleting and inserting its rules. We also describe FAF's latest additions, such as revoking granted permissions, provisional authorizations, and obligations.

Chapter V by Rezgui et al., "Enforcing Privacy on the Semantic Web," presents a reputation-based system for web environments aimed at an automatic process of privacy enforcement in a semantic web. Since web services and software agents exchange a large amount of semantically correlated information, the chapter presents a model for assigning a reputation to services. Reputation is a set of attributes built upon "how well" the services has per-

formed in its life cycle using a common perception on the service behavior. Reputation attributes are assigned to services using five criteria defined in the chapter related to security (permeability, authentication-based disclosure of information, correct delivery of data to authorized users, use of cryptography, and seniority seen as period of correct behavior). The architecture presented for a reputation management system sees a Reputation Manager, a set of Probing Agents, and a set of Service Wrappers. The system is distributed to enable support of peer-to-peer applications. Examples are provided in the field of e-government applications.

Section III: Data Distribution and Dissemination on the Net

Chapter VI by Bertino et al., "Secure Data Dissemination," considers the development of a new class of information-centered applications focused on the Selective Dissemination of Information (SDI). The purpose of these applications is the delivery of data to a large user community. "Selective" means that each user should not receive all the data but he/she may receive only specific portions of them. Such portions can be determined according to several factors, such as the user interests and needs, or the access control policies that the data source has in place. Additionally, SDI services can be classified by taking into account additional aspects, such as for instance the adopted distribution mode, the events starting up the distribution, and the network and architecture supporting the service. Due to these reasons, the chapter provides a taxonomy of SDI services and presents a detailed overview of the current approaches. Then, the chapter focuses on security issues for selective data dissemination services. In particular, focus is on four security properties: authenticity, integrity, confidentiality, and completeness, in the scope of Secure SDI applications is wide and heterogeneous. For instance, a relevant scenario for such kinds of applications is related to electronic commerce or digital libraries or electronic news (e.g., stock price, sport news, etc.). In such a case, users subscribe to a source and they can access information on the basis of the fee they have paid. Additionally, the service must ensure that contents are not eavesdropped on during transmission. Another important scenario for Secure SDI applications is data dissemination within an organization or community, where the delivery is controlled by security rules defined by system administrator(s), for instance, documents containing sensitive information about industrial projects.

Chapter VII by Fernandez-Medina et al., "Multimedia Security and Digital Rights Management Technology," considers the crucial topic of multimedia content delivery applications on high bandwidth networks. It considers the pervasiveness of XML as a data interchange format, which has given origin to a number of standard formats for multimedia, such as SMIL for multimedia presentations, SVG for vector graphics, VoiceXML for dialog, and MPEG-21 and MPEG-7 for video. Innovative programming paradigms (such as the one of

web services) rely on the availability of XML-based markup and metadata in the multimedia flow in order to customize and add value to multimedia content distributed via the Net. In such a context, a number of security issues around multimedia data management need to be addressed. First of all, it is important to identify the parties allowed to use the multimedia resources, the rights available to the parties, and the terms and conditions under which those rights may be executed; this is fulfilled by the Digital Rights Management (DRM) technology. Secondly, a new generation of security and privacy models and languages is needed, capable of expressing complex filtering conditions on a wide range of properties of multimedia data. In this chapter, the general problem of multimedia security is analyzed, summarizing the most important XML-based formats for representing multimedia data; a language for expressing access control policies is presented and finally, the most important concepts of the DRM technology are discussed.

Section IV: Service Oriented Computing Frameworks

Chapter VIII by Lin et al., "Data and Application Security for Distributed Application Hosting Services," considers web and Internet services and the emergence of enabling techniques, such as J2EE and .NET, which have led to a trend toward distributed application hosting services (DAHSs). Such hosting services, using rented Internet, computation power, and data storage space to clients are relatively a cheap and effective solution for achieving data and service availability, a balanced load on the servers, and increased scalability. However, these DAHSs, implemented within the Internet environment, introduce many security concerns for the content and application owners. This chapter discusses security concerns for DAHSs, the available security technologies and protocols at different tiers in the Internet information management hierarchy, and the open challenges.

Chapter IX by Fernandez et al., "Comparing the Security Architectures of Sun ONE and Microsft .NET," is an evaluation of claimed security features in a couple of products oriented to web service management. In fact, several companies have announced strategies for supporting web services, all using two basic reference architectures: Microsoft .NET or Sun ONE. Barely these architectures mention security, while the authors rightly point out that this aspect can be one of the fundamental success factors of the products. Therefore, the chapter examines the security features in .NET and ONE web services architectures, in particular, on how web service programs on specialized, shared systems are stored, on how user's data are managed on these shared systems, e.g., on repositories or catalogs. Examined security features are confidentiality and integrity of the web service data, control on the code actions, access control (only paying subscribers can use the service), and service availability.