Network Security
Current Status and Future Directions

Edited by
Christos Douligeris
Dimitrios N. Serpanos

IEEE PRESS

Wiley-Interscience
A John Wiley & Sons, Inc., Publication

Network Security

IEEE Press
445 Hoes Lane
Piscataway, NJ 08854

Network Security
Current Status and Future Directions

Edited by
Christos Douligeris
Dimitrios N. Serpanos

IEEE PRESS

Wiley-Interscience
A John Wiley & Sons, Inc., Publication

Published by John Wiley & Sons, Inc., Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data is available.

ISBN 978-0-471-70355-6

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To
Vicky, Pennie, Kostis, Mariada, and our parents
Christos Douligeris

To
Georgia, Loukia, and my parents
Dimitrios N. Serpanos

Contents

Preface

Network security is a critical parameter in the increasingly connected (networked) world.

Advances in communication systems and protocols, wired and wireless, achieving high speeds, high availability and low cost have enabled the development of high bandwidth backbones and have delivered high throughput to end users of private and public networks. Homes today are able to send and receive high bandwidth, real-time data, enabling high quality communication and a wide range of services. The progress in development, deployment and management of large, reliable networks has resulted not only in the evolution of new services, but to an infrastructure that leads to the provision of a wide range of consumer services that are significantly more cost-effective than traditional ones. It is no surprise that the evolution of all these networks, and especially the Internet—a public network—is changing the economy worldwide.

The continuous deployment of network services over this wide range of public and private networks has led to transactions and services that include personal, and sometimes quite sensitive, data. One only needs to consider simple, everyday services from pay-per-view and cable telephony to bill payments by phone, credit card charging and Internet banking. Such services require significant effort not only to protect the sensitive data involved in the transactions and services, but to ensure integrity and availability of network services as well.

A typical approach to provide these services and increase security and dependability has been to deploy services over private networks, which are easier to protect than public ones. However, the advent of the Internet has changed electronic business models, providing high flexibility, ease of use, and enabling service deployment with substantially lower cost. Thus, the role of network security is significantly more important in emerging network environments, where even private networks connect to the Internet, in order to exploit its multiple advantages.

As the view of traditional distributed systems has changed to a network-centric view in all types of application networks—financial, citizen support, military, etc.—and as the requirement for employing heterogeneous networks and systems becomes increasingly important, the complexity of these systems has led to significant security flaws and problems. The traditional approach to network service development, using several layers and protocols, together with the lack of systematic methods to design and implement secure end systems leads to vulnerabilities and difficulties in implementing and managing security. Attackers continuously find vulnerabilities at various levels, from the network itself to operating systems, and exploit them to crack systems and services.

The result of these phenomena is a significant effort by the research community to address the design and implementation of secure computing systems and networks in order to enable the deployment of secure services. Due to the conventional approaches for service development over such complex, and most often heterogeneous networks and systems, the efforts of the networking community have been several and at various fronts. Thus, currently, there exist several approaches to provide security at various levels and degrees: secure protocols, secure protocol mechanisms, secure services (e.g., phone), firewalls, intrusion detection systems (IDS), etc.

This book considers and addresses several aspects of network security, in an effort to provide a publication that summarizes the main current status and the promising and interesting future directions and challenges. The presented approaches are state-of-the-art, described by leaders in the field. They include trends at several fronts, from Internet protocols to firewalls and from mobile systems to IDS systems.

The chapters of the book are divided into four main sections which consider the main research challenges of today and the important approaches providing promising results for the future: (a) Internet security, (b) secure services, (c) security in mobile systems and (d) trust, anonymity and privacy. In each part several chapters address the main research results and trends. Importantly, we have included 3 appendices of critical background knowledge for the reader who is new to this important research area; the appendices cover (a) a primer in cryptography, (b) legal aspects and (c) standards in network security. Considering the debate about the increasing importance of security in everyday life and the catastrophic results its illegal and unethical use may bring, we believe that the appendices provide a good basis for readers who are interested in the role, restrictions, and limitations of network security in the emerging globally networked world.

In our effort to put this book together, we had the support of several authors, who have written the chapters, providing knowledge and insight through their efforts. The 25 chapters constitute a significant effort on their behalf and we thank them for their efforts. The results of these efforts are a collection of high-quality chapters, which enable the reader to understand the main problems, results, and trends in most aspects of modern network security.

Also, we thank the reviewers of the book, who have provided insightful comments and helped improve the presentation and the quality of the book. Finally, we thank IEEE for its support to this effort and its high-quality work in the production of the final result. As the overall effort has taken longer than expected, we also appreciate the patience of the authors until the production of the final book. We certainly hope that the publication will prove to be a useful tool to all readers interested in network security.

Christos Douligeris
Dimitrios N. Serpanos

Piraeus, Greece
Patras, Greece
March 2007

Contributors

Ioannis Avramopoulos
Department of Computer Science,
Princeton University,
Princeton, New Jersey

Olivier Benoit
Security Labs,
Gemalto, La Ciotat, France

Constantinos Boukouvalas
Research and Development,
OTE SA, Athens, Greece

Mike Burmester
Department of Computer Science,
Florida State University, Tallahassee, Florida

Luis Sousa Cardoso
Portugal Telecom,
Lisboa, Portugal

Anirban Chakrabarti
Department of Electrical and Computer Engineering,
Iowa State University, Ames, Iowa

Lidong Chen
Computer Security Division,
National Institute of Standards and Technology (NIST),
Gaithersburg, Maryland

Vassilios Chrissikopoulos
Department of Archiving and Library Studies,
Ionian University, Corfu, Greece

Joris Claessens
European Microsoft Innovation Center,
Aachen, Germany

Nora Dabbous
Ingenico,
Paris, France

Christos Douligeris
Department of Informatics,
University of Piraeus,
Piraeus, Greece

Laurent Gauteron
Security Labs,
Gemalto, La Ciotat, France

Christian Gehrmann
Ericsson Mobile Platforms AB,
Lund, Sweden

Pierre Girard
Security Labs,
Gemalto, La Ciotat, France

Manimaran Govindarasu
Department of Electrical and Computer Engineering,
Iowa State University,
Ames, Iowa

Yaser Haggag
Department of Computer Science,
Dalhousie University,
Halifax, Canada

Helena Handschuh
Spansion,
Levallois-Perret, France

Angelos D. Keromytis
Department of Computer Science,
Columbia University,
New York, New York

Hisashi Kobayashi
Department of Electrical Engineering,
School of Engineering and Applied Science,
Princeton University,
Princeton, New Jersey

Nikos Komninos
Athens Information Technology,
Peania, Attiki, Greece

Panayiotis Kotzanikolaou
Department of Informatics,
University of Piraeus,
Piraeus, Greece

Arvind Krishnamurthy
Department of Computer Science and Engineering,
University of Washington,
Seattle, Washington

Christian Labonte
Department of Computer Science,
Dalhousie University,
Halifax, Canada

Yugyung Lee
School of Computing Engineering,
University of Missouri—Kansas City,
Kansas City, Missouri

Daniel L. Lough
Global Security Consultants,
Warrenton, Virginia

Rosa Mavropodi
Department of Informatics,
University of Piraeus,
Piraeus, Greece

John C. McEachen
Department of Electrical and Computer Engineering,
Naval Postgraduate School,
Monterey, California

Manish Mehta
School of Computing Engineering,
University of Missouri—Kansas City,
Kansas City, Missouri

Lazaros Merakos
Department of Informatics and Telecommunications,
University of Athens,
Athens, Greece

Andreas Mitrakas
European Network and Information Security Agency (ENISA),
Heraklion, Greece

Aikaterini Mitrokotsa
Department of Informatics,
University of Piraeus,
Piraeus, Greece

Magda M. Mourad
IBM Thomas J. Watson Research Center,
Yorktown Heights, New York

David Naccache
Université Paris II, Panthéon-Assas,
Paris, France

George P. Ninios
Department of Informatics,
University of Piraeus,
Piraeus, Greece

Anthony G. Petropoulos
Department of Informatics,
University of Piraeus,
Piraeus, Greece

Despina Polemi
Department of Informatics,
University of Piraeus,
Piraeus, Greece

Vassilis Prevelakis
Department of Computer Science,
Drexel University,
Philadelphia, Pennsylvania

David J. Robinson
Global Security Consultants,
Odenton, Maryland

Snirivas Sampalli
Department of Computer Science,
Dalhousie University,
Halifax, Canada

Ian G. Schneller
Global Security Consultants,
Odenton, Maryland

Dimitrios N. Serpanos
Department of Electrical and Computer Engineering,
University of Patras,
Patras, Greece

Kapil Kumar Singh
Department of Computer Science,
University of British Columbia,
Vancouver, Canada

Sachin Singh
Heartlab,
Westerly, Rhode Island

Panagiotis Sklavos
Technical Department,
Expertnet SA,
Chalandri, Greece

Stéphane Socié
Security Labs,
Gemalto, La Ciotat, France

Kyriakos Stefanidis
Department of Electrical and Computer Engineering,
University of Patras,
Patras, Greece

Ahmed N. Tantawy
IBM Thomas J. Watson Research Center,
Yorktown Heights, New York

Artemios G. Voyiatzis
Department of Electrical and Computer Engineering,
University of Patras,
Patras, Greece

Son Vuong
Department of Computer Science,
University of British Columbia,
Vancouver, Canada

Randy Wang
Microsoft Research,
Bangalore, India

Claire Whelan
School of Computing,
Dublin City University,
Dublin, Ireland

Christos Xenakis
Department of Informatics and Telecommunications,
University of Athens,
Athens, Greece

John M. Zachary
Department of Electrical and Computer Engineering,
Naval Postgraduate School,
Monterey, California

Alf Zugenmaier
DoCoMo Euro-Labs,
Munich, Germany

Chapter 1

Computer Network Security: Basic Background and Current Issues

Panayiotis Kotzanikolaou and Christos Douligeris

1.1 SOME TERMINOLOGY ON NETWORK SECURITY

The purpose of this chapter is to introduce some basic network security terms and lead the reader through the rest of the book. It provides a baseline level of knowledge in the areas of information technology (IT) security and network security for those readers who are unfamiliar with these concepts. It also provides a set of common terms and definitions which will help those readers who already have some basic knowledge in network security to have a common understanding of the chapters that follow. However, advanced readers with a good background in networking and IT security may skip this chapter and proceed to the more specific areas covered in this book.

A broad definition of *network security* can be constructed by defining its two components, security and networks. Security may be given a wide variety of definitions. According to the *Oxford Dictionary, security is the freedom from danger or anxiety.* Security can also be defined as follows:

- A situation with no risk, with no sense of threat
- The prevention of risk or threat
- The assurance of a sense of confidence and certainty

In traditional information theory [1], security is described through the accomplishment of some basic security properties, namely *confidentiality*, *integrity*, and *availability* of information. Confidentiality is the property of protecting the content of information from all users other than those intended by the legal owner of the information. The nonintended users are generally called unauthorized users. Other terms such as *privacy* have been used almost synonymously with confidentiality. However, the term privacy represents a human attribute with no quantifiable definition. Integrity is the property of protecting information from alteration by unauthorized users. Availability is the property of protecting information from nonauthorized temporary or permanent withholding of information.

Other basic security properties are *authentication* and *nonrepudiation*. Authentication is divided into peer-entity authentication and data origin authentication. Peer entity authentication is the property of ensuring the identity of an entity (also called subject), which

Network Security: Current Status and Future Directions, Edited by C. Douligeris and D. N. Serpanos

may be a human, a machine, or another asset such as a software program. Data origin authentication is the property of ensuring the source of the information. Finally, nonrepudiation is the property of ensuring that principals that have committed to an action cannot deny that commitment at a latter time. Detailed treatment of security properties can be found in several security standards, such as the ISO/IEC (International Organization for Standardization/International Engineering Consortium) 7498-2 [2] and the ITU-T (International Telecommunication Union) X.800 security recommendation [3].

In a practical approach, IT security involves the protection of information *assets* [4]. In a traditional IT risk analysis terminology, an asset is an object or resource which is "worthy" enough to be protected. Assets may be physical (e.g., computers, network infrastructure elements, buildings hosting equipment), data (e.g., electronic files, databases), or software (e.g., application software, configuration files). The protection of assets can be achieved through several security *mechanisms*, that is, aimed at the prevention, detection, or recovery of assets from security threats and vulnerabilities. A security *threat* is any event that may harm an asset. When a security threat is realized, an IT system or network is under a security *attack*. The *attacker* or *threat agent* is any subject or entity that causes the attack. The *impact* of the threat measures the magnitude of the loss that would be caused to the asset or asset owner if the threat were realized against it. A security *vulnerability* is any characteristic in a system which makes an asset more vulnerable to threats. The combination of threats, vulnerabilities, and assets provides a quantified and/or qualified measure of the likelihood of threats being realized against assets as well as the impact caused due to the realization of a threat. This measure is known as the security *risk.* Thus, the security mechanisms provide capabilities that reduce the security risk of a system. Note that system and network security do not rely solely on technical security mechanisms. In almost every information system and network, procedural and organizational measures are generally required in addition to technical mechanisms in order to accomplish the desired security goals.

A *computer network*, or simply a network, is a collection of connected computers. Two or more computer systems are considered as connected if they can send and receive data from each other through a shared-access medium. The communicating entities in a computer network are generally known as *principals, subjects*, or *entities.* These principals can be further divided into *users, hosts*, and *processes*:

- A user is a human entity responsible for its actions in a computer network.
- A host is an addressable entity within a computer network. Each host has a unique address within a network.
- A process is an instance of an executable program. It is used in a client–server model in order to distinguish between the client and the server processes:
  - A client process is a process that makes requests of a network service.
  - A server process is a process that provides a network service, for example, a demon process running continuously in the background on behalf of a service.

A network is considered as a *wired* or *fixed* network if the access medium is some kind of physical cable connection between the computers, such as a copper cable or a fiber-optic cable. On the other hand, a network is considered as a *wireless* network if the access medium relies on some kind of signaling through the air, such as radio frequency (RF) communication. A network can also be divided according to its geographical coverage. Depending on its size, a network can be a personal area network (PAN), a local area network (LAN), a metropolitan area network (MAN), or a wide area network (WAN).

Regardless of the access medium and the coverage of a network, *network security* can be considered through the achievement of two security goals: *computer system security* and *communication security*:

- The goal of computer system security is to protect information assets against unauthorized or malicious use as well as to protect the information stored in computer systems from unauthorized disclosure, modification, or destruction.
- The goal of communication security is to protect information during its transmission through a communication medium from unauthorized disclosure, modification, or destruction.

1.2 ISO/OSI REFERENCE MODEL FOR NETWORKS

In order to have a deep understanding of the way that networking is performed, network reference models have been developed that group similar functions into abstractions known as *layers*. Each layer's functions can communicate with the same layer's functions of another network host. On the same host, the functions of a particular layer have interfaces to communicate with the layers below and above it. This abstraction simplifies and properly defines the necessary actions for networking.

The ISO *Open Systems Interconnection* (OSI) reference model [5] defines seven network layers as well as their interfaces. Each layer depends on the services provided by its intermediate lower layer all the way down to the physical network interface card and the wiring. Then, it provides its services to its immediate upper layer, all the way up to the running application. It needs to be noted that not all protocol stacks include all seven layers. The most popular protocol suite, Transmission Control Protocol/Internet Protocol (TCP/IP), has five layers. There are no presentation and no session layers; the functions of these layers are incorporated in the layers above and below.

The seven layers of the OSI reference model are briefly described bellow, from the highest to the lowest one:

- ***Layer 7: Application Layer.*** This layer deals with the communication issues of an application. It identifies and establishes the availability of the communicating principals and is also responsible to interface with the user. Examples of application layer protocols include the Session Initiation Protocol (SIP), the HyperText Transfer Protocol (HTTP), the File Transfer Protocol (FTP), the Simple Mail Transfer Protocol (SMTP), and Telnet, to name just a few.
- ***Layer 6: Presentation Layer.*** This layer is responsible for presenting the data to the upper application layer. Essentially, it translates the data and it performs tasks like data compression and decompression and data encryption and decryption. Some of the well-known standards and protocols of this layer include ASCII, ZIP, JPEG, TIFF, RTP, and the MIDI format.
- ***Layer 5: Session Layer.*** This layer is responsible for initiating the contact between two computers and setting up the communication lines. It formats the data for transfer and it maintains the end-to-end connection. Two examples of session layer protocols are the remote procedure call (RPC) and the secure sockets layer (SSL) protocols.
- ***Layer 4: Transport Layer.*** This layer defines how to address the physical locations of the network, establish connections between hosts, and handle network messag-

ing. It also maintains the end-to-end integrity of the session and provides mechanisms to support session establishment for the upper layers. The TCP and the User Datagram Protocol (UDP) are the most widely known protocols of this layer, with the Stream Control Transmission Protocol (SCTP) gaining in usage.

- ***Layer 3: Network Layer.*** This layer is responsible for routing and relaying the data between the network hosts. Its primary function is to send fragments of data called *packets* from a source to a destination host. It also includes the management of error detection, message routing, and traffic control. The IP belongs at this layer.
- ***Layer 2: Data Link Layer.*** This layer defines the conditions that must be followed by a host in order to access the network. It establishes the link between the hosts over a physical channel. It ensures message delivery to the proper device and translates the transmitted bits for the lowest physical layer. Ethernet and Token Ring are typical examples of protocols that operate at this layer.
- ***Layer 1: Physical Layer.*** This layer defines the physical connection between a host and a network. It mainly converts the bits into physical signaling suitable for transmission, such as voltages or light impulse. The device drivers that handle the communications hardware (network cards, wireless cards etc) operate at this layer.

The X.200 [6] recommendation of the ITU-T is aligned with the ISO/IEC 7498-1 standard.

1.2.1 Security in ISO/OSI Reference Model

According to the ISO/IEC 7498-1 [5] standard, each protocol layer is composed of three functional planes: users (also called bearers), signaling and control, and management. In order to secure network communications the security objectives should be accomplished in each appropriate protocol layer and in each suitable functional plane. The ISO/IEC 7498-2 [2] standard and the ITU-T X.800 Security Architecture for Open Systems Interconnection recommendation [3] extend the ISO/OSI 7498-1 reference model (also described in the ITU-T recommendation X.200) to cover security aspects which are general architectural elements of communications protocols. The X.800 recommendation provides a general description of security services and related mechanisms, which may be provided by the reference model. It also defines the positions within the reference model where the services and mechanisms may be provided.

Based on [2, 3], the security objectives are accomplished through *security policies* and *security services*. A security policy is the set of criteria that define the provision of security services, where a security service is a service which is provided by a layer of communicating open systems, in order to ensure adequate security of the systems or of data transfers. The security services are implemented by *security mechanisms* which are in general mechanisms that can be used to technically enforce and implement a security service.

1.2.2 Security Services and Security Mechanisms

As described in [2, 3], the basic security services in OSI communications include the following:

1. ***Authentication.*** This service may be used to prove that the claimed identity of a communicating principal is valid (*peer entity authentication*) or that the claimed source of a data unit is valid (*data origin authentication*).
2. ***Access Control.*** This service can be used to protect the information assets and resources available via OSI from unauthorized access. This service may be applied to various types of access, such as read, write, or execute or combinations of the above. Access to resources may be controlled through various types of access policies, such as rule-based or identity-based security policies. The access control services should cooperate with the authentication services, since granting access rights to a principal requires prior authentication of the principal requesting a particular access.
3. ***Data Confidentiality.*** This service protects the data from disclosure to unauthorized principals. According to the X.800 recommendation, variants of this service include *connection confidentiality* (when it involves all the layers of the communication), *connectionless confidentiality* (when it provides confidentiality in a connectionless service data unit), *selective field confidentiality* (when it protects selective fields of the data), and *traffic flow confidentiality* (when it protects information that could be potentially derived from observation of traffic flows).
4. ***Data Integrity.*** This service ensures that during their transmission the data are not altered by unauthorized principals. This service may have several forms. *Connection integrity with recovery* provides integrity of the data and also detects modification, insertion, deletion, and replay of data. In contrast, *connection integrity with recovery* does not attempt recovery. *Selective field connection integrity* provides integrity for selective data fields within a connection. Connectionless versions of the above services also exist for connectionless data units.
5. ***Nonrepudiation.*** This service ensures that a principal cannot deny the transmission or the receipt of a message. This service may take one or both of two forms. With *nonrepudiation with proof of origin* the recipient of data is provided with proof of the origin of data, so that the sender cannot later deny that he or she sent the particular data. With *nonrepudiation with proof of delivery* the sender of data is provided with proof of the delivery of data, so that the receiver cannot later deny having received the particular data.

Table 1.1 describes the relationship of security services and layers, as described [3]. It should be noted that in the application layer 7 it is possible that the application process itself provides security services.

The implementation of the security services is provided through security mechanisms. These can also be divided into several categories:

1. ***Encipherment Mechanisms.*** These mechanisms provide data confidentiality services by transforming the data to forms not readable by unauthorized principals. The encipherment mechanisms can also complement a number of other security mechanisms. The encipherment algorithms are generally divided into *symmetric* (or secret key), where the same secret key is used for both encipherment and decipherment, and *asymmetric* (or public key), where two mathematically bounded keys are used, the *public key* for encipherment and the *private, or secret, key* for decipherment. Knowledge of the public key does not imply knowledge of the secret key. Issues related with the management of the keys are raised both in symmetric and asymmetric encipherment mechanisms. Examples of symmetric encipherment

Table 1.1 Relationship of Security Services and Layers 1–7

Service	1	2	3	4	5	6	7
Peer entity authentication			X	X			X
Data origin authentication			X	X			X
Access control service			X	X			X
Connection confidentiality	X	X	X	X		X	X
Connectionless confidentiality		X	X	X		X	X
Selective field confidentiality						X	X
Traffic flow confidentiality	X		X				X
Connection integrity with recovery				X			X
Connection integrity without recovery			X	X			X
Selective field connection integrity							X
Connectionless integrity			X	X			X
Selective field connectionless integrity							X
Nonrepudiation of origin							X
Nonrepudiation of delivery							X

algorithms are AES, Twofish, and RC5, where examples of asymmetric encipherment algorithms are RSA and ElGamal. These are described in more detail in Appendix A. Network security protocols such as SSL/transport-level security (TLS) and IP Security (IPSec) discussed in Chapter 5 as well as security mechanisms such as virtual private networks (VPNs) discussed in Chapter 4 also use encipherment mechanisms to protect the confidentiality of the communication.

2. ***Digital Signatures.*** Digital signatures are the electronic equivalent of ordinary signatures in electronic data. Such mechanisms are constructed by properly applying asymmetric encipherment. The decipherment of a data unit with the private key of an entity corresponds to the signature procedure of the data unit. The result is the digital signature of the particular data unit produced by the holder of the private key. The encipherment of the generated digital signature with the corresponding public key of the particular entity corresponds to the verification procedure. Digital signatures can be used to provide peer entity authentication and data origin authentication, data integrity, and nonrepudiation services. RSA, ElGamal, and DSA are examples of signature algorithms (see Appendix A for more details).
3. ***Access Control Mechanisms.*** The access control mechanisms are used to provide access control services. These mechanisms may use the authenticated identity of an entity or other information related with an entity (e.g., membership, permissions, or capabilities of the entity) in order to determine and enforce the access rights of the entity. The access control mechanisms may also report unauthorized access attempts as part of a security audit trail. Examples of access control mechanisms are firewalls (see Chapter 3) and operating system user access privileges.
4. ***Data Integrity Mechanisms.*** These mechanisms provide data integrity services by appending some kind of checksums to the data which may prove alteration of the data. Data integrity may involve a single data unit or field or a stream of data units or fields. In general, provision of the second without the first is not practical. The message authentication codes (MACs) and the digital signatures described in Appendix A can be used as data integrity mechanisms.

Rosa Mavropodi is a Ph.D. candidate at the University of Piraeus, Greece. She received a Bachelor of Science in Computer Science from the University of Piraeus in 1999. Her main research interest is software engineering for telecommunication networks, distributed systems and architectures, intelligent networks, and performance evaluation of high-speed networks.

John C. McEachen, Ph.D., is an associate professor in the Department of Electrical and Computer Engineering of the Naval Postgraduate School, Monterey, California. He is also a co-director for the NPS Advanced Networking Laboratory. He received a Ph.D. and Master of Philosophy from Yale University, New Haven, Connecticut, a Master of Electrical Engineering and Electronics from the University of Virginia, Charlottesville, and a Bachelor of Science in Electrical Engineering from the University of Notre Dame, South Bend, Indiana. His research interests include managing routing in computer networks, wireless networking protocols, patternless intrusion detection, and steganographic communications. Currently, He has served as the NPS Research Desk representative to the Commander, Third Fleet and the U.S. Navy Sea-Based Battle Laboratory (SBBL). In 2003, he was awarded the Richard W. Hamming Award for excellence in interdisciplinary teaching and research. He is a member of the IEEE, Tau Beta Pi, and Eta Kappa Nu.

Manish Mehta is a Ph.D. candidate in Computer Science at University of Missouri, Kansas City (UMKC), Kansas. He earned a Master of Science in Computer Science from UMKC in 2002 and Bachelor of Engineering in Computer Engineering from Mumbai University, India in 1999. He has published several research papers in refereed journals and conferences during his graduate studies.

Lazaros Merakos is a professor in the Department of Informatics and Telecommunications at the University of Athens, Greece and director of the Communication Networks Laboratory and the Networks Operations and Management Center, also at the University of Athens. His research interests are in wireless/mobile communication systems, services, and security on which he has authored more than 170 papers. He is chairman of the board of the Greek Universities Network, the Greek Schools Network, and member of the board of the Greek Research Network. In 1994, he received the Guanella Award for the Best Paper presented at the International Zurich Seminar on Mobile Communications.

Andreas Mitrakas, Ph.D., is legal adviser at the European Network and Information Security Agency (ENISA). He has previously been senior counsel at Ubizen (a Cybertrust company) and general counsel at GlobalSign, (Vodafone Group). He is co-editor of the book *Secure eGovernment Web Service*, IGP, 2007. He holds a Ph.D. in electronic commerce and law from Erasmus University of Rotterdam, the Netherlands, a Master degree in Computers and Law from Queen's University of Belfast, United Kingdom, a degree in law from University of Athens, Greece and a certificate in Finance and Strategy from ParisTech, France.

Aikaterini Mitrokotsa is a Ph.D. candidate at the Department of Informatics of the University of Piraeus, Greece. She received the Bachelor of Science in Informatics from the University of Piraeus in 2001. Her research interests are network security, denial of service attacks and performance evaluation of computer networks, intrusion detection, neurocomputing and machine learning in network security. She has also been active both in European and national research projects in the 6th Framework Programme.

Magda Mourad, Ph.D., is an executive IT architect in the IBM Software Strategy Group. Since joining IBM in 1989, she held several management as well as technical leadership positions. She was CTO of the IBM Digital Media Unit until March 2006. Prior to that she was a research staff member and manager at the IBM T.J. Watson Research Center in Yorktown Heights, New York, where she established and led advanced research projects in various areas, including utilities and hosting services, digital rights management for secure content distribution, multimedia collaboration tools and applications, virtual organizations, and eLearning and training systems based on the internet as well as digital broadcast networks. She also led the deployment of a number of technology pilots around the world.

David Naccache is a computer science professor at the University of Paris II Panthéon-Assas and a member of the Computer Science Laboratory of the Ecole Normale Superieure, Paris, France. His research interests are public-key cryptography and mobile code security.

George P. Ninios is a Ph.D. candidate at the Department of Informatics of the University of Piraeus, Greece. He received a Bachelor degree from the Department of Electronic and Computer Engineering of the University of Crete, Greece. He also holds a Master of Business Administration. His work focuses on secure B2B and G2G transactions where his principal field of interest is designing and building secure transactional systems.

Anthony G. Petropoulos is a Ph.D. candidate at the University of Piraeus, Greece. He received a Bachelor of Science in Informatics from the Department of Informatics of the University of Piraeus. Since 2002, he has also been working at the Software and Applications Labs at OTE R&D in Greece.

Despina Polemi. Ph.D., is a lecturer in the University of Piraeus R&D Department, in Greece where her current research interest is security. She also serves as an evaluator, reviewer, and expert in the European Commission and consultant for the FP5, FP6 and FP7. She obtained a Bachelor of Science in Applied Mathematics from Portland State University, Portland, Oregon in 1984 and a Ph.D. in Applied Mathematics (Coding Theory) from City University of New York (Graduate Center) in 1991. Dr. Polemi held teaching positions (1984–1995) at Queens College, Baruch College of City University of New York and the State University of New York at Farmingdale in the Department of Mathematics. From 2000 to 2003, she was president of the BoD in Expertnet (www.expertnet.net.gr)

and technical manager of the company from 2000–2004. She participated in the EC security projects of the programs COST, ACTS, and NATO security projects. She is a member of IEEE.

Vassilis Prevelakis, Ph.D., is assistant professor of Computer Science at Drexel University, Philadelphia, Pennsylvania. He received a Ph.D. from the University of Geneva in Switzerland and Bachelor and Master degrees from the University of Kent at Canterbury, United Kingdom. His interests include home network security, robust and self-healing systems, and security for control and data acquisition networks.

David J. Robinson is co-founder and partner of Global Security Consultants in Odenton, Maryland, where he lives with his wife and two children.

Srinivas Sampalli is a professor and 3M Teaching Fellow in the Faculty of Computer Science, Dalhousie University, Halifax, Nova Scotia, Canada. His research interests are security and quality of service in wireless and wireline networks. Specifically, he has been involved in research projects on protocol vulnerabilities, security best practices, risk mitigation and analysis, and the design of secure networks. He was the Dalhousie University principal investigator for the Secure Active VPN Environment (SAVE) project sponsored by the Canadian Institute for Telecommunications Research (CITR) and is currently the principal investigator for the wireless security project sponsored by Industry Canada. Dr. Sampalli has received many teaching awards, including the 3M Teaching Fellowship, Canada's most prestigious teaching acknowledgement.

Ian Schneller is co-founder and partner of Global Security Consultants, Odenton, Maryland. He has provided computer and information security services to the U.S. government and commercial companies since 1991. Mr. Schneller resides in Maryland with his wife and twin boys.

Kapil Kumar Singh is a Ph.D. candidate at the College of Computing, Georgia Institute of Technology, Atlanta, Georgia. He received a Master of Science in Computer Science from University of British Columbia, Canada in 2005, and a Bachelor of Technology in Computer Science from Indian Institute of Technology (IIT), Roorkee, India in 2001. He also worked as a senior software engineer on a number of telecom/satellite networking projects at Hughes Software Systems, India from 2001 to 2003. His research focuses on many aspects of computer and network security, including VoIP security, intrusion detection systems and botnets.

Sachin Singh works for Heartlab, an AGFA Company, in Westerly, Rhode Island, where he creates software solutions to manage and analyze critical clinical information for cardiovascular medicine. He earned a Master degree in Computer Science at the University of Missouri, Kansas City (UMKC) and did research at the UMKC Distributed Intelligent Computing Lab (UDIC) in data mining, semantic web, pervasive computing

and e-services, mainly focusing on application to medical informatics. Prominent amongst his work were the Sem-ether project, based on global pervasive computing, selected for AAAI 2004, and the I-CareNet project, which provided intelligent emergency response system to healthcare workers on mobile devices. Mr. Singh also worked at the Children's Mercy Hospitals, Kansas City, Missouri. His work at Heartlab addressed the Dynamic Z-Score tool and continues in the fields of e-services, semantic web, and pervasive computing.

Kyriakos Stefanidis is a computer engineer conducting Ph.D. research at the Department of Electrical and Computer Engineering of the University of Patras, Greece. His research interests include network security, distributed denial-of-service attacks and grids. He has participated in several projects on network and systems security funded either by the Greek government or by the European Commission.

Stéphane Socié is a security specialist in the Security Labs at Gemalto, France, where he is focusing on mobile code security. He holds a Master degree in Computer Security from the University of Toulon, France.

Panagiotis Sklavos, Ph.D., is a telecommunications security engineer at EXPERTNET S.A. His current research interests are system and network security, PKI, IP security and dynamic virtual private networks, secure network management and performance evaluation of IPv6 and IP over ATM. He received a master degree in Electrical and Computer Engineering from the National Technical University of Athens (NTUA), Greece, in July 1998 and a Ph.D. in Information and Network Security from the same university in 2005. He has 11 publications and has participated in eight European research projects.

Ahmed Tantawy, Ph.D., is the technical director of IBM in the Middle East and North Africa. His previous positions at IBM include director of Advanced Development in the Software Group, worldwide director of Video Technology Solutions, and manager of Multimedia Communications in the T.J. Watson Research Center in Yorktown Heights, New York. Prior to joining IBM in 1988, he was a Computer Engineering professor and consultant in the United States, France, and Saudi Arabia. His technical achievements include 29 patents, four books, and more than 100 refereed papers.

Artemios G. Voyiatzis is a Ph.D. candidate with the Department of Electrical and Computer Engineering, University of Patras, Greece. He holds a Bachelor of Science in Mathematics, a Bachelor of Science in Computer Science, and a Master of Science in Computer Science, all from the University of Crete, Greece. His interests are in the areas of secure network architectures, network security, secure embedded systems, and cryptography.

Son Vuong, Ph.D., is a professor of Computer Science at the University of British Columbia in Vancouver, Canada since 1983, where he founded the Distributed System