Editorial

With the proliferation of open systems and networks in general, and the Internet and the World Wide Web (WWW) in particular, network security has become a major concern. Earlier this year, we experienced distributed denial of service (DDoS) attacks launched against commercial Internet sites, such as Yahoo, Amazon, eTrade, eBay, CNN, and ZDNet, and a couple of weeks later, we learnt about the destructive power of malicious code demonstrated by the ILOVEYOU virus. Both incidents have again shown that the networking infrastructures we use for our daily businesses are inherently vulnerable, insecure, and fragile. The reason for the resulting security problems we face today is that most of these networking infrastructures have not been designed with security in mind. Consequently, we have to secure the infrastructures in the aftermath of security-related incidents. Unfortunately, retrofitting security into existing systems and networks is always expensive, whereas the design of secure systems and networks would not be expensive at first place if security issues were considered during the design of the systems and networks.

The aim of network security is to design, implement, and deploy effective and efficient patches for vulnerabilities or countermeasures to protect against relevant threats and attacks. In the recent past, many networking conferences and trade-shows have taken place that centered around the notion of "scalability" and "security". The most challenging questions, however, arise at the intersection point of these two terms: How can we develop mechanisms and technologies that are both secure and scalable? How can security technologies be deployed on a large scale without any impact on the resulting protection levels? How can legacy systems be made more secure, and how can we teach users to actually make use of the security mechanisms that are available? Today, computer and network practitioners are equally interested in answers to these (and related) questions. This is particularly true for new applications related to electronic commerce (e-commerce) and electronic business (e-business). The advent of business-to-business applications over Internet has brought up requirements for sophisticated security services like non-repudiation and access control beyond basic network availability and integrity.

Against this background, the field of network security has become very broad and includes many topics of interest ranging from applied cryptography through computer security to firewalls. The aim of this special issue of Les Annales des Télécommunications is to overview and discuss some exemplary topics and to point its readers to open and challenging questions for further research. The first part of the issue is an overview of existing security solutions for Internet and mobile networks. The second part tackles with the impact of the mobile code paradigm on computer and communications security and the last article presents a broad vision of new security requirements brought by future communication technologies.

In the first article entitled "Analyse des fonctions des protocols IPSec et leur intégration dans un réseau privé virtuel", Mohammed Achemlal from France Télécom and Maryline Laurent from IRISA-INRIA overview the IPSec protocol suite and elaborate on its usefulness to build virtual private networks (VPNs) and to secure corporate intranet and extranet environments. IPSec is considered to be one of the key security technologies of the future. In its current form, however, the IPSec protocol suite does not address all problem areas, and one area for which IPSec does not provide a solution is IP multicast (i.e., IP packets sent from one source to multiple destinations). This is particularly true for the Internet Key Exchange (IKE), the key management part of the IPSec protocol suite. IKE established security associations (SAs) between two entities, and as such it is not very useful for UDP-based multicast traffic. As of this writing, the security problems related to IP multicast are studied in the Internet Research Task Force (IRTF) Secure Multicast Group (SMuG). In the second article entitled "IP Multicast Security: Issues and Directions", Thomas Hardjono from Nortel Networks (the co-chair of the IRTF SMuG) and Gene Tsudik from the University of

California at Irvine identify and discuss various concept and issues related to IP multicast security, and give some perspective for future research directions.

Similar to many other security protocols, the IPSec protocol suite also requires public key certificates and a corresponding public key infrastructure (PKI). In the third article entitled "Managing Certificates in a Corporate Environment", Rolf Oppliger from eSECURITY Technologies (Switzerland) overviews and briefly discusses the issues that suround the management of both public key and attribute certificates in a corporate environment.

With the increased use of mobile networks (e.g., GSM networks in Europe), security issues (related to mobile networks) must also be addressed. In the fourth article entitled "Security services for protecting radio mobile systems", Thierry Baritaud, Henri Gilbert, and Sébastien Ngyen Ngoc from CNET (France Télécom) present examples of currently existing security solutions against frauds and attacks, and gives an overview of potential solutions for protecting future radio mobile networks.

In the fifth article entitled "A Revised Taxonomy for Intrusion-Detection Systems", Hervé Debar, Marc Dacier, and Andreas Wespi from IBM Research revise a taxonomy for intrusion detection systems (IDSs) they have introduced in a previous paper. Security scanning and intrusion detection are assumed to replace formal risk analysis in future approaches for risk management.

In the sixth paper entitled "Techniques for Secure Execution of Mobile Code: a Review", J.-M. Mas-Ribés and B. Macq from the Université catholique de Louvain (Belgium) address the problem of how to protect a runtime environment against potentially hostile or malicious mobile code. As such, the authors present a survey of different techniques aimed at resolving the problem of secure resource management, and argue within which context they are appropriate. Similarly, in the seventh paper entitled "Mobile Agents and Telcos' Nightmares", Joachim Posegga from Deutsche Telekom AG and Günther Karjoth from IBM Research analyze the state-of-the-art of mobile agents technology with regard to security. Contrary to the previous article, however, this article discusses security from the point of view of a public network operator. Reading these two articles, however, you must keep in mind that there is another major security obstacle to overcome with regard to the deployment of mobile agents technology: Protecting mobile agents against potentially malicious runtime environments. There are hardly any research proposals to address this problem.

Finally, in the eighth paper entitled "Creating a new security for tomorrow's communication networks and information systems", Michel Riguidel from Thomson-CSF Communications overviews the situation of information security and discusses requirements for future security technologies and solutions.

We hope that this special issue of Les Annales des Télécommunications serves as starting point to initiate further research in the field of network security. There are many open questions and research areas to be addressed before fully networked and distributed systems can be operated without putting their resources at risk. It will be interesting to view a similar issue in a couple of years, and to see whether the effort that is currently put on network security research will be fruitful.

Refik Molva, Institut Eurécom (France)
Rolf Oppliger, eSECURITY Technologies (Switzerland)