

Overview of Research Interests

Rolf Oppliger, Ph.D.

I am interested in all topics and fields of research related to information security. This includes the fundamentals of information security, computer security, communication and network security, as well as specific applications related to information security.

Fundamentals

From a practical viewpoint, information security is about risk management, and there is a large body of research on risk management that is potentially relevant and applicable to information security. I have done some preliminary research in this area. In a future line of research, however, I intend to more thoroughly investigate on the applicability of risk management technologies and techniques to information security. This includes, among other things, economical aspects and considerations.

From a more theoretical and technical viewpoint, the fundamentals of information security are very much related to mathematics in general, and cryptography in particular. Since the early 1990s, I have been working in this area (most recently on digital signatures and digital signature legislation). In 2005, I published a book entitled *Contemporary Cryptography* in Artech House's book series on computer security. As its title suggests, the book provides a mathematical introduction and overview of all aspects related to contemporary cryptography.

Computer Security

Informally speaking, computer security is about securing data that is stored, processed, and/or transmitted in computer systems. The major fields of research are related to authentication, authorization, and access control. This includes, for example, the notions of public key infrastructures (PKIs), authentication and authorization infrastructures (AAIs), and—maybe most importantly—identity management. All of these topics have been at the center of my research activities during the last decade. In fact, I published a book entitled *Authentication Systems for Secure Networks* in 1996. The book is narrowly focused on Kerberos and a few other authentication and key distribution systems. Due to its use on Microsoft Windows platforms, Kerberos and the integration thereof in networked and distributed systems is still an important and very timely topic today.

From a practical viewpoint, computer security also comprises malware protection and intrusion detection and prevention (IDP). Furthermore, there is an industrial interest in security evaluation and certifications programs (according

to, for example, the Common Criteria). Last but not least, trusted computing and digital rights management (DRM) have recently become hotly debated and fairly controversial topics and fields of study. I am interested in all of these topics and intend to continue my basic research activities in these areas.

Communication and Network Security

Informally speaking, communication and network security is about controlling access and securely communicating data in computer networks and distributed systems. Most importantly, this includes network firewalls (for access control) and cryptographic security protocols (for secure communications).

I have been working on communication and network security for a considerably large part of my professional life. This is particularly true for TCP/IP-based networks. The corresponding results are, for example, summarized in two books published in Artech House's book series on computer security, i.e., *Internet and Intranet Security* (1998 and 2002) and *Security Technologies for the World Wide Web* (2000 and 2003). Both books are in the second edition and are frequently used in the field. Secure messaging is another topic I am working at. On the one hand, I published a book entitled *Secure Messaging with PGP and S/MIME* in 2001; on the other hand, I have coined a patent-pending technology that can be used to provide certified mail services on the Internet in a highly scalable way. In the future, it is reasonable to expect that wireless networks and voice over IP (VoIP) applications will become ubiquitous. Consequently, the security implications of these technologies are going to be at the center of my short-term research activities in communication and network security.

Specific Applications

There are many specific applications that are related to information security, or that employ technologies and techniques normally used to secure computer systems and/or networks. Examples include remote Internet voting, electronic payment systems, electronic ticketing systems, and Internet banking. The last application is particularly interesting, because it has been challenged recently with the proliferation of phishing and Web spoofing, visual spoofing, and man-in-the-middle (MITM) attacks. In the very recent past, I have been involved in the development of a patent-pending technology that can be used to protect SSL/TLS-based e-commerce applications, such as Internet banking, against MITM attacks. This work is ongoing.

More recently, I have also started to investigate on the privacy requirements of Internet-based e-commerce applications, and the development of corresponding privacy-enhancing technologies (PETs). The use of PETs (and the ability to provide privacy services, accordingly) is likely to become a differentiating factor in the marketing of otherwise very similar and comparable products and services.