FOREWORD

I have been teaching computer engineering in courses like Software Engineering and Operating Systems for more than 20 years. In all my teaching I have stressed making students understand the principles of the focal area of a course and not just having them memorize one technique or another. The increasing complexity of networks and our whole information society challenges this understanding even more. Different parts of the information structure can communicate with each other and understand each other via communication protocols. This opens up new threats in communication networks. Vulnerability in any of the communication protocols may make the whole system weak. It is of utmost importance that our developers and experts today and tomorrow have a good understanding of security aspects and can apply them.

Tomorrow, all communications will happen over IP. In the past, telecom operators handled most communications, and the main business for them was voice communication. In reality, almost all last-mile communications today still happen over the conventional telecom infrastructure. The backbone of the Internet has been going through a fast transition to faster and faster fiber optics and digital data transfer. The era of analog communications has been over for some time already. But, there are other changes in the communications landscape. I will describe some of them based on experiences we have had as one of the most advanced high-tech countries. This is so because here in Oulu, Finland, we have been surrounded by high-tech inventions, and several enterprises use the city as a test bed for their inventions and their business models.

In the past, the first GSM network was launched in Oulu. GSM technology took over the communications landscape quickly, and today in Finland we have people in their thirties who have never in their life owned a fixed-line telephone. Today there are more cellular phones in Finland than there are people. Less than 50% of households have a fixed-line phone, and the number of fixed-line connections is still dropping faster every year.

At the same time, the transition from fixed-line voice communications to fixed-line data communications has happened very rapidly globally. Most households now subscribe to broadband service, and they use services such as e-mail and the web in their everyday life. Necessary cabling to the households existed due to the transition from fixed-line to mobile, and the cabling was reused by the broadband providers.

Today the transition is from providing services to providing bandwidth. Recently, the next step in breaking traditional business models was taken in Oulu. One of the first free WiFi networks was also launched here. With the introduction of WiFi-enabled cellular phones, consumers in Finland are testing various free VoIP services, and that might be the end of all voice-based business models. The transition from voice to data, and from fixed to mobile, results in personal, always connected wireless communication devices.

Today, people speak of Voice over IP, but a better name for the Next Generation Networks is Everything over IP (EoIP). And all of that communication will be wireless. But what does that have to do with the topic of this book? It means the world has to finally wake up to the security of the communications networks.

To build security, you have to understand the application you use. For many, Internet security equals web security. This false impression is created by security companies, the media, and the software industry. For many, an application is the same thing as a web application. Application security equals web application security. But today, the web is not the biggest threat to your business. True, some businesses are built on web services, but other applications such as e-mail and voice can be much more critical for enterprises and for consumers. Web security can have a high profile, as a compromised server is seen by hundreds of thousands of people. A compromised voice connection or e-mail client might escape public attention but could result in the loss of the most critical assets of a company, or cause irreversible damage to an individual.

To be secure, you have to understand that wireless networks are always open. While in traditional telephone networks all the switches were kept behind locked doors and all the cabling was protected, in wireless technology there are no cables and everyone has access to wireless access points. One compromised infrastructure component, and the entire network is compromised. One virus-contaminated access device, and everyone in the network will be contaminated.

To be secure, you have to understand that client security is as important as, or even more important, than server security. Servers can be protected, upgraded, and updated and potential damages can be restored. These are standard processes for all IT administrators. Now, take laptops as an example of a mobile device of the future. Most, if not all, critical data is stored on the laptop. All the keys and passwords are there. Communication behavior is stored there. The laptop also can eavesdrop on all behavior, including listening to the surroundings of the user of the laptop. A mobile device of the future is all that and more.

This book by Peter and Ari is built around voice as the application to be secured, but the principles apply to any communications. Studying this book should be obligatory to all students in computer engineering and computer science, not only due to its content and deep understanding of VoIP security, but also to allow them to learn how to apply the best practices in other fields, no matter what their future field of study will be. The key to learning is not only studying things and memorizing the various topics, but learning how to apply the best practices of other fields in your own. Combining the best practices of traditional telecommunications, e-mail, and the web into new next-generation technologies is essential to be able to build reliable and usable communication technologies. Voice over IP is potentially the killer application, destroying conventional communication networks and creating a new IP-based communication infrastructure. I truly hope it will not be built by business people only, but also by people who understand the security aspects of the new technologies.

Prof. Juha Röning
Principal Investigator of Oulu University Secure Programming Group (OUSPG)
Head of Department of Electrical Engineering
University of Oulu

May 30, 2007