Since the birth of the Internet, guaranteeing proper security requirements has been one of the main challenges. Besides, 30 years of evolution have changed in a very impressive way the meaning, and the approach, to this problem. In the beginning, the Internet had to cope with security issues in a scenario where users, programmers, system and network managers were highly skilled. Nevertheless, engineers had to deal with very simple network topologies and few media for handling data. Also, applications had a quite long lifecycle (i.e., telnet has been around for more than 20 years, which is unthinkable for a modern “app”, yet is still widely used… sigh). Among the others, the most important fact was the embryonic stage of ideas characterizing the “misuse” of network resources. Nowadays it is quite clear that security is not only related to the technical part of the Internet, but it also includes users’ awareness and behaviors. In fact, the world has dramatically changed, and being a security professional, or just an enthusiastic, requires a deep and sound knowledge on the areas that are well depicted in this book. In this perspective, the work is a valuable source of information for people involved in Internet related technologies and services.

The areas covered in this book can be summarized as follows:

- Social networks, which are now places where a lot of individuals exchange/integrate their experiences and create a sort of augmented reality. As it happens in the “real” world, new questions arise. For instance: “How do I trust someone?” “How can I avoid disclosing unwanted personal details?” “How can I prevent data fusion as a way to inherit a deeper knowledge about myself?” “How can I implement a solid access control to my (Web) services?” Answers to these – and more questions – will be easily found in this book, which also covers general and sociological aspects related to Social Networks.

- New “cyber” threats, such as the Cyberbullying, which makes the Web a new arena where aggressiveness takes place, also allowing the bothering and harassing people an easier task (e.g., we do not have to take a car and go somewhere, and keyboards do not require muscle power as needed in a street).

- Collective intelligence and opinion building. A very fragile process that sometimes may have its foundation on inaccurate information or, at its worst, intentionally false data in order to bias the public opinion. However, in the past, it was easier for people to measure trustworthiness, since “sources of information” where very stable (few newspapers, radio channels, and TV broadcasts) and, even if not always reliable in their contents, they had to pass through some sort of editing and approval. On the contrary, in today’s scenario, it is very hard to clearly measure the reliability of sources. Thus, in this book some innovative techniques for identifying which information is trusted/un-trusted are presented.
• Issues related to the sharing of wanted/unwanted information. The book covers risks and benefits of having semantic contents widely spread over peer-to-peer social networks, as opposite of having a few centralized systems. Also, it explains how people can be forced to share unwanted personal data, which can be inferred through data fusion and integration.

• Privacy and targeted attacks. The book also offers a robust coverage of the concerns related to privacy and data leakage to help the reader in gaining a better consciousness. This will be of great help either to final users or professionals involved in planning, development, testing, management and deployment of social networks based services and products.

In conclusion, I have found in this book a very interesting and innovative way to discuss and examine the problem of security for Web data and services, avoiding the classical “stacked” approach (i.e., wired/wireless transport data security, host integrity, application testing and so on). Instead, a multidisciplinary methodology is favored, and it has been centered on present most critical aspects, i.e., the human behavior and perception. This is why I would definitely recommend reading it.

Massimo Ianigro
National Research Council of Italy, Italy

Massimo Ianigro is a Research Technologist and Security Expert of the Institute of Intelligent Systems for Automation – Italian National Research Council. His main interests are in the networking field, with focus on security, Internet services, traffic measurement and management, heterogeneous networks and distributed systems. After receiving a MD in Computer Science with a thesis about mobile robot navigation, he has started working at the CNR in 1992 and he is responsible for the networking infrastructure and telematic services for a large number of users and sites disseminated around the country. He is also a member of the GARR-CERT (Computer Emergency Response Team of the nation-wide network of academic institutions) and he is an expert appointed by Italian law enforcement agencies in many computer forensic cases.