Review of the book

"Handbook of Information and Communication Security"

by Stavroulakis, P., Stamp, M. (Eds.)
Springer, 2010

ISBN: 978-3-642-04116-7

Kilian David Luigi Lo Iacono

1 What the book is about and like

This book is a compilation of *several surveys of some of the most important, interesting, and timely topics, along with a significant number of research-oriented papers* from the field of information and communication security—to cite from the authors' preface.

2 Detailed Summary

The organization of the book structures the surveys and papers topic-wise in seven parts as follows:

- Fundamentals and Cryptography
- Intrusion Detection and Access Control
- Networking
- Optical Networking
- Wireless Networking
- Software
- Forensics and Legal Issues

In the following, each chapter of these parts is reviewed in detail.

Part A: Fundamentals and Cryptography

Chapter 1: A Framework for System Security

Chapter 1 aims to describe a conceptual framework for the design and analysis of secure systems with the goal of defining a common language to express "concepts". Since it is designed both for theoreticians and for practitioners, there are two kinds of applicability. On the one hand a meta-model is proposed to theoreticians, enabling them to express arbitrary axioms of other security models in this special framework. On the other hand the framework provides a language for describing the requirements, designs, and evaluations of secure systems. This information is given to the reader in the introduction and as a consequence he wants to get the specification of the framework. Unfortunately, the framework itself is not described!
However, the contents cover first some surrounding concepts like "systems, owners, security and functionality". These are described sometimes in a confusing way, so that it remains unclear, what the author really wants to focus on.[1] The following comparison of "Qualitative and Quantitative Security" is done

[1] For example: if the reader is told, that "every system has an owner, and every owner is a system", there obviously seems to be no difference between these entities (cp. p. 4).

to describe the limitations of a system analysis. Therein topics like the Gaussian measurement error, methods of actuarial analysis or those "faced by a 16th century naval captain in unchartered waters" are covered. The next sub-topic describes the authors understanding of "Security Requirements and Optimal Design", which is directly followed by "Architectural and Economic Controls; Peerages; Objectivity". Herein the relationships between the actors are described. Surprisingly, there are nearly no citations of corresponding or relevant research papers given so that it is difficult to get the benefit from this chapter, too. In addition to this, "Legal and Normative Controls" are described very shortly without giving a focus on compliance or metrics for measurement.[2] This first block is finalized with "Four Types of Security", "Types of Feedback and Assessment" and "Alternatives to Our [the authors] Classification". Well, just a few words referring to these three chapters. The first one is – in my humble opinion – only a theoretically doctrine since it is questionable to achieve a state of full security. It would be better to do a risk assessment (according to the authors' words: "Four Types of Risk") and based on the results to implement, monitor and report the fulfillment of the discovered gaps. This methodology would also be a better proposal since the author is focusing in the second part on trust and distrust as well as on "human psychology and sociology" (cp. p. 11). Because of expecting technical topics in the main, this is a little bit confusing.

The remainder of the paper is devoted to applications of the authors model. Even though the first part was a little bit out-of-focus, the second one covers four interesting value-adding aspects in regard to applications. Therefore "Trust Boundaries", "Data Security and Access Control", "Miscellaneous Security Requirements" and "Negotiation of Controls" are covered. The wording is easy to understand, all the relevant and essential key-words are precise defined and the author follows his plot. Since all the described methodologies are only static, the author accentuates the need for dynamic systems referring to the Clark-Wilson-System and finalizes the chapter with a link to a recent set of guidelines for the design of a computer system defining a collaboration oriented architecture.

To sum it up, the first chapter – according to the expectations precipitated by the topic of the paper[3] – generates an added value only in the second part. Because of the first part focusing primarily on the surrounding topics, it remains unclear how to set up such a framework since the key facts are not worked out in detail. The second part is completely different since the author gives you a much more structured overview about the static and dynamic approaches for designing a framework for system security on a theoretic (!) basis.

Chapter 2: Public-Key Cryptography

Chapter 2 covers the well-known aspects of "Public-Key Cryptography". After the "Overview" the differences between "Public-Key Cryptography vs. Symmetric-Key Cryptography" are explained focusing on the "Distribution of Public Keys" as well as on the organizational requirements. In addition to this the "Public-Key Encryption" is defined with regard to Indistinguishability, the Security for Multiple Encryptions and Security Against Chosen-Ciphertext Attacks. The conjunction of the Public-Key- and Symmetric-Key-methodologies is described in the chapter about "Hybrid Encryption". This chapter is finalized with the relevant "Examples of Public-Key Encryption Schemes" like RSA and ElGamal whereas the theory of elliptic curves is missing (it will be presented later in chapter 3, p. 35-57). The chapter ends with a word on signature schemes.

Chapter 3: Elliptic Curve Cryptography

This article is great – only some previous knowledge is required: a basic understanding of protocol weaknesses and the resulting possible attacks, an advanced knowledge of number theory (especially about groups and discrete logarithms, finite fields and elliptic curves). Although these underlying principles are explained in detail, the description is the shortest I have ever seen. In addition to this the reader also has to be familiar with the mathematical notation. It nearly covers every single aspect of the elliptic curve

[2] It should be mentioned that the compliance requirements are directly triggered by the legal requirements.

[3] According the Merriam-Webster, a "framework" is "a basic conceptional structure (as of ideas)" or a "skeletal, openwork, or structural frame".

topic but, if you have never heard of these concepts, it is possible that one has to read some chapters again.
This chapter is really state-of-the-art and covers all relevant aspects. It was a pleasure for me to read it (the only thing to complain about are the examples since the author often uses very big integers containing of 20 ore more digits – making it impossible to verify them easily with your pocket calculator).

Chapter 4: Cryptographic Hash Functions

This chapter is subdivided in nine parts, first introducing the understanding of the notations used concerning hash functions. Therefore, a nice overview about the properties of preimage resistance, second preimage resistance, collusion resistance, near-collusion resistance and partial-preimage resistance are given. Based on this, the design principles of the Merkle-Damgard construction are described mentioning the widely used standard hash functions such as MD5 and SHA-1. An overview of the generic attacks and short-cut attacks on the iterated hash functions is provided and important hash function applications (like digital signatures and the hashing of passwords) are described. Finally, the concepts of hash based MACs[4] are presented with regard to generic attacks on MAC algorithms. The chapter is completed with an overview about the aims of the NIST SHA-3 competition and its current progress.
The first thing that is mentionable is the very extensive amount of references. Although the paper only consists of twenty pages, there are 130 references (six pages/one third). So, if the reader has any additional need to read further material, nearly every single relevant source is given to get a really deep understanding. Since lots of aspects are covered, this chapter gives a short and comprehensive overview about the subject of cryptographic hash functions and therefore is suitable for undergraduates as well as practitioners.

Chapter 5: Block Cipher Cryptanalysis

This chapter consists only of nine pages, where two fundamental classes of techniques are described that are often used to break block ciphers. Therefore some basic concepts are introduced (like Martin Hellmann's time-space trade-off or the faster approach of constructing rainbow tables) followed by the general technique of using the principals of differential cryptanalysis.
Unfortunately, the presented concept of attacking the single DES gives no new information. First of all, the concept is considered as broken/unsecure and second, the author itself complains about the technique, when DES uses the full 16 rounds, since this technique "requires more work than brute force". If the reader is familiar with the topic he could also complain about the missing theoretical attack from Biham and Shamir (1992) with less complexity than brute force requiring "only" 2^{47} chosen plaintexts as well as the further development in form of 3DES in 1998.

Chapter 6: Chaos-Based Information Security

This chapter is very comprehensive covering nearly 40 pages of a new scientific research topic – chaos-based information security (subtitled with: "Chaos-Based Block and Stream Ciphers in Information Security").
After a short introduction the basic paradigms to design chaos-based cryptosystems are described. These paradigms are called analog chaos-based cryptosystems and digital chaos-based cryptosystems and allow to design chaotic cryptosystems on the basis of discrete-time or continuous-time dynamic chaotic systems. These analog chaos-based cryptosystems are briefly presented. In this context four different chaos schemes are distinguished (i. e., additive chaos masking scheme, chaotic switching scheme, parameter modulation scheme, and hybrid message-embedding scheme), where the most interesting one is the hybrid message-embedding scheme which is coupled with the inverse system approach.
Followed by this, the ideas of discrete analog chaos-based cryptosystems and chaos theory are described. They contain the basic information concerning chaotic maps, their features, and their usage in the design process of stream and block ciphers, which then are analyzed with various examples of algorithms. Some of them are vulnerable to cryptanalytic attacks and the security level of the other is high according to an inventor's evaluation.

[4] MAC: Message Authentication Code

The chaotic stream ciphers and block ciphers mentioned above are designed on the basis of discrete-time and continuous-value chaotic systems and all computations are done in finite-precision floating-point arithmetic. It is presented that the finite-precision computations generate another problem – a degradation of the properties of chaotic maps. This degradation is than used for the design of block ciphers or their components. The last section is a conclusion to the chapter and presents some suggestions for reading on additional usage of chaotic maps.

Chapter 7: Bio-Cryptography

Chapter 7 covers the different aspects of bio-cryptography and is divided in three subsections. Unfortunately, the first one is redundant since it gives an introduction to cryptography which should be supposed to be preexisting.[5] The second chapter describes the properties of biometric concepts like fingerprint matching and different challenges of biometric systems. Finally, biometric methods are described in detail in the third one making this last subsection the most valuable (also suitable for scientific research). In this context, the "Fingerprint Fuzzy Vault" is introduced followed by special designated algorithms and implementations. This chapter gives a good overview about the approaches done in the biometric division of cryptography. The only thing to complain about is the first subsection, because it is a little bit out of scope.

Chapter 8: Quantum Cryptography

Chapter 8 explains the concepts of "Quantum Cryptography" (which should better be named as "Quantum Key Distribution" (QKD) since the quantum cryptography is not a cryptographic technology). The physical details are described in an easy to understand comprehensive way including the basics. In addition to this some limitations, network concepts and applications of QKD are described. This chapter ends up with only four references with avoids the reader to get a deeper understanding or to do more research.

Part B: Intrusion Detection and Access Control

Chapter 9: Intrusion Detection and Prevention Systems

This chapter provides an overview of intrusion detection and prevention systems (IDPS) technologies. It explains the key functions that IDPS technologies perform and the detection methodologies that they use. In addition to this it highlights the most important characteristics of each of the major classes of IDPS technologies as well as interoperability and complementary technologies.

The content is divided in three subsections which cover the Fundamental Concepts, different Types of IDPS Technologies (like Network-Based, Wireless, Host-Based IDPS and NBAD[6] Systems) and the use and integration of multiple IDPS technologies.

The main concepts are explained in an easy way making this introduction especially useful for practitioners and undergraduates. For scientific research it is not suitable since neither technical details nor mathematical concepts are explained.

Chapter 10: Intrusion Detection Systems

Chapter 10 extends the topic already described in chapter 9 with the much more interesting implementation approaches, the different methodologies for system testing and the concepts of metric-based system evaluation. Within this "lifecycle" the different advantages and disadvantages are described highlighting the impact on the monitored system. Finally a detailed example is given within a case study making this chapter also useful for practitioners.

[5] For example, the properties of symmetric-key cryptography, the Data Encryption Standard (DES), the Advanced Encryption Standard (AES), the concepts of Public-Key Encryption or the RSA Algorithm are described.

[6] NBAD: Network Behavior Analysis Detection

Chapter 11: Intranet Security via Firewalls

This chapter addresses the problems that arise because of the complexity involved in managing firewall policies in a multiple-firewall enterprise network environment. Although this content doesn't cover the technical aspects of firewalls, a basic understanding of their functionality is needed. Focusing strictly on policies, the added value is generated through the interesting aspect of identifying policies and their relations as well as anomalies and special message exchange sequences in a firewall system. The given references are helpful since this topic is quite often out-of-scope.

Chapter 12: Distributed Port Scan Detection

Covering only ten pages, this chapter first gives a short and straight overview of "classical" port scans followed by the motivation and approach to do (and detect) them in a distributed way. Therefore the reader should be familiar with the basic ideas and aims of the technical implementation. Because of this, the added value is especially generated for practitioners like security experts or penetration testers as well as scientific research aspects.
If the reader has this previous knowledge (or the time to understand/learn the required details), there will be an excellent demanding article which is – in my humble opinion – one of the top five of this handbook. The explanations are clear and complete only covering the new aspects, the figures are necessary adding lots of details and the references are up-to-date and helpful.

Chapter 13: Host-Based Anomaly Intrusion Detection

This chapter provides fundamentals of host-based anomaly IDS as well as their developments. Therefore a new architectural framework is proposed to integrate multiple detection engines. The novelty presented is a feedback loop that enables one output from a detection engine to be used as an input for another detection engine. The sections are subdivided in background information providing basics, basic concepts in HIDS[7] and their developments and some examples to illustrate the implementation procedures. Finally, the hidden Markov models and hereon-based anomaly intrusion detection schemes are explained. In addition to this a theoretic framework for designing new IDS architectures is presented. To sum it up, this chapter is in my opinion suitable for postgraduates in advanced security courses and not – like proposed by the author - suitable for undergraduates since the approaches presented sometimes need an extended scientific or mathematical previous knowledge.

Chapter 14: Security in Relational Databases

This chapter consists of 14 pages covering first some basics to relational databases. Based on this knowledge the following two sections focus on classic as well as modern database security. Unfortunately, the contents are sometimes only useful for a historical overview. For example, the "Orange Book" is no longer (since 2003!) supported by the Department of Defense and was replaced by the "Common Criteria"[8]. This new framework was established as an international standard (ISO/IEC 15408) for computer security. Although some of these facts are mentioned, the relationship to database security is not obvious since only abstract guidelines for IT security are covered. The given information only covers general knowledge about databases and gives no new or interesting facts or research aspects. Finally, this chapter is not worth reading except for readers who never stayed in contact with IT security aspects or databases.

Chapter 15: Anti-bot Strategies Based on Human Interactive Proofs

This chapter gives an comprehensive overview about the existing technologies and methodologies used in anti-bot strategies based on human interactive proofs. It is easy to read and suitable for undergraduates as well as for practitioners. The used figures are helpful and make the different sections enjoyable to read.

[7] HIDS: host-based intrusion detection system

[8] Abbreviation for "Common Criteria for Information Technology Security Evaluation" or just CC.

Chapter 16: Access and Usage Control in Grid Systems

This very specialized chapter focuses on grid systems and their access and usage control. Since it is completely based on the "Globus Toolkit" it is especially suitable for dedicated interest groups. After explaining the basic approaches of grid computing, the security features of the toolkit are explained. Based on this knowledge the author gives a comprehensive overview about the different access control technologies which can be used. The presented content is useful for practitioners working in the area of IT-security and access control. Useful examples (like a policy for computational services) are given and the resources and references are also quite useful.

Chapter 17: ECG-Based Authentication

The chapter extends over twenty pages and is divided into eight subsections. The focus is given on authentications based on electrocardiograms (ECG), which represent the electrical activities of the heart. To understand this biometric approach, first the background knowledge of ECG is introduced followed by a detailed classification and comparison of existing techniques in ECG based biometric. Ideas for future research as well as for the detailed application of ECG based biometrics to security are given, concluded by the obligatory summary. The aim of the chapter, to be suitable for "for senior undergraduate and postgraduate studying in the computer security courses" is achieved and a very nice overview with lots of new aspects is given. To sum it up, this chapter is worth reading since it gathers the newest information related to biometric "heart-activities-based" authentication approaches.

Part C: Networking

Chapter 18: Peer-to-Peer Botnets

Since classic botnets with a centralized command and control (C&C) architecture are already well known, this chapter focuses on the peer-to-peer (P2P) botnets. In detail, botnet construction, C&C mechanisms, performance measurements, and mitigation approaches are covered. After presenting bot-net architectures, the P2P approach is explained in an easy to understand way. Based on this, the methodologies for constructing P2P botnets are explained in a very basic way, where no knowledge about malware technologies, protocol handshakes or mathematical procedures is needed. The required level of knowledge is very low, which makes the first part of the chapter suitable for undergraduates as well as for other interested people. More interesting facts are presented in the second part, wherein the "quality" of a botnet is measured.[9] After the presentation of the identified risks and their assessment, the countermeasures are explained finally. This is done in a summarizing way, citing only the relevant papers and current scientific work.

Although this chapter wanted to provide "a systematic study on P2P botnets" it only gives a fundamental overview about existing (threatening) technologies and how to deal with them in an appropriate way. For practitioners, the added value is only a compact summary – for implementation uses the related work has to be studied. Scientific research interests can not be satisfied.

Chapter 19: Security of Service Networks

This chapter focuses on the security of service networks. Therefore, basic knowledge of service oriented architectures (SOA) and infrastructures (SOI) is desirable to enable the reader to extract the relevant information of the comprehensive presentation of diverse subtopics quickly. The content extends over 32 pages which are illustrated by several figures and two summarizing and useful tables pointing out the "main challenges and innovations against aspects of business life-cycle".

It satisfies the interests of practitioners as well as the ones derived from scientific research although it is sometimes a little bit confusing because of the contents being not clearly separated. To get a short impression of the topics mixed up, here are some of the summarized contents.

- Security Token Service design for identity and access management
- internal functional components and external interactions of a "next-generation prototype of an service-level authorization capability"

[9] Therefore, the metrics of effectiveness, efficiency and robustness are analyzed.

- guidelines for the creation of policies
- architectural design of compliance and governance aspects (concerning frameworks, best-practices and standards)

To sum it up, it has to be said that it is not clearly pointed out if the concepts and frameworks which are presented in this chapter are suitable for practitioners or scientific research. On the one hand, they are presented in a way that is (currently) far away from applicability focusing on the so called "next generation" features. On the other hand, detailed hands-on guides for implementing the technologies presented are given. Although the research was done very well and the article is comprehensive and full of information, it would be better to have less subtopics in some separated papers with a better focus.

Chapter 20: Network Traffic Analysis and SCADA Security

This chapter focuses on network traffic monitoring and analysis. After introducing the fundamental concepts, the methods for collecting traffic measurements are explained followed by different methodologies of analyzing traffic mixtures. The content is presented in a short and concise way, illustrated by about twenty figures (including tables), which are sometimes dispensable because of only showing long traces or network traffic flow reports. Although it is nice to know what kind of reports and protocols can be generated, a simple overview of the abilities would be more suitable for the reader. For the chapter "Frequency-Based Clustering Using Frequent Itemsets" some previous knowledge of Set Theory is necessary to understand the content which is also applicable to the final case study where in addition to this, the reader should be familiar with the concepts of the Big O Notation (Landau notation) to assess the different complexities of the n-dimensional clustering. Since the SCADA systems are currently used for monitoring and controlling industrial systems the security-concepts of these systems are only applicable by special interest groups (practitioners).
Finally, this chapter gives a good overview about network traffic monitoring and analysis.

Chapter 21: Mobile Ad Hoc Network Routing

Chapter 21 deals with the so called MANETs (mobile ad hoc networks). Every section takes notice of the reputation – especially in one-layer and two-layer systems and finishes with an overview about the limitations. The whole chapter gives a good overview about the topic and is supported through important tables comparing the different reputation schemes. Although this overview only covers 14 pages the authors accomplish to provide an enhancement of the MANET routing mechanisms.

Chapter 22: Security for Ad Hoc Networks

After having introduced the mechanisms of "Ad Hoc Networks" in the previous chapter, the concepts are extended focusing on security aspects.[10] First, the security requirements are explained and the different challenges arising in this context are presented. Since they are "similar to those of other practical networks" there are no new aspects for readers who are familiar with concepts besides the so called "wormhole-attack". The most interesting aspects are identified during the implementation of the AES- and the Needham-Schroer-protocol. In my opinion, there was no need to examine the MD5-protocol because of the different attacks already in place.[11] To sum it up, this chapter is really giving some new aspects to the reader concerning the implementation of detailed protocols including the different challenges which may arise.

Chapter 23: Phishing Attacks and Countermeasures

The last chapter of the third big block (Part C) covers the aspects of phishing attacks and the corresponding countermeasures. Therefore this tiny part of the cyber crime economy is described first giving an overview about the historical background and the ways of how to proceed a phishing attack. The following article explains the different classic concepts which might be interesting for readers who have

[10] It has to be mentioned that the chapter is not written by the same authors. Therefore some concepts are redundant.

[11] Collision-attack, chosen-prefix collision attack and the theoretically broken preimage resistance.

never heard about the topic. New aspects are given in the chapter which describes the advanced techniques of phishing like Fast Flux, Randomized Subdomains of Flash Phishing. The obligatory chapter about countermeasures is questionable in my opinion. Although the presented concepts are correct and useful it looks a little bit like an advertisement of a product specification of the company where the author works at. To avoid this indirect product placement it would be useful to give some hints on further work and not only citing five year-old resources as well as the Symantec Security Response blog.

Part D: Optical Networking

This part focuses on optical networks and more specifically how these networks can be used in conjunction with chaos theory to implement secure communication links.

Chapter 24: Chaos-based Secure Optical Communications Using Semiconductor Lasers

This chapter gives an overview of the developments and achievements in the field of secure optical communication realized using semiconductor lasers. The introduction starts by explaining chaos theory basics to bootstrap the content with its origins. Then it lays further fundamentals by illustrating the phenomenon of chaos synchronisation, which allows to produce synchronized chaos by two distinct and coupled systems opening the door to chaos-based secure communications and message encryption techniques, which describe different categories to construct chaos-based encryption schemes. The three main categories are dealt with in this chapter (chaos masking, chaos-shift keying and chaos modulation), before going into the basics of chaotic laser systems. Here, the essentials of lasers and laser dynamics are given as well as how such lasers can be used to generate chaos. Bringing all this together, results in the main discussion thread of this chapter. The available schemes—from early experiments to the current state of the art—are described and evaluated in detail. A conclusion at the end summerazises the comparative advantages of the different schemes and gives a guide on where the route is heading.
Overall the author of this chapter, Alexandre Locquet, introduces the topic of chaos-based secure communication from the ground up. This enables the reader, who is not familiar with the topic or all of the involved disciplines, to understand basics concepts and to follow the content flow of the paper. Moreover, the author managed to give a comprehensive overview of the advances in the field of secure optical communications based on chaotic semiconductor diode lasers from the early beginnings to the contemporary state of the art. By this, the reader gets a friendly introduction to message encryption techniques making use of chaos synchronisation and the laser type, which by far provided most of the momentum in this field proving e.g. to reach transmission rates of Gb/s through a commercial fibre network spanning one hundred kilometer. For more advanced readers this chapter is still useful, since it sums up the field as well as its literature in a very handy manner and gives some thoughts on open research and development challenges.

Chapter 25: Chaos application in Optical Communications

This chapter deals with the same topic as the previous one. In fact, huge parts in both chapters are similar. Although it may be nice to read about the same concepts and technologies twice, written from different authors providing different viewpoints and details, still the essential contents remains the same. In addition to the previous chapter, the reader gets some more insights in current developments based on either the all-otpical or the optoelectronic concept. Then, a short description of the experimental testbed in Athens, which marks the current state of the art for laser diode based chaotic optical communication systems and let to the Nature article by Argyris, Syvridis et al. (who are the authors of this work).
Overall the question remains, why these two chapters could not have been merged or synchronized in a way to build upon on each other.

Part E: Wireless Networking

This part of the handbook deals mainly with security in wireless sensor networks (WSN). An overview and comprehensive state of the art is given in chapter 26. The following chapter 27 focusses on secure routing in WSNs and chapter 28 discusses a specific application for surveillance purposes. Only chapter 29 is more general and includes other wireless networks such as GSM, UMTS, WLAN and WiMAX.

Chapter 26: Security in Wireless Sensor Networks

This overview paper starts with an basic introduction to wireless sensor networks (WSN). The typical structure of a WSN is described as well as the different sensor nodes. For illustration purposes available sensor nodes are listed in a table with some example nodes being showed in figures. The specific security challenges of WSNs are motivated in general and by describing use-case scenarios from different domains including military, environmental, health and home applications. Following a short introduction to communication aspects in WSNs the paper discusses challenges in WSNs including fault tolerance, routing, mobility and scalability.

Security is another challenging area, which is focused in depth. Security topics in WSNs such as data confidentiality, data integrity, authentication, key establishment, availability, privacy, secure routing, secure group management, intrusion detection and secure data aggregation are briefly discussed. The available research work and relevant results are presented in a short but pregnant manner, referencing the main contributions in the respective field. Attacks related to WSNs are described subsequently. The targeted attacks are node capture, side channel, denial of service, software, routing, traffic analysis, sybil and replication attacks as well as attacks on in-network processing and on time synchronization protocols.

The remaining sections focus on key management in WSNs, since this is a core prerequisite to enable security services such as confidentiality, integrity and authentication. The distinct approach are structured into four categories according to the properties of the available schemes. Key pool based key management relies on the core principle of a key pool containing a large number of keys with unique identifiers. The different methods that have been proposed are presented, describing how they organize and distribute the keys amongst the nodes. In session based key management the keys are generated dynamically on-demand during the establishment of a session between pairs of nodes. Hierarchical based key management makes use of hierarchical data structures (mainly trees) to establish and manage keys of child and parent nodes. Finally, key management for heterogeneous sensor networks (HSN) which consist of a few powerful and a large number of low-end sensors is discussed.

Chapter 27: Secure Routing in Wireless Sensor Networks

After a short introduction into WSNs the challenges and importance of implementing a secure routing protocol are emphasized. Known attacks on WSN routing are introduced along an attack classification. Following specific WSN routing protocols which have shown to be vulnerable to the presented attacks are described. By this, the practical relevance of the attacks as well as the awareness of pitfalls are raised. The present chapter closes by giving an overview of secure WSN routing protocols. Due to the fact that a secure routing protocol which has been designed for a hierarchical routing platform will neither have the same efficiency nor scalability when implemented on a flat or planar routing environment.

Chapter 28: Security via Surveillance and Monitoring

A case study on applying WSNs for surveillance and monitoring purposes such as indoor smoke detection is presented in this chapter. It examines how energy efficiency might be achieved by utilizing the redundancy in the network and turning sensor nodes on and off periodically (also known as duty-cycling). Two distinct approaches are modelled and simulated. One is based on randomness to determine the sleep schedule and the other relies on a coordinated sleep schedule.

In addition, instead of constantly monitoring of any particular anomaly, this type of WSNs also needs to continuously monitor itself. This work analysis according approach again with the focus on energy efficiency.

Chapter 29: Security and Quality of Service in Wireless Networks

This chapter is the first and only targeting other wireless networks than WSNs. The security of wireless networks is address broadly. After setting the foundations of general security aspects and requirements, the integrated security mechanisms of four major wireless networks are described, namely GSM, UMTS, WLAN and WiMAX.

The following section is dedicated to security from the viewpoint of the physical layer. It is argued, that high-layer encryption techniques will not provide a comprehensive answer to the challenges of the

upcoming 4G networks. The early fundamental work on wireless information theoretic security (WITS) is revisited under the light of contemporary breakthrough research in channel coding. This opens the path for future research, for which open issues are discussed.
The last part of this chapter deals with the interoperability of distinct wireless networks and schemes supporting security provision in such heterogeneous environments.

Part F: Software

This part accumulates articles with a focus on software. The covered aspects range from low-level attacks and defence techniques to software, reverse engineering of software, viruses and other malware to security consideration at the programming language layer. Two sections on Trusted Computing related aspects are furthermore included in this part.

Chapter 30: Low-Level Software Security by Example

This chapter aims at providing insights into low-level software attacks and defence techniques. By selecting four representative examples, major types of attacks on C/C++ software are discussed. Amongst these are stack-based buffer overflows, heap-based buffer overflows, jump-to-libc attacks and data-only attacks. Each of these attacks is described along the lines of an example. Constraints as well as variants are discussed at the end of each attack section.
To protect software against the introduced attacks, four defence techniques are described. They have been selected according to their effectiveness, wide applicability and low enforcement overhead. The given defences include stack canaries, non-executable data, control-flow integrity on code execution and randomized in-memory code and data layout. Again, each defence is discussed according to the introduced overhead, limitations, variants and possible counter attacks.
The attacks and defences are described in enough detail to be understood even by readers without background in software security.

Chapter 31: Software Reverse Engineering

In this chapter, Teodoro Cipresso and Mark Stamp cover software reverse engineering (SRE). They introduce the topic by first giving reasons for reverse engineering of software. In general, SRE is deployed when the interoperability with proprietary software is required, the conformance of design and implementation needs to be verified, the quality and robustness has to be evaluated and the maintenance of legacy software is necessary. In the context of security, SRE follows other goals, which are the detection and neutralization of malware, the testing for weaknesses (of e.g. implementations of cryptographic algorithms) as well as DRM or license protection and the auditing of the security of program binaries. To explain the foundations and most common techniques, the authors focus on two comprehensive case studies for C/C++ based executables for Windows/Intel machines and Java programs. For both case studies, the reversing and patching of a program as well as the application of antireversing techniques are explained in depth. Again for both scenarios, the authors provide a non-trivial implementation of a password safe application which is used to explan the possibilities of reverse engineering. On the other side, by enhancing these programs with antireversing protections, the effects of these protections can be studied by example. The authors offer these resources for download and have added video tutorials in addition. All this makes this chapter a very gentle introduction to the topic suited for self-studies as well as material for lectures and other courses.

Chapter 32: Trusted Computing

Antonio Lioy and Gianluca Ramunno give an overview of trusted computing as defined by the Trusted Computing Group (TCG). Before diving into the details, an introduction lays the foundation of the the abstract concept of trust and summarises shortly previous work on terminology and technology in relation to trusted computing. The rest of the chapter is structured in three main sections providing an overview of the TCG specifications. The first is related to the basic ideas and concepts forming the TCG Trusted Platform Architecture including the trust and threat model as well as remote attestation. The following section focuses on the Trusted Platform Module with its core functionalities and defined cryptographic keys. The chapter closes by giving a short glimpse at the available TCG working groups, which are responsible for specifying infrastructure components such as the development of integration and interoperability standards for the Internet, enterprise and mixed environments as developed by the Infrastructure Working Group or requirements and specifics for server platforms as defined by the Server-Specific Working Group.

Chapter 33: Security via Trusted Communications

This chapter builds upon trusted computing to create a solution for autonomic trust management for mobile communications, services and applications. Trusted computing is one pillar and provides the mechanisms for trust sustainability among the platforms. The other pillar is an adaptive trust control model. It is demonstrated how both layers can cooperate in order to obtain a holistic trust management solution.

Although this topic is targeting a very specific field of application of trust management and presents one particular proposed approach, still the included overview of literature background provides a valuable starting point for a broader audience interested in trust management.

Chapter 34: Viruses and Malware

Viruses and Malware is the topic of this chapter. The author Eric Filiol starts by setting the terminology from a contemporary viewpoint defining the existing categories and modes of operations for these programs. Based on Adleman's classification computer infection programs are discussed from simple malware including logic bombs and trojan horses to self-reproducing malware including viruses and worms. These malware types are gently introduced. Different instantiations and their deployed spreading mechanisms are explained always by emphasizing them by well-known examples. Further attention is paid to the techniques implemented by malware to hide themselves on infected machines as well as make them more resistant to healing attempts. This chapter closes by discussing general strategies to defence and fight against malware and a set of guidelines for "computer hygiene".

Overall this chapter is a well-structured introduction into the malware arena, but it lacks novelty and does reference too few relevant sources for further readings.

Chapter 35: Designing a Secure Programming Language

In opposition of the expectations raised by the title of this chapter, Thomas Austin does not discuss the design of a secure programming language but gives examples how contemporary programming languages and frameworks answer to widely effective attacks coming from vulnerabilities software created by inexperienced or careless developers. In the first two sections some example attacks are introduced along with available defence mechanisms. Code injection attacks are presented first. In the context of web applications this attack type is explained by example. Some defence mechanisms are briefly discussed and available deployments in modern programming languages and frameworks are mentioned mainly for Ruby on Rails and PHP. Buffer overflow attacks are considered next. Some countermeasures are described in general terms without going into any detail. The following section is dedicated to sandboxing and describes according solutions provided by Java and JavaScript. In the last section Metaobject protocols in general and aspect-oriented programming in particular are discussed from a security perspective. Overall, the paper presents a pot pourri of topics at a very high level which have some relation to the chapter's topic but does hardly satisfy a reader's expectation in the anticipated or the containing content.

Part G: Forensics and Legal Issues

In the last part of the present handbook, two chapters on forensic topics and one on technical and legal aspects of large-scale telecommunications systems.

Chapter 36: Fundamentals of Digital Forensic Evidence

The characteristic of chapter 36 is, that it introduces the field of digital forensics and more specifically the capturing of digital forensic evidence (DFE) by describing the general process. DFE must be identified, collected, preserved, transported, stored, analysed, interpreted, attributed, perhaps reconstructed, presented, and, depending on the court orders, destroyed. The structure of this chapter follows exactly this process order and explains each steps in general terms. Further aspects including forensic tools, legal requirements, faults, testimony and many more complete this chapter. It leaves out the consideration of forensic tools intentionally and focuses on the underlying process and challenges. By this, it becomes a valuable source for those who want to enter this field. A bit of a drawback is that the legal discussions are considering US law only.

Chapter 37: Multimedia Forensics for Detecting Forgeries

To detect forgeries in multimedia content, three different classes of schemes can be distinguished: watermarking, perceptual hash functions and multimedia forensics. All of these methods act at different levels of efficiency and accuracy. Examples of multimedia forgeries are given in the first section in order to motivate the demand for such detection methods. Then a general forgery detection techniques are reviewed and compared. The main part focuses on multimedia forensics and investigates the state of the art of which each available scheme performs an unique function such as duplication, photo montage and synthetic image detection. The comprehensive overview and analysis is followed by a section on open issues including e.g. detection accuracy, counter attacks and test beds. Overall, this chapter is a valuable introductory source and state of the art analysis for readers interesting in entering this topic.

Chapter 38: Technological and Legal Aspects of CIS

The final chapter of the present handbook of information and communication security deals with the introduction of basic security services, discusses their adoption in two concrete real world systems and lists the legal frameworks to be considered when developing security architectures for large-scale telecommunications systems. In conjunction with the OSI model, the security services confidentiality, integrity, authentication, non-repudiation, access control and availability are briefly discussed. For each OSI layer the authors list some common best practice security components available for implementing these security services. A historic view on the development of international legislation in the context of information networks is described next. This description is limited to the appearance and existence of particular milestones, but does neither go into details nor does it give a comprehensive view on all relevant legal frameworks. The real value of this chapter should have come through the description of real world systems as case studies. The explanations are essentially focused on a specific telemedicine system to improve emergency health care services at understaffed rural areas and out of coverage urban spots, such as the underground rail way. Its adoption to other domains is mentioned but is not further detailed. Together with a confusing structure, the merits of this chapter remain low. Especially the weak legal part does not provide any suitable insides or guidance for the reader to the this complex topic—which is by the way the only on legal aspects and the reason why the whole book part contains the word legal in its name.

3 Recommendation

What this handbook impressively shows is that the field of information and communication security is huge. Thus, such a handbook is definitely required in order to give a structured guide to access the domain and its topics. This is what the book aims at having researchers, graduate students and university instructors as audience in mind.

The handbook achieves this goal only partly. As can be seen from the individual discussions on each chapter, the content is presented in very different ways by the distinct authors. Since this is somehow natural, still one's expectation is to have a book at hand which enforces a much stricter policy on how to introduce, describe and explain each topic. The only common ground of each chapter is the references and authors' biography sections at the end. Due to the lack of such a policy, some chapters remain much too unspecific and high level whereas others go into much detail. Overall the reader can get the impression, that this is just a decoupled collection of papers, whereof a few seem actually dispensable.

Giving a clear recommendation for the present handbook is henceforth not straightforward. The strength of it remains in the individual strength of each chapter. A reader interested in purchasing a copy is therefore recommended to inspect the most targeted chapters in order to evaluate whether this handbook provides the desired content.

Kilian David works as an IT-auditor in Germany.
Luigi Lo Iacono is professor at the Cologne University of Applied Sciences in Germany.