BOOK REVIEWS

EDITED BY PIOTR CHOLDA

CRYPTOGRAPHY FOR SECURITY AND PRIVACY IN CLOUD COMPUTING

BY STEFAN RASS AND DANIEL SLAMANIG

ARTECH HOUSE, 2013, ISBN 978-1-60807-575-1, HARDCOVER, 255 PAGES

REVIEWER: MIRALEM MEHIC

Cloud computing is progressively entering our lives with the idea of renting computing infrastructures to customers. Therefore, it is important to consider the security of this service as the user's data is now deployed to distant remote storages not controlled by the data owner. The classical CIA+ security approach should be extended in such a way that a cloud can guarantee an adequate security level for the offered services. It is especially important to consider usage of paid cloud services: from the provider's perspective it is necessary to give only those resources that have been paid for. Similarly, for the clients it is important to receive everything they have purchased. Consequently, access control and authentication mechanisms must be considered at a much more fine-grained level than we are used to. Rass and Slamanig explore major security challenges in clouds, avoiding the technical details of cloud computing, legal aspects, platform and hardware details. They provide a well-organized book divided into six chapters forming a complete reference on the topic.

Chapter 1 briefly explains the main goals of the authors' research and provides a good introduction to cryptography and security problems in clouds. Chapter 2 focuses on the fundamentals of cryptography, refreshing the reader's knowledge of the basic mathematical tools, security postulates and requirements. The authors briefly show how to practically use complex mathematics, and give definitions with short examples. The chapter contains an explanation of number theory, algebraic structures, elliptic curves, Hamming distance, the RSA problem, basic cryptographic primitives, and security models.

Chapter 3, the longest in the book, is mainly concerned with privacy and challenges for conversation in cloud computing. Techniques for protecting identities inferred from a protocol participation (anonymous communication, authentication, and access control), as well as information leakage from pure data, are presented. Attention is especially paid to anonymous authentication, a comparison of several such methods, and algorithms to dissolve anonymity of a user in case of fraud. The chapter also gives a short explanation of popular anonymous credential systems like Camenisch-Lysyanskaya Credentials and Brands Credentials. The authors finalize this chapter with a very interesting explanation of methods for preventing a service provider from learning which data items have been accessed in which order by which client.

Chapter 4 provides an explanation of access control via encryption. Various encryption schemes are presented and compared. A very interesting fragment of this chapter is devoted to the analysis of homomorphic encryption schemes proposed for the first time in 1978 by Rivest. Due to this concept, public key encryption schemes with algebraic manipulations on ciphertext take effects on the inner plaintext through the encryption. Homomorphic encryption types are explained, including example systems such as Unpadded RSA, ElGamel, Paillier, BGN, and Gentry.

Chapter 5 is focused on remote data storage problems. The authors begin with an analysis of remote data checking and the possibility for the user to efficiently verify that a remotely stored file is available and can be fully recovered on demand. Then the authors deal with secure data deduplication reducing the storage overhead for a provider. This chapter is interesting from the steganography viewpoint, since it presents possible covert channels created using options to upload and download a file from the cloud.

The book concludes with the analysis of practical issues, standardization, and implementations of cryptographic primitives which are displayed in a short Chapter 6. Cryptography in clouds is still at an early stage from the practical implementation standpoint. As the authors noted in the final outlook, many of the methods are the subject of intensive ongoing research, and it will take time to develope the results of current research.

This book is organized in a readable form, with brief explanations at the beginning of each topic covered. The authors reference a broad literature, putting the reader in a great position for further research. Cloud architects and security administrators will find this work useful and interesting. Although the authors tried hard to reduce the mathematical complexity of the discussed problems, some fragments will not be easily understood without having a broad knowledge of the related theoretical methods. Thus, I recommend this work to readers with a solid mathematical background.

COMMUNICATIONS NETWORKS: AN OPTIMIZATION, CONTROL AND STOCHASTIC NETWORKS PERSPECTIVE

BY R. SRIKANT AND LEI YING

CAMBRIDGE UNIVERSITY PRESS, 2014, ISBN 978-1-107-03605-5, HARDCOVER, 352 PAGES

REVIEWER: KRZYSZTOF RUSEK

In their short book Srikant and Ying include many topics important to deal with performance evaluation of modern telecommunications networks. The book is a good source of applications of optimization, control, and queuing theories, as well as scheduling and selected graph algorithms that can be applied in the design and operation of communication networks.

The book is organized in two parts. In the first, entitled "Network Architecture and Algorithms," the authors present basic algorithms to be used as tools. They also elaborate on mathematical properties of these algorithms. While Chapter 1 presents a basic introduction, Chapter 2 provides fundamental notions of optimization and control theory with additional remarks about game theory and utility functions, all in the context of network resource allocation. In Chapter 3 networks are presented in a dynamic way. The authors begin with the Chernoff bound and the concept of statistical multiplexing. Other topics covered embrace discrete-time Markov chains and Little's law. The chapter ends with discrete time queuing systems. Chapter 4 exposes the internal architecture of switches and routers. After a short technical description, different scheduling algorithms are discussed. The next two chapters are oriented toward wireless networking. Chapter 5 describes scheduling in wireless environments, while Chapter 6 extends the idea of network utility maximization (presented in Chapter 2) to wireless networks.

Chapter 7 is devoted to network protocols and the principles behind their design. The chapter begins with a basic introduction of the TCP protocol and its mathematical model. Later on, different variants of TCP are discussed. Then the chapter focuses on routing with Dijkstra and Bellman-Ford algorithms. Surprisingly, the chapter contains some basic information about IP addressing, but this can be treated only as a short revision. The last chapter of the first part is devoted to Peer-to-Peer (P2P) networking. A reader seeking information about Distributed Hash

Tables (DHT) will not be disappointed. The chapter also offers remarks about streaming and file sharing in P2P network.

The second part of the book, entitled "Performance Analysis," describes more advanced mathematical techniques. Chapter 9 contains a highly condensed yet easy to read queuing theory in continuous time, including simple Markov chain systems and even Jackson networks. Chapter 10 presents asymptotic analysis of queues in the two regimes: with heavy traffic and large deviations. As the authors point out, heavy traffic analysis of queuing systems using Lyapunov techniques is quite unique, and increases the value of the book considerably. The last chapter describes the capacity scaling of wireless ad hoc network and the maximum achievable network throughput.

All the chapters are self-contained, and it makes the book easy to comprehend by a reader interested in a selected, particular topic. The book's structure also helps in this. Chapters follow the logical flow of designing layers of the network. Each chapter brings another aspect of network modeling. Although many algorithms are presented in the form of pseudo-code only, no clarity is lost and the book can be recommended to programmers seeking a solid reference. The most important theorems are presented with proofs, a feature that is desirable but not common in books targeted to engineers.

The level of mathematical formalism required to understand the book is not beyond the level of graduate students after a strong course in probability. Short revisions of mathematical backgrounds along with working examples also make it easier to understand the material. Exercises are interesting and feel like real research problems. With solutions available to instructors, this book is also an excellent choice as a textbook for a performance evaluation course. The most appreciated feature of this work is its freshness: all the examples and exercises are up to date. This makes classic theories more attractive to students, who can see the real applications of complex mathematics, and motivate them to dive into the exciting world of network optimization and control.