SAFETY OF WEB APPLICATIONS: RISKS, ENCRYPTION AND HANDLING VULNERABILITIES WITH PHP

By Eric Quinton, ISTE Press–Elsevier, 2017, ISBN 978-1-78548-228-1, hardcover, 209 pages

Reviewer: Piotr Cholda

Security of communication networks is one of the broadest fields in today's vivid list of subjects interesting from the viewpoint of our magazine. 'Broad' means here that it covers topics starting from a very classical and sophisticated theoretical group of ideas (such as cryptology) to the ones focused on very practical problems. The latter are of the transient nature due to very fast changes in technology, protocols, software languages applied, etc. These topics concern current aspects of dealing with vulnerabilities of popular Internet applications. The book by Quinton is devoted to a subset of them. In this case, we are given a book focused on web applications, mainly supported by PHP. The book is written by an experienced practitioner for practitioners. While there is some data provided that can be treated as an introduction or revision of basic material, the main advantage of this concise, yet very informative, position is especially related to precise recipes given to programmers with the aim to make software and systems developed by them less vulnerable to attacks.

Chapter 1 is devoted to a presentation of the concept of web applications and the rationale why and how in general they should be secured. Chapter 2 gives an overview of risk and the related notions, such as CIA (confidentiality, integrity, availability), along with their desired levels. Then, the next chapter discusses the basics of encryption supporting web applications. Except for presenting the concepts, some examples of instructions start to be given (e.g., how to create certificates with the use of OpenSSL). The author also describes how to read the related configuration files. Then, the two most comprehensive and important chapters of this work follow. They deal with some of the most important recognized vulnerabilities and give exact instructions about how to remove them (with a description of the mitigation philosophy and the related code). This way, Chapter 4 is devoted to the most important threats as listed by the OWASP project (2013). On the other hand, Chapter 5 focuses on how to manage user logins and assign permissions in relation to web applications. Again, a ready-to-use code is provided. The last two chapters deal with the MVC (model, view, controller) model of development for web applications as well as with recommendations on how to implement and test a secure application.

The book is written in a very clear way, easy to understand even for undergraduate students. However, due to the fact that some level of understanding of a code is necessary, experts will gain the most of getting acquainted with this position. For sure, this is a must have book for anybody interested in developing web applications.

THE MATHEMATICS OF SECRETS: CRYPTOGRAPHY FROM CAESAR CIPHERS TO DIGITAL ENCRYPTION

By Joshua Holden, Princeton University Press, 2017, ISBN 978-0-691-14175-6, hardcover + jacket, 373 pages

Reviewer: Piotr Cholda

Security is surely a hot topic in communications. Except for protocol and management issues, the most classical and venerable part of the field is obviously related to enciphering information so that it cannot be read by an unauthorized user. Surely, this is one of the oldest and mostly mathematics-oriented aspect of security.

To briefly summarize what the book prepared by Joshua Holden shows to a reader, I will only present the skeleton of the main ideas, yet it is necessary to emphasize that each of the chapters contains a lot of side information, which is always relevant. On the other hand, not the selection of the topics, but the way they are presented, is really distinguishing. First, substitution and transposition ciphers, along with the main ideas on the related cryptanalysis, are described. Then, more contemporary ciphers are given, i.e., DES, AES, and stream ciphers. Next, the public-key cryptography based on the exponentiation is covered. As the presentation is generally given with respect to the historical development, at the end some newer topics are gathered, such as elliptic curve cryptography, as well as threats and opportunities related to quantum-related concepts.

What I like about the book is that the author always shows that the area of cryptography is related to the application of mathematics. This idea is perfectly aligned with the book title. That is, even if the author presents a very basic cipher, such as the Caesar's cipher, he presents its mathematical description, in this case related to modular arithmetic, and he also introduces the notion of inverse modulo and Euclidean algorithm. On the other hand, while the book clearly shows that mathematics is necessary to understand and develop ciphers, the contents give the theoretical material at the basic level. Yet simultaneously, the readers are encouraged to broaden their knowledge: each chapter is appended with very interesting related notes. They form a good extension for those readers interested in broadening their knowledge on a topic, and the notes are enriched with a set of references to the literature.

Except for giving the definition of the most important groups of ciphers, and their mathematical description, the book also elaborates on the main cryptanalysis methods. While the most evident successes related to this subfield have been achieved on the basis of sophisticated mathematical works, the book balances the need to present the ideas with theoretical depth. Hence, it is neither too shallow nor too complex. Surely, the ideas are presented very clearly with many examples that are easy to understand. This way, Holden's work can be treated as a perfect introduction to a layman, whose mathematical skills are at most at a high school level. On the other hand, the book can also be perceived as a good introduction for a person who has not met the topic before, but will be encouraged by the book to reach for a more advanced description.