Chapter 1

Introduction to information security foundations and applications

Ali Ismail Awad[1,2]

1.1 Background

Information security has extended to include several research directions like user authentication and authorization, network security, hardware security, software security, and data cryptography. Information security has become a crucial need for protecting almost all information transaction applications. Security is considered as an important science discipline whose many multifaceted complexities deserve the synergy of the computer science and engineering communities.

Recently, due to the proliferation of Information and Communication Technologies, information security has started to cover emerging topics such as cloud computing security, smart cities' security and privacy, healthcare and telemedicine, the Internet-of-Things (IoT) security [1], the Internet-of-Vehicles security, and several types of wireless sensor networks security [2,3]. In addition, information security has extended further to cover not only technical security problems but also social and organizational security challenges [4,5].

Traditional systems' development approaches were focusing on the system's usability where security was left to the last stage with less priority. However, the new design approaches consider security-in-design process where security is considered at the early phase of the design process. The new designed systems should be well protected against the available security attacks. Having new systems such as IoT or healthcare without enough security may lead to a leakage of sensitive data and, in some cases, life threatening situations.

Taking the social aspect into account, security education is a vital need for both practitioners and system users [6]. Users' misbehaviour due to a lack of security knowledge is the weakest point in the system security chain. The users' misbehaviour is considered as a security vulnerability that may be exploited for launching security attacks. A successful security attack such as distributed denial-of-service attack will impose incident recovery cost in addition to the downtime cost.

[1] Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Sweden
[2] Faculty of Engineering, Al Azhar University, Qena, Egypt

These are just some representative examples to illustrate the diversity and importance of a broad understanding of security issues across the wide range of information processing tasks encountered in the modern world. While, naturally, a single book cannot cover every relevant technique and security approach which can be deployed, or present an example of every application for which a detailed security analysis is important in a practical environment, by introducing carefully selected topics and, especially, by inviting key practitioners in the field to present and discuss them, it is possible to provide both a thorough overview of the field and an appreciation of the fundamentals of this increasingly important and influential area.

As the following section will explain, the book is split between a discussion of some principles and fundamentals which underpin the study of information security in all its diversity, and the working out of these principles in practice, giving an insight into practical system implementation in a range of different application domains and deploying a variety of technologies.

1.2 The structure of this book

This book comes in two main sections: Theories and Foundations and Technologies and Applications. The first section offers theoretical foundations to different information security aspects; however, the second section deals with many technologies and applications from a technical perspective. The general philosophy behind the book is to present balanced materials from the theoretical and the technical viewpoints. In the following pages, we shed light on the contents of the book.

1.2.1 Part I: Theories and foundations

This part is mainly dedicated to the foundations and the theoretical concepts of information security in different domains. The part has eight chapters in total, including this chapter, Chapter 1. A brief summary of each chapter in this part is as follows:

Chapter 2, 'Information security foundation, theories and future vision', presents a solid overview on information security theories and foundations with a focus on information security needs and applications. Several information security-related aspects such as information assurance, cybersecurity, and information systems security are highlighted. Information security confidentiality, integrity, and availability and other information security key definitions are described throughout this chapter according to International Organization for Standardization and National Institute of Standards and Technology [7]. Security vulnerabilities and threat protection approaches are also discussed as part of this chapter [8]. An overview of the information security future vision is presented as the last section at the end of the chapter.

Chapter 3, 'Information systems security issues in the context of developing countries', takes information systems security to the developing countries' dimension [9,10]. This review presented throughout this chapter is relevant for understanding the current state of information systems security in the developing countries. The chapter finds security vulnerabilities and risks increase together with the technology proliferation. The chapter identifies the reasons behind the lack of information systems security deployments in the developing countries from non-technical perspectives. Issues such as education, legalization, policies, and cultures are discussed to emphasize their impacts on information systems security applications within the developing counties' framework.

Chapter 4, 'Biometric systems, modalities and attacks', focuses on biometrics as science for human identification using some physiological or behavioural characteristics [11]. Biometrics is considered as an emerging technology for providing access control for civilian and forensic applications [12,13]. The chapter presents an overview of the biometric system's components and attributes, biometric modalities, and the required features or criteria for selection of biometric modalities. The performance evaluation parameters for a generic biometric system such as false match rate and false non-match rate are offered [14]. Data fusion techniques and performance evaluation of multi-model biometric systems are described as well [15]. Biometric standardizations are well documented at the end of this chapter.

Chapter 5, 'Foundation of healthcare cybersecurity', studies healthcare as an area where information and cybersecurity play a crucial role due to the sensitivity of hosted or exchanged patients' information [16,17]. The chapter offers a solid foundation of the healthcare security and privacy considerations. Major components of generic healthcare systems and the associated security and privacy requirements are presented within the contents of the chapter. Security threats' landscape and vulnerabilities exploited for healthcare cyberattacks are identified and discussed in addition to several attack types [18]. Tools for defending and mitigating security attacks are discussed and reported at the end of the study [19].

Chapter 6, 'Security challenges and solutions for e-business', connects e-business domain to information security by studying the common security attacks, threats, and countermeasures in e-business [20,21]. The chapter discusses new attacks mitigation approaches as of biometrics authentication [22–24], attacks identification using machine learning and data mining mechanisms, blockchains for peer-to-peer security accomplishment, security modelling, and security-as-a-service [25]. Apart from the technical concepts, the chapter sheds light on the social dimension by studying the impact of information security education and user involvement on defending the security attacks on e-business [26]. The chapter is also well connected to biometric systems described in Chapter 4.

Chapter 7, 'Recent security issues in Big Data: from past to the future of information systems', bridges both information security and Big Data by presenting a study on the trendy security issues in Big Data [27,28]. The chapter highlights information security concepts such as privacy, integrity, availability, and confidentiality on the Big Data discipline. Advanced Big-Data-related topics like Cloud Security Alliance, security standards in Big Data, and Information Systems Audit and Control Association are also described [29]. Finally, the chapter explains a use case on Big-Data security.

Chapter 8, 'Recent advances in unconstrained face recognition', goes a step further in biometric technology by reporting the recent trends and advances in face recognition systems in unconstrained environments [30,31]. In two separate sections, the chapter presents comprehensive information on face representation methods and the available benchmark databases for face recognition [32,33]. The chapter explains the metric learning approaches and pose-invariant face recognition challenges as advanced topics in the face recognition domain. Performance evaluation of face recognition and open issues for future consideration are mentioned at the end of this chapter. The foundation information in this chapter is well connected to the previous chapters such as Chapters 4 and 6.

1.2.2 Part II: Technologies and applications

This part of the book covers specific technologies and applications of information security. A broad scope of technical topics is covered in eight chapters contained in this part. A brief summary of each chapter is explained in the following paragraphs:

Chapter 9, 'Hardware security: side-channel attacks and hardware Trojans', addresses relevant topics related to hardware security with a focus on side-channel attacks [34]. The chapter starts with a good preliminary discussion of the significance of hardware security in comparison to the software one. Several side-channel attacks such as power analysis attack, fault analysis attack, and timing analysis attack are presented [35]. A countermeasure for every mentioned attack is described in this chapter. The chapter also clarifies the hardware design and fabrication processes in connection to the security considerations. A separate section is devoted for malicious hardware Trojans detection, classification, and protection at the end of the study [36].

Chapter 10, 'Cybersecurity: timeline malware analysis and classification', focuses on cybersecurity challenges and tackles the problems associated with the proliferation of malware types as serious threats in information systems security [37,38]. A comprehensive malware analysis and classification are presented as preliminary work. The chapter presents a cumulative timeline analysis approach for malware detection that achieves high accuracy over an extended time period. The chapter offers very rich information on malware collection, analysis, and classification with a great focus on presenting different algorithms and technical explanations [39].

Chapter 11, 'Recent trends in the cryptanalysis of block ciphers', presents cryptanalysis of block ciphers as a challenge in data cryptography research domain. The chapter starts with an interesting overview of cryptography and moves forward to focus on symmetric key cryptographic primitives [40,41]. Block cipher definitions, design, and security are explained in separate sections. Attacks on block ciphers such as linear cryptanalysis, differential cryptanalysis, and integral cryptanalysis are intensively covered within the chapter [42,43]. The developments in the conventional block cipher attacks along with the newly surfaced ones are presented. The chapter concludes that block ciphers and their security are still hot research topics.

Chapter 12, 'Image provenance inference through content-based device fingerprint analysis', focuses on digital forensics as a relevant domain of information security. It offers a technical study on image provenance inference that aims to determine the source of a digital image. The chapter highlights the current challenges in image provenance [44,45], and it goes further by introducing different intrinsic device fingerprints and their applications in image provenance inference. The chapter ends by a comprehensive outlook to the future of image provenance inferences in the light of Internet development and Big-Data proliferation [46].

Chapter 13, 'EEG-based biometrics for person identification and continuous authentication', offers a study of the usage of electroencephalogram (EEG) signals as a biometric identifier for human identification and authentication [47]. The chapter offers detailed descriptions on human brain, types of EEG signals, EEG sensing techniques and EEG analysis [48,49]. A separate section is devoted for EEG signals as a biometric trait, including the selection criteria and EEG feature extraction [50]. Human continuous authentication, using EEG in multi-modal biometric systems, and the current challenges of EEG-related research are explained at the end of this chapter [51]. The chapter is well connected with Chapters 4, 6, and 8.

Chapter 14, 'Data security and privacy in the Internet-of-Things', bridges information security with the IoT paradigm [52]. Nowadays, IoT model has plenty of applications in many domains, including healthcare, smart cities, smart homes, and automation and controls [53]. The chapter presents the IoT infrastructure and the emerging security risks from deploying IoT. Security solutions and countermeasures for IoT systems are studied and discussed throughout the chapter. The chapter tackles a social security aspect by connecting human factors with other aspects in IoT security and privacy [54]. The chapter has a good balance between technical and conceptual aspects, and it is well connected to Big-Data security in Chapter 7.

Chapter 15, 'Information security algorithm on embedded hardware', presents a study on the deployment of information security algorithms on embedded hardware [55,56]. The chapter opens by a general introduction and moves forward to the classification of embedded systems [57]. The chapter explains the security requirements and deployment mechanisms for embedded hardware with a little focus on hardware security vulnerabilities [58]. This part of the chapter is well connected with Chapter 9 about side-channel attacks. The chapter closes by discussing the implementation strategies of a security algorithm on embedded hardware. This chapter is considered as a reference point for future applications of information security algorithms on different types of embedded hardware.

References

[1] King J, and Awad AI. 'A distributed security mechanism for resource-constrained IoT devices'. *Informatica (Slovenia)*. 2016;40(1):133–143.

[2] Grzenda M, Furtak J, Legierski J, and Awad AI. Network Architectures, Security, and Applications: An Introduction. Grzenda M, Awad AI, Furtak J, and Legierski J, editors. Advances in Network Systems : Architectures, Security, and Applications. Cham: Springer International Publishing; 2017. pp. 1–10. Available from: https://doi.org/10.1007/978-3-319-44354-6_1.

[3] Grzenda M, Awad AI, Furtak J, and Legierski J. *Advances in Network Systems: Architectures, Security, and Applications*. Advances in Intelligent Systems and Computing; Springer International Publishing Switzerland; 2017.

[4] Charif B, and Awad AI. Business and Government Organizations' Adoption of Cloud Computing. Corchado E, Lozano JA, Quintián H, and Yin H, editors. Intelligent Data Engineering and Automated Learning – IDEAL 2014: 15th International Conference, Salamanca, Spain, September 10–12, 2014. Proceedings. Cham: Springer International Publishing; 2014. pp. 492–501. Available from: https://doi.org/10.1007/978-3-319-10840-7_59.

[5] Charif B, and Awad AI. 'Towards smooth organisational adoption of cloud computing a customer-provider security adaptation'. *Computer Fraud & Security*. 2016;2016(2):7–15. Available from: http://dx.doi.org/10.1016/S1361-3723(16)30016-1.

[6] Okoh E, Makame MH, and Awad AI. 'Toward online education for fingerprint recognition: A proof-of-concept web platform'. *Information Security Journal: A Global Perspective*. 2017;26(4):186–197. Available from: http://dx.doi.org/10.1080/19393555.2017.1329462.

[7] Kissel R, Kissel R, Blank R, and Secretary A. 'Glossary of key information security terms'. NIST Interagency Reports NIST IR 7298 Revision 1, National Institute of Standards and Technology; 2011.

[8] McGuire MR, and Holt TJ. *The Routledge Handbook of Technology, Crime and Justice*. Routledge International Handbooks. Routledge; UK, 2017.

[9] Kim D, and Solomon MG. *Fundamentals of Information Systems Security*. Information Systems Security & Assurance Series. Jones & Bartlett Learning; 2010.

[10] Bwalya KJ, and Mutula S. 'A conceptual framework for e-government development in resource-constrained countries'. *Information Development*. 2016;32(4):1183–1198. Available from: http://dx.doi.org/10.1177/0266666915593786.

[11] Jain AK, Ross AA, and Nandakumar K. *Introduction to Biometrics*. 1st ed. Springer US; 2011.

[12] Unar JA, Seng WC, and Abbasi A. 'A review of biometric technology along with trends and prospects'. *Pattern Recognition*. 2014;47(8):2673–2688.

[13] Awad AI, and Hassanien AE. Impact of Some Biometric Modalities on Forensic Science. Muda AK, Choo YH, Abraham A, and N Srihari S, editors. Computational Intelligence in Digital Forensics: Forensic Investigation and Applications. Cham: Springer International Publishing; 2014. pp. 47–62. Available from: https://doi.org/10.1007/978-3-319-05885-6_3.

[14] Dunstone T, and Yager N. *Biometric System and Data Analysis: Design, Evaluation, and Data Mining*. 1st ed. Springer US; 2008.

[15] Gavrilova ML, and Monwar M. *Multimodal Biometrics and Intelligent Image Processing for Security Systems*. 1st ed. Hershey, PA, USA: IGI Global; 2013.

[16] Dong N, Jonker H, and Pang J. Formal Analysis of Privacy in an eHealth Protocol. Foresti S, Yung M, and Martinelli F, editors. Computer Security – ESORICS 2012: 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10–12, 2012. Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012. pp. 325–342. Available from: https://doi.org/ 10.1007/978-3-642-33167-1_19.

[17] Mansfield-Devine S. 'Your life in your hands: The security issues with healthcare apps'. *Network Security*. 2016;2016(4):14–18.

[18] York TW, and MacAlister D. *Hospital and Healthcare Security*. 6th ed. Butterworth-Heinemann; 2015.

[19] Okoh E, and Awad AI. Biometrics Applications in e-Health Security: A Preliminary Survey. Yin X, Ho K, Zeng D, Aickelin U, Zhou R, and Wang H, editors. Health Information Science: 4th International Conference, HIS 2015, Melbourne, Australia, May 28–30, 2015, Proceedings. Cham: Springer International Publishing; 2015. pp. 92–103. Available from: https://doi.org/10.1007/978-3-319-19156-0_10.

[20] Hinde S. 'Privacy and security the drivers for growth of E-commerce'. *Computers & Security*. 1998;17(6):475–478. Available from: http://dx.doi.org/10.1016/S0167-4048(98)80069-2.

[21] Nabi F. 'Secure business application logic for e-commerce systems'. *Computers & Security*. 2005;24(3):208–217. Available from: http://dx.doi.org/10.1016/j.cose.2004.08.008.

[22] Zhang D, and Yu L. *Payment Technologies for E-commerce*. New York, NY, USA: Springer-Verlag New York, Inc.; 2003. pp. 71–94.

[23] Awad AI, and Baba K. 'Evaluation of a Fingerprint Identification Algorithm with SIFT Features'. *Proceedings of the 3rd 2012 IIAI International Conference on Advanced Applied Informatics*. Fukuoka, Japan: IEEE; 2012. pp. 129–132.

[24] Egawa S, Awad AI, and Baba K. Evaluation of Acceleration Algorithm for Biometric Identification. Benlamri R, editor. Networked Digital Technologies. Vol. 294 of Communications in Computer and Information Science. Berlin, Heidelberg: Springer; 2012. pp. 231–242. Available from: http://dx.doi.org/10.1007/978-3-642-30567-2_19.

[25] Zheng Q, Li S, Han Y, Dong J, Yan L, and Qin J. Security Technologies in E-commerce. Zheng Q, editor. Introduction to E-commerce. Berlin, Heidelberg: Springer, Berlin, Heidelberg; 2009. pp. 135–168. Available from: https://doi.org/10.1007/978-3-540-49645-8_4.

[26] Kennedy SE. 'The pathway to security mitigating user negligence'. *Information and Computer Security*. 2016;24(3):255–264. Available from: https://doi.org/10.1108/ICS-10-2014-0065.

[27] Hashem IAT, Yaqoob I, Anuar NB, Mokhtar S, Gani A, and Khan SU. 'The rise of "big data" on cloud computing: Review and open research issues'. *Information Systems*. 2015;47:98–115. Available from: http://dx.doi.org/10.1016/j.is.2014.07.006.

[28] Bertino E. 'Big Data – Security and Privacy'. *2015 IEEE International Congress on Big Data*; 2015. pp. 757–761.

[29] Weber AS. 'Suggested legal framework for student data privacy in the age of big data and smart devices'. *Frontiers in Artificial Intelligence and Applications*. 2014;262:669–678.

[30] Zeng Z, Pantic M, Roisman GI, and Huang TS. 'A survey of affect recognition methods: Audio, visual, and spontaneous expressions'. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2009;31(1):39–58.

[31] Wolf L, Hassner T, and Maoz I. 'Face recognition in unconstrained videos with matched background similarity'. *Proceedings of IEEE International Conference on Computer Vision and Pattern Recognition*. (CVPR'11); 2011. pp. 529–534.

[32] Cao Q, Ying Y, and Li P. 'Similarity Metric Learning for Face Recognition'. *2013 IEEE International Conference on Computer Vision*; 2013. pp. 2408–2415.

[33] Sun Y, Wang X, and Tang X. 'Deep Learning Face Representation from Predicting 10,000 Classes'. *Proceedings of the 2014 IEEE Conference on Computer Vision and Pattern Recognition*. (CVPR'14). Washington, DC, USA: IEEE Computer Society; 2014. pp. 1891–1898. Available from: http://dx.doi.org/10.1109/CVPR.2014.244.

[34] Tehranipoor M, and Wang C. *Introduction to Hardware Security and Trust*. Springer-Verlag New York; 2011.

[35] Lumbiarres-Lopez R, Lopez-Garcia M, and Canto-Navarro E. 'Hardware architecture implemented on FPGA for protecting cryptographic keys against side-channel attacks'. *IEEE Transactions on Dependable and Secure Computing*. 2017;In Press(99):1–1. DOI: https://doi.org/10.1109/TDSC.2016.2610966

[36] Tehranipoor M, and Koushanfar F. 'A survey of hardware Trojan taxonomy and detection'. *IEEE Design Test of Computers*. 2010 January;27(1):10–25.

[37] Singer PW, and Friedman A. *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. Oxford University Press; UK, 2013.

[38] Lee N. *Counterterrorism and Cybersecurity: Total Information Awareness*. Springer International Publishing Switzerland; 2015.

[39] Islam R, Tian R, Batten LM, and Versteeg S. 'Classification of malware based on integrated static and dynamic features'. *Journal of Network and Computer Applications*. 2013;36(2):646–656. Available from: http://dx.doi.org/10.1016/j.jnca.2012.10.004.

[40] Menezes AJ, Vanstone SA, and Oorschot PCV. *Handbook of Applied Cryptography*. 1st ed. Boca Raton, FL: CRC Press, Inc.; 1996.

[41] Tilborg HCA, and Jajodia S. *Encyclopedia of Cryptography and Security*. 2nd ed. Springer US; 2011.

[42] Kim J, Hong S, and Lim J. 'Impossible differential cryptanalysis using matrix method'. *Discrete Mathematics*. 2010;310(5):988–1002. Available from: http://dx.doi.org/10.1016/j.disc.2009.10.019.

[43] Peeters E. *Side-Channel Cryptanalysis: A Brief Survey*. New York, NY: Springer New York; 2013. pp. 11–19. Available from: https://doi.org/10.1007/978-1-4614-6783-0_2.

[44] Zhu X, Ho ATS, and Marziliano P. 'A new semi-fragile image watermarking with robust tampering restoration using irregular sampling'. *Signal Processing: Image Communication*. 2007;22(5):515–528. Available from: http://dx.doi.org/10.1016/j.image.2007.03.004.

[45] Kee E, Johnson MK, and Farid H. 'Digital image authentication from JPEG headers'. *IEEE Transactions on Information Forensics and Security*. 2011 September;6(3):1066–1075.

[46] Lin X, and Li CT. 'Large-scale image clustering based on camera fingerprints'. *IEEE Transactions on Information Forensics and Security*. 2017 April;12(4):793–808.

[47] Armstrong BC, Ruiz-Blondet MV, Khalifian N, Kurtz KJ, Jin Z, and Laszlo S. 'Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics'. *Neurocomputing*. 2015;166:59–67. Available from: http://dx.doi.org/10.1016/j.neucom.2015.04.025.

[48] Logothetis NK, Pauls J, Augath M, Trinath T, and Oeltermann A. 'Neurophysiological investigation of the basis of the fMRI signal'. *Nature*. 2001;412(6843):150.

[49] Tadel F, Baillet S, Mosher JC, Pantazis D, and Leahy RM. 'Brainstorm: A user-friendly application for MEG/EEG analysis'. *Intell Neuroscience*. 2011;2011:8:1–8:13. Available from: http://dx.doi.org/10.1155/2011/879716.

[50] He C, and Wang J. 'An independent component analysis (ICA) based approach for EEG person authentication'. *2009 3rd International Conference on Bioinformatics and Biomedical Engineering*; 2009. pp. 1–4.

[51] Wang M, Abbass HA, and Hu J. 'Continuous authentication using EEG and face images for trusted autonomous systems'. *2016 14th Annual Conference on Privacy, Security and Trust (PST)*; 2016. pp. 368–375.

[52] Arias O, Wurm J, Hoang K, and Jin Y. 'Privacy and security in internet of things and wearable devices'. *IEEE Transactions on Multi-Scale Computing Systems*. 2015 April;1(2):99–109.

[53] Wilson DH, Atkeson C. Gellersen HW, Want R, and Schmidt A, editors. Simultaneous Tracking and Activity Recognition (STAR) Using Many Anonymous, Binary Sensors. Berlin, Heidelberg: Springer Berlin Heidelberg; 2005. pp. 62–79. Available from: https://doi.org/10.1007/11428572_5.

[54] Li N, Zhang N, Das SK, and Thuraisingham B. 'Privacy preservation in wireless sensor networks: A state-of-the-art survey'. *Ad Hoc Networks*. 2009;7(8): 1501–1514.

[55] Rakers P, Connell L, Collins T, and Russell D. 'Secure contactless smartcard ASIC with DPA protection'. *IEEE Journal of Solid-State Circuits*. 2001 March;36(3):559–565.

[56] Fathy A, Tarrad IF, Hamed HFA, and Awad AI. Advanced Encryption Standard Algorithm: Issues and Implementation Aspects. Hassanien AE, Salem ABM, Ramadan R, and Kim Th, editors. Advanced Machine Learning Technologies and Applications: First International Conference, AMLTA 2012, Cairo, Egypt, December 8–10, 2012. Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012. pp. 516–523. Available from: https://doi.org/10.1007/978-3-642-35326-0_51.

[57] Zhang J, and Qu G. 'A survey on security and trust of FPGA-based systems'. *2014 International Conference on Field-Programmable Technology (FPT)*; 2014. pp. 147–152.

[58] Elfatah AFA, Tarrad IF, Awad AI, and Hamed HFA. 'Optimized hardware implementation of the advanced encryption standard algorithm'. *2013 8th International Conference on Computer Engineering Systems (ICCES)*; 2013. pp. 197–201.