Security and Privacy



Maryam Mehrnezhad Thyla van der Merwe Chris Mitchell

Over the past two decades, a wide range of cyber security and privacy standards and regulations have been developed, covering a large number of application areas being both technical and business-oriented in nature. These standards and guidelines have been published by formal national and international standardization bodies and government agencies, as well as by industry consortia. Many of them are widely used, including the IETF standards that form the basis for the operation of the Internet; the ISO/IEC 27000 series of standards that has become the internationally adopted system for managing corporate information security; and the standards for mobile telephony published by the 3GPP that underlie all generations of mobile telephone networks. Despite their wide deployment, there will always be a need to revise existing standards and to develop new standards to cover new domains.

The purpose of this Special Issue on Security and Privacy in *IEEE Communications Standards Magazine* is to discuss the many challenges deriving from the study of existing standards, the revision of these standards, and the exploration of completely new areas of standardization. This issue has seven exciting and informative articles on a variety of topics including reviewing and assessing standards, and new frameworks and protocols for various applications such as 5G and IoT platforms.

In the article "Developing Maritime Digital Competencies" the author argues that there is a clear link between seafarer training and maritime safety. As such, there is a need to develop standardized digital competencies for all seafarers. The creation of these competencies needs to be considerate of company-specific and operation-specific risk management practices. This article presents one possible solution for the development of maritime digital competencies utilizing the well-established NIST Cybersecurity Framework.

Timestamping services are used to prove that a data item existed at a given point in time. This proof is represented by a timestamp token that is created by a timestamping authority. ISO/IEC 18014 specifies timestamping services and details how they should be implemented. In the article "Reviewing the ISO/IEC Standard for Timestamping Services" the authors review this standard, discover several issues, and provide a solution to each issue.

Confidentiality protections have become a major focus of standards development for the Domain Name System (DNS) protocol. DNS encryption techniques as well as alternative techniques with lower operational impact have both emerged. In the article "Standardizing Confidentiality Protections for Domain Name System Exchanges: Multiple Approaches, New Functionality" the author provides a high-level overview of these techniques and the considerations for applying them in various parts of the DNS ecosystem.

Secure bootstrapping of Internet of Things (IoT) devices is often a multi-step process that begins with enabling Internet access through a local wireless network. The process of enabling Internet access on IoT devices includes network discovery and selection, access authentication, and configuration of necessary credentials and parameters. On one hand, there are many standard protocols available for network access authentication of IoT devices. On the other hand, Extensible Authentication Protocol (EAP) is a standard framework with support for many authentication methods, and it is primarily used for network access authentication in enterprise networks. In the article "Secure Network Access Authentication for IoT Devices: EAP Framework vs. Individual Protocols" the authors discuss whether the EAP framework is beneficial for network access authentication of IoT devices.

From June 2019 to March 2020, the IETF conducted a selection process to choose password authenticated key exchange (PAKE) protocols for standardization. Similar standardization efforts were conducted before by IEEE (P1362.2) and ISO/IEC (11770-4). In the article "Prudent Practices in Security Standardization" the author reflects on the IETF PAKE selection process as a case study, and summarizes lessons in a set of principles with the hope of improving security standardization in the future.

With the popularization of the Internet of Things (IoT) in the home environment, security incidents have become more recurrent with end users. Knowledge sharing on incident mitigation with intrusion prevention systems (IPSs) can improve domestic IoT security, but both signature-based and anomaly-based approaches pose challenges of updating, portability, and privacy. In a previous work, the authors extended the RFC 8520 functionality and proposed the Intra-Network eXposure analyzer Utility (INXU) as a signature-based IPS to address these challenges. The INXU's architecture solves the

signature update problem, and its Malicious Traffic Description (MTD) data model solves the portability and privacy issues. However, the referred MTD data model is prone to high false-positive detection rates due to the lack of contextual information for identifying effective threats. In the article "Malicious Traffic Description: Toward a Data Model for Mitigating Security Threats to Home IoT" the authors propose an improvement to the MTD data model that reduces the false-positive detection rates.

Authentication and key management for applications (AKMA) is the new cellular-network-based delegated authentication system of 5G. In the article "AKMA: Delegated Authentication System of 5G" the authors explain what a delegated authentication system is and how it relates to concepts like federated identity management. They also explain why a cellular-network-based delegated authentication system is more secure than a password-based delegated authentication system.

Biographies

Maryam Mehrnezhad is a Research Fellow in cybersecurity and privacy, Newcastle University (NU), UK. She received her Ph.D. in security and privacy of sensing technologies from NU in 2017. She works on inter/multi-disciplinary research topics resulting in several papers with industrial impact. She has a special interest in standardization research, serving as a W3C invited expert. She has won national and international prizes for her research, including the Economist and Kaspersky cybersecurity award on using Blockchain for end-to-end verifiable e-voting and the best Ph.D. research award at Academic Centre of Excellence in Cyber Security Research (ACE-CSR) in 2016.

Thyla van der Merwe is the Managing Director of the ETH Future Computing Laboratory, an industry-funded research center focused on the development of next-generation technologies in the fields of computer engineering and computer science. She received her Ph.D. in cyber security from Royal Holloway, University of London. Her research focuses on the security of network protocols, and in 2018 she won the EPSRC Connected Nations award (Safe and Secure Cyber Society category) for her work on the Transport Layer Security (TLS) protocol. Prior to starting at ETH Zurich, she was the Security Engineering Manager at Mozilla, where her team was responsible for developing and maintaining the cryptographic libraries that power the Firefox browser. She served on the ISO/IEC committee responsible for standardizing cryptographic mechanisms and protocols for several years, and has extensive experience working on academia-industry collaborations.

Chris Mitchell has worked in cryptography and security for well over 40 years, and has been actively involved in security standardization for nearly 35 years, during which time he has edited over 20 ISO/IEC standards. He has been a full professor at Royal Holloway since 1990, where he co-founded the Information Security Group and for which he is currently serving as Head of Department. He has published over 250 articles in refereed conference proceedings and journals, and supervised over 30 Ph.D. students to completion. He is a Senior Member of the IEEE.