Protocols For Authentication And Key Establishment

The second International Conference on Applied Cryptography and Network Security (ACNS 2004) was sponsored and organized by ICISA (the International Communications and Information Security Association). It was held in Yellow Mountain, China, June 8–11, 2004. The conference proceedings, representing papers from the academic track, are published in this volume of the Lecture Notes in Computer Science (LNCS) of Springer-Verlag. The area of research that ACNS covers has been gaining importance in recent years due to the development of the Internet, which, in turn, implies global exposure of computing resources. Many ?elds of research were covered by the program of this track, presented in this proceedings volume. We feel that the papers herein indeed re?ect the state of the art in security and cryptography research, worldwide. The program committee of the conference received a total of 297 submissions from all over the world, of which 36 submissions were selected for presentation during the academic track. In addition to this track, the conference also hosted a technical/industrial track of presentations that were carefully selected as well. All submissions were reviewed by experts in the relevant areas.
We have telephony to talk to each other, messaging to dispatch mail or instant messages, browsing to read published content and search engines to locate content sites. However, current mobile networks do not provide the possibility for one application rich terminal to communicate with another in a peer-to-peer session beyond voice calls. Mobile telephony with the current technology has been hugely successful and shows that there is immense value in communicating with peers while being mobile, and with increasingly available smarter multimedia terminals the communication experience will be something more than just exchanging voice. Those multimedia terminals need IP multimedia networks. Hence, the Third Generation Partnership Project (3GPP) has developed a standard for SIP based IP multimedia service machinery known as 'The IMS (IP Multimedia Subsystem)' and this informative book explains everything you need to know about it..... Presents the architecture and functionality of logical elements of IMS and their interfaces providing detailed description of how elements are connected, what protocols are used and how they are used Explains how the optimisation and security of the mobile communication environment has been designed in the form of user authentication and authorisation based on mobile identities Illustrates how optimisation at the radio interface is achieved using specific rules at the user to network interface. This includes signalling compression mechanisms as well as security and policy control mechanisms, allowing radio loss and recovery detection Addresses important aspects from an operator's point of view while developing architecture such as charging framework, policy and service control Describes many services on top of IMS in detail, including voice, presence, messaging and conferencing. Written in a manner that allows readers to choose the level of knowledge and understanding they need to gain about the IMS, this volume will have instant appeal to a wide audience ranging from marketing managers, research and development engineers, network engineers, developers, test engineers to university students.
Annotation. This volume constitutes the refereed proceedings of the 24th International Workshop on Computer Science Logic, CSL 2010, held in Brno, Czech Republic, in August 2010. The 33 full papers presented together with 7 invited talks, were carefully reviewed and selected from 103 submissions. Topics covered include automated deduction and interactive theorem proving, constructive mathematics and type theory, equational logic and term rewriting, automata and games, modal and temporal logic, model checking, decision procedures, logical aspects of computational complexity, finite model theory, computational proof theory, logic programming and constraints, lambda calculus and combinatory logic, categorical logic and topological semantics, domain theory, database theory, specification, extraction and transformation of programs, logical foundations of programming paradigms, verification and program analysis, linear logic, higher-order logic, and nonmonotonic reasoning.
The purpose of designing this book is to discuss and analyze security protocols available for communication. Objective is to discuss protocols across all layers of TCP/IP stack and also to discuss protocols independent to the stack. Authors will be aiming to identify the best set of security protocols for the similar applications and will also be identifying the drawbacks of existing protocols. The authors will be also suggesting new protocols if any.
Implement end-to-end and gateway security for IP networks. "Internet Security Protocols: Protecting IP Traffic" is a complete networking professional's guide to providing end-to-end and gateway Internet security for the user's information. World-renowned consultant Uyless Black covers the essential Internet security protocols designed to protect IP traffic. The book's coverage includes: Key Internet security challenges: privacy, secrecy, confidentiality, integrity of information, authentication, access control, non-repudiation, denial of service attacks Dial-in authentication with CHAP, RADIUS, and DIAMETER The role of IPSec in acquiring privacy and authentication services The Internet Key Distribution, Certification, and Management Systems (ISAKMP and IKE) Security in mobile Internet applications From the basics of firewalls to the latest public key distribution systems, Uyless Black reviews the alternatives for securing Internet traffic. If you're responsible for securing information traveling on IP networks, "Internet Security Protocols" is a fine source for the authoritative answers you're looking for.
The LNCS journal Transactions on Computational Science reflects recent developments in the field of Computational Science, conceiving the field not as a mere ancillary science but rather as an innovative approach supporting many other scientific disciplines. The journal focuses on original high-quality research in the realm of computational science in parallel and distributed environments, encompassing the facilitating theoretical foundations and the applications of large-scale computations and massive data processing. It addresses researchers and practitioners in areas ranging from aerospace to biochemistry, from electronics to geosciences, from mathematics to software architecture, presenting verifiable computational methods, findings, and solutions and enabling industrial users to apply techniques of leading-edge, large-scale, high performance computational methods. The 17th issue of the Transactions on Computational Science journal consists of two parts. The first part is comprised of four papers, spanning the areas of robotics and augmented reality, computer game evaluation strategies, cognitive perception in crowd control simulation, and reversible processor design using look-ahead. The second part consists of five papers covering the topics of secure congestion adaptive routing, cryptographic schemes for wireless sensor networks, intersection attacks on anonymity, and reliable message delivery in Vehicular Ad Hoc Networks (VANET).
The CRYPTO ’93 conference was sponsored by the International Association for Cryptologic Research (IACR) and Bell-Northern Research (a subsidiary of Northern Telecom), in co-operation with the IEEE Computer Society Technical Committee. It took place at the University of California, Santa Barbara, from August 22-26, 1993. This was the thirteenth annual CRYPTO conference, all of which have been held at UCSB. The conference was very enjoyable and ran very of the General Chair, Paul Van Oorschot. smoothly, largely due to the efforts It was a pleasure working with Paul throughout the months leading up to the conference. There were 136 submitted papers which were considered by the Program Committee. Of these, 38 were selected for presentation at the conference. There was also one invited talk at the conference, presented by Miles Smid, the title of which was “A Status Report On the Federal Government Key Escrow System.” The conference also included the customary Rump Session, which was presided over by Whit Diffie in his usual inimitable fashion. Thanks again to Whit for organizing and running the Rump session. This year, the Rump Session included an interesting and lively panel discussion on issues pertaining to key escrowing. Those taking part were W. Diffie, J. Gilmore, S. Goldwasser, M. Hellman, A. Herzberg, S. Micali, R. Rueppel, G. Simmons and D. Weitzner.
"Cryptographic Protocol: Security Analysis Based on Trusted Freshness" mainly discusses how to analyze and design cryptographic protocols based on the idea of system engineering and that of the trusted freshness component. A novel freshness principle based on the trusted freshness component is presented; this principle is the basis for an efficient and easy method for analyzing the security of cryptographic protocols. The reasoning results of the new approach, when compared with the security

conditions, can either establish the correctness of a cryptographic protocol when the protocol is in fact correct, or identify the absence of the security properties, which leads the structure to construct attacks directly. Furthermore, based on the freshness principle, a belief multiset formalism is presented. This formalism’s efficiency, rigorousness, and the possibility of its automation are also presented. The book is intended for researchers, engineers, and graduate students in the fields of communication, computer science and cryptography, and will be especially useful for engineers who need to analyze cryptographic protocols in the real world. Dr. Ling Dong is a senior engineer in the network construction and information security field. Dr. Kefei Chen is a Professor at the Department of Computer Science and Engineering, Shanghai Jiao Tong University.

This book constitutes the refereed proceedings of the 23rd Annual International Cryptology Conference, CRYPTO 2003, held in Santa Barbara, California in August 2003. The 34 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 166 submissions. The papers are organized in topical sections on public key cryptanalysis, alternate adversary models, protocols, symmetric key cryptanalysis, universal composability, zero knowledge, algebraic geometry, public key constructions, new problems, symmetric key constructions, and new models.

This book constitutes the refereed proceedings of the 7th International Conference on Cloud Computing, Security, Privacy in New Computing Environments, CloudComp 2016, and the First EAI International Conference SPNCE 2016, both held in Guangzhou, China, in November and December 2016.The proceedings contain 10 full papers selected from 27 submissions and presented at CloudComp 2016 and 12 full papers selected from 69 submissions and presented at SPNCE 2016. CloudComp 2016 presents recent advances and experiences in clouds, cloud computing and related ecosystems and business support. SPNCE 2016 focuses on security and privacy aspects of new computing environments including mobile computing, big data, cloud computing and other large-scale environments.

An introduction to CSP - Modelling security protocols in CSP - Expressing protocol goals - Overview of FDR - Casper - Encoding protocols and intruders for FDR - Theorem proving - Simplifying transformations - Other approaches - Prospects and wider issues.

Managing Information Technology Resources in Organizations in the Next Millennium contains more than 200 unique perspectives on numerous timely issues of managing information technology in organizations around the world. This book, featuring the latest research and applied IT practices, is a valuable source in support of teaching and research agendas.

AAA (Authentication, Authorization, Accounting) describes a framework for intelligently controlling access to network resources, enforcing policies, and providing the information necessary to bill for services. AAA and Network Security for Mobile Access is an invaluable guide to the AAA concepts and framework, including its protocols Diameter and Radius. The authors give an overview of established and emerging standards for the provision of secure network access for mobile users while providing the basic design concepts and motivations. AAA and Network Security for Mobile Access: Covers trust, i.e., authentication and security key management for fixed and mobile users, and various approaches to trust establishment. Discusses public key infrastructures and provides practical tips on certificates management. Introduces Diameter, a state-of-the-art AAA protocol designed to meet today’s reliability, security and robustness requirements, and examines Diameter-Mobile IP interactions. Explains RADIUS (Remote Authentication Dial-In User Services) and its latest extensions. Details EAP (Extensible Authentication Protocol) in-depth, giving a protocol overview, and covering EAP-XXX authentication methods as well as use of EAP in 802 networks. Describes IP mobility protocols including IP level mobility management, its security and optimizations, and latest IETF seamless mobility protocols. Includes a chapter describing the details of Mobile IP and AAA interaction, illustrating Diameter Mobile IP applications and the process used in CDMA2000. Contains a section on security and AAA issues to support roaming, discussing a variety of options for operator co-existence, including an overview of Liberty Alliance. This text will provide researchers in academia and industry, network security engineers, managers, developers and planners, as well as graduate students, with an accessible explanation of the standards fundamental to secure mobile access.

The four volume set assembled following The 2005 International Conference on Computational Science and its Applications, ICCSA 2005, held in Suntec International Convention and Exhibition Centre, Singapore, from 9 May 2005 till 12 May 2005, represents the ?ne collection of 540 refereed papers selected from nearly 2,700 submissions. Computational Science has ?rmly established itself as a vital part of many scienti?c investigations, a?ecting researchers and practitioners in areas ranging from applications such as aerospace and automotive, to emerging technologies such as bioinformatics and nanotechnologies, to core disciplines such as ma- ematics, physics, and chemistry. Due to the shear size of many challenges in computational science, the use of supercomputing, parallel processing, and - phisticated algorithms is inevitable and becomes a part of fundamental t- oretical research as well as endeavors in emerging ?elds. Together, these far reaching scienti?c areas contribute to shape this Conference in the realms of state-of-the-art computational science research and applications, encompassing the facilitating theoretical foundations and the innovative applications of such results in other areas.

This book constitutes the refereed proceedings of the 9th IMA International Conference on Cryptography and Coding, held in Cirencester, UK in December 2003. The 25 revised full papers presented together with 4 invited contributions were carefully reviewed and selected from 49 submissions. The papers are organized in topical sections on coding and applications, applications of coding in cryptography, cryptography, cryptanalysis, network security and protocols.

An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

This book constitutes the thoroughly refereed post-proceedings of the Third International Conference on Security in Communication Networks, SCN 2002, held in Amalfi, Italy in September 2002. The 24 revised full papers presented together with two invited papers were

carefully selected from 90 submissions during two rounds of reviewing and revision. The papers are organized in topical sections on forward security, foundations of cryptography, key management, cryptanalysis, systems security, digital signature schemes, zero knowledge, and information theory and secret sharing.

Please note that the content of this book primarily consists of articles available from Wikipedia or other free sources online. Pages: 121. Chapters: Diffie-Hellman key exchange, Secure Shell, HTTP Secure, Dining cryptographers protocol, IPsec, Chaffing and winnowing, Electronic money, Key-agreement protocol, Transport Layer Security, X.509, Zero-knowledge proof, DomainKeys Identified Mail, Digital credential, Wired Equivalent Privacy, Digest access authentication, Secret sharing, Internet Key Exchange, BitTorrent protocol encryption, Wi-Fi Protected Access, 3-D Secure, Oblivious transfer, Publius Publishing System, SSH File Transfer Protocol, Secure Remote Password protocol, Secure multi-party computation, Kerberized Internet Negotiation of Keys, Off-the-Record Messaging, Needham-Schroeder protocol, Temporal Key Integrity Protocol, Station-to-Station protocol, Hashcash, Online Certificate Status Protocol, ZRTP, Secure Communications Interoperability Protocol, WLAN Authentication and Privacy Infrastructure, Proof of knowledge, IEEE 802.11i-2004, ANSI ASC X9.95 Standard, Socialist millionaire, Alice and Bob, Secure Real-time Transport Protocol, Yao's Millionaires' Problem, Diffie-Hellman problem, Interlock protocol, Password-authenticated key agreement, Universal composability, Non-interactive zero-knowledge proof, Wi-Fi Protected Setup, HTTPsec, Certificate signing request, Private information retrieval, Password Authenticated Key Exchange by Juggling, StrongSwan, High Assurance Internet Protocol Encryptor, Homomorphic secret sharing, SPNEGO, Proactive secret sharing, Simple Authentication and Security Layer, Secure channel, AS2, Generic Bootstrapping Architecture, Group Domain of Interpretation, Certificate Management Protocol, Code Access Security, SPEKE, Secure copy, Web-based SSH, Certification path validation algorithm, CAVE-based authentication, Wireless Transport Layer Security, Cipher suite, Neuman-Stubblebine protocol, Cryptographic protocol, Vouch...

Helping current and future system designers take a more productive approach in the field, Communication System Security shows how to apply security principles to state-of-the-art communication systems. The authors use previous design failures and security flaws to explain common pitfalls in security design. Divided into four parts, the book begins with the necessary background on practical cryptography primitives. This part describes pseudorandom sequence generators, stream and block ciphers, hash functions, and public-key cryptographic algorithms. The second part covers security infrastructure support and the main subroutine designs for establishing protected communications. The authors illustrate design principles through network security protocols, including transport layer security (TLS), Internet security protocols (IPsec), the secure shell (SSH), and cellular solutions. Taking an evolutionary approach to security in today’s telecommunication networks, the third part discusses general access authentication protocols, the protocols used for UMTS/LTE, the protocols specified in IETF, and the wireless-specific protection mechanisms for the air link of UMTS/LTE and IEEE 802.11. It also covers key establishment and authentication in broadcast and multicast scenarios. Moving on to system security, the last part introduces the principles and practice of a trusted platform for communication devices. The authors detail physical-layer security as well as spread-spectrum techniques for anti-jamming attacks. With much of the material used by the authors in their courses and drawn from their industry experiences, this book is appropriate for a wide audience, from engineering, computer science, and mathematics students to engineers, designers, and computer scientists. Illustrating security principles with existing protocols, the text helps readers understand the principles and practice of security analysis.

Protocols for Authentication and Key EstablishmentSpringer Science & Business Media

Intelligent computing refers greatly to artificial intelligence with the aim at making computer to act as a human. This newly developed area of real-time intelligent computing integrates the aspect of dynamic environments with the human intelligence. This book presents a comprehensive practical and easy to read account which describes current state-of-the art in designing and implementing real-time intelligent computing to robotics, alert systems, IoT, remote access control, multi-agent systems, networking, mobile smart systems, crowd sourcing, broadband systems, cloud computing, streaming data and many other applications areas. The solutions discussed in this book will encourage the researchers and IT professional to put the methods into their practice.

This book constitutes the thoroughly refereed post-conference proceedings of the 12th International Conference on Information Security and Cryptology, Inscrypt 2016, held in Beijing, China, in November 2016. The 32 revised full papers presented were carefully reviewed and selected from 93 submissions. The papers are organized in topical sections on symmetric ciphers; public-key cryptosystems; signature and authentication; homomorphic encryption; leakage-resilient; post-quantum cryptography; commitment and protocol; elliptic curves; security and implementation.

This book provides a concise yet comprehensive overview of computer and Internet security, suitable for a one-term introductory course for junior/senior undergrad or first-year graduate students. It is also suitable for self-study by anyone seeking a solid footing in security – including software developers and computing professionals, technical managers and government staff. An overriding focus is on brevity, without sacrificing breadth of core topics or technical detail within them. The aim is to enable a broad understanding in roughly 350 pages. Further prioritization is supported by designating as optional selected content within this. Fundamental academic concepts are reinforced by specifics and examples, and related to applied problems and real-world incidents. The first chapter provides a gentle overview and 20 design principles for security. The ten chapters that follow provide a framework for understanding computer and Internet security. They regularly refer back to the principles, with supporting examples. These principles are the conceptual counterparts of security-related error patterns that have been recurring in software and system designs for over 50 years. The book is “elementary” in that it assumes no background in security, but unlike “soft” high-level texts it does not avoid low-level details, instead it selectively dives into fine points for exemplary topics to concretely illustrate concepts and principles. The book is rigorous in the sense of being technically sound, but avoids both mathematical proofs and lengthy source-code examples that typically make books inaccessible to general audiences. Knowledge of elementary operating system and networking concepts is helpful, but review sections summarize the essential background. For graduate students, inline exercises and supplemental references provided in per-chapter endnotes provide a bridge to further topics and a springboard to the research literature; for those in industry and government, pointers are provided to helpful surveys and relevant standards, e.g., documents from the Internet Engineering Task Force (IETF), and the U.S. National Institute of Standards and Technology.

This book is an introduction to fundamental concepts in the fields of cryptography and network security. Because cryptography is highly vulnerable to program errors, a simple testing of the cryptosystem will usually uncover a security vulnerability. In this book the author takes the reader through all of the important design and implementation details of various cryptographic algorithms and network security protocols to enforce network security. The book is divided into four parts: Cryptography, Security Systems, Network Security Applications, and System Security. Numerous diagrams and examples throughout the book are used to explain cryptography and network security concepts. FEATURES: Covers key concepts related to cryptography and network security Includes chapters on modern symmetric key block cipher algorithms, information security, message integrity, authentication, digital signature, key management, intruder detection, network layer security, data link layer security, NSM, firewall design, and more.

This book constitutes the thoroughly refereed post-proceedings of the 16th International Workshop on Security Protocols, SP

2008, held in Cambridge, UK, in April 2008. The 17 revised full papers presented together with edited transcriptions of some of the discussions following the presentations have gone through multiple rounds of reviewing, revision, and selection. The theme of this workshop was “Remodelling the Attacker” with the intention to tell the students at the start of a security course that it is very important to model the attacker, but like most advice to the young, this is an oversimplification. Shouldn’t the attacker’s capability be an output of the design process as well as an input? The papers and discussions in this volume examine the theme from the standpoint of various different applications and adversaries.

This book is the most comprehensive and integrated treatment of the protocols required for authentication and key establishment. In a clear, uniform presentation the authors classify most protocols in terms of their properties and resource requirements, and describe all the main attack types, so the reader can quickly evaluate protocols for particular applications. In this edition the authors introduced new chapters and updated the text throughout in response to new developments and updated standards. The first chapter, an introduction to authentication and key establishment, provides the necessary background on cryptography, attack scenarios, and protocol goals. A new chapter, computational security models, describes computational models for key exchange and authentication and will help readers understand what a computational proof provides and how to compare the different computational models in use. In the subsequent chapters the authors explain protocols that use shared key cryptography, authentication and key transport using public key cryptography, key agreement protocols, the Transport Layer Security protocol, identity-based key agreement, password-based protocols, and group key establishment. The book is a suitable graduate-level introduction, and a reference and overview for researchers and practitioners with 225 concrete protocols described. In the appendices the authors list and summarize the relevant standards, linking them to the main book text when appropriate, and they offer a short tutorial on how to build a key establishment protocol. The book also includes a list of protocols, a list of attacks, a summary of the notation used in the book, general and protocol indexes, and an extensive bibliography.

Your expert guide to information security As businesses and consumers become more dependent on complexmultinational information systems, the need to understand anddevise sound information security systems has never been greater.This title takes a practical approach to information security byfocusing on real-world examples. While not sidestepping the theory,the emphasis is on developing the skills and knowledge thatsecurity and information technology students and professionals needto face their challenges. The book is organized around four majorthemes: * Cryptography: classic cryptosystems, symmetric key cryptography,public key cryptography, hash functions, random numbers,information hiding, and cryptanalysis * Access control: authentication and authorization, password-basedsecurity, ACLs and capabilities, multilevel and multilateralsecurity, covert channels and inference control, BLP and Biba'smodels, firewalls, and intrusion detection systems * Protocols: simple authentication protocols, session keys, perfectforward secrecy, timestamps, SSL, IPSec, Kerberos, and GSM * Software: flaws and malware, buffer overflows, viruses and worms,software reverse engineering, digital rights management, securesoftware development, and operating systems security Additional features include numerous figures and tables toillustrate and clarify complex topics, as well as problems-rangingfrom basic to challenging-to help readers apply their newlydeveloped skills. A solutions manual and a set of classroom-testedPowerPoint(r) slides will assist instructors in their coursedevelopment. Students and professors in information technology,computer science, and engineering, and professionals working in thefield will find this reference most useful to solve theirinformation security issues. An Instructor's Manual presenting detailed solutions to all theproblems in the book is available from the Wiley editorialdepartment. An Instructor Support FTP site is also available.

Table of contents

Provides information on the features, functions, and implementation of Active Directory, covering such topics as management tools, searching the AD database, and the Kerberos security protocol.

This book constitutes the proceedings of the 15th IFIP TC8 International Conference on Computer Information Systems and Industrial Management, CISIM 2016, held in Vilnius, Lithuania, in September 2016. The 63 regular papers presented together with 1 inivted paper and 5 keynotes in this volume were carefully reviewed and selected from about 89 submissions. The main topics covered are rough set methods for big data analytics; images, visualization, classification; optimization, tuning; scheduling in manufacturing and other applications; algorithms; decisions; intelligent distributed systems; and biometrics, identification, security.

Expanded into two volumes, the Second Edition of Springer’s Encyclopedia of Cryptography and Security brings the latest and most comprehensive coverage of the topic: Definitive information on cryptography and information security from highly regarded researchers Effective tool for professionals in many fields and researchers of all levels Extensive resource with more than 700 contributions in Second Edition 5643 references, more than twice the number of references that appear in the First Edition With over 300 new entries, appearing in an A-Z format, the Encyclopedia of Cryptography and Security provides easy, intuitive access to information on all aspects of cryptography and security. As a critical enhancement to the First Edition’s base of 464 entries, the information in the Encyclopedia is relevant for researchers and professionals alike. Topics for this comprehensive reference were elected, written, and peer-reviewed by a pool of distinguished researchers in the field. The Second Edition’s editorial board now includes 34 scholars, which was expanded from 18 members in the First Edition. Representing the work of researchers from over 30 countries, the Encyclopedia is broad in scope, covering everything from authentication and identification to quantum cryptography and web security. The text’s practical style is instructional, yet fosters investigation. Each area presents concepts, designs, and specific implementations. The highly-structured essays in this work include synonyms, a definition and discussion of the topic, bibliographies, and links to related literature. Extensive cross-references to other entries within the Encyclopedia support efficient, user-friendly searches for immediate access to relevant information. Key concepts presented in the Encyclopedia of Cryptography and Security include: Authentication and identification; Block ciphers and stream ciphers; Computational issues; Copy protection; Cryptanalysis and security; Cryptographic protocols; Electronic payment and digital certificates; Elliptic curve cryptography; Factorization algorithms and primality tests; Hash functions and MACs; Historical systems; Identity-based cryptography; Implementation aspects for smart cards and standards; Key management; Multiparty computations like voting schemes; Public key cryptography; Quantum cryptography; Secret sharing schemes; Sequences; Web Security. Topics covered: Data Structures, Cryptography and Information Theory; Data Encryption; Coding and Information Theory; Appl.Mathematics/Computational Methods of Engineering; Applications of Mathematics; Complexity. This authoritative reference will be published in two formats: print and online. The online edition features hyperlinks to cross-references, in addition to significant research.

This thesis includes my research on efficient cryptographic protocols, sensor network key management, and radio frequency identification (RFID) authentication protocols. Key exchange, identification, and public key encryption are among the fundamental protocols studied in cryptography. There are two important requirements for these protocols: efficiency and security. Efficiency is evaluated using the computational overhead to execute a protocol. In modern cryptography, one way to ensure the security of a protocol is by means of provable security. Provable security consists of a security model that specifies the capabilities and the goals of an adversary against the protocol, one

or more cryptographic assumptions, and a reduction showing that breaking the protocol within the security model leads to breaking the assumptions. Often, efficiency and provable security are not easy to achieve simultaneously. The design of efficient protocols in a strict security model with a tight reduction is challenging. Security requirements raised by emerging applications bring up new research challenges in cryptography. One such application is pervasive communication and computation systems, including sensor networks and radio frequency identification (RFID) systems. Specifically, sensor network key management and RFID authentication protocols have drawn much attention in recent years.

How prepared are you to build fast and efficient web applications? This eloquent book provides what every web developer should know about the network, from fundamental limitations that affect performance to major innovations for building even more powerful browser applications—including HTTP 2.0 and XHR improvements, Server-Sent Events (SSE), WebSocket, and WebRTC. Author Ilya Grigorik, a web performance engineer at Google, demonstrates performance optimization best practices for TCP, UDP, and TLS protocols, and explains unique wireless and mobile network optimization requirements. You'll then dive into performance characteristics of technologies such as HTTP 2.0, client-side network scripting with XHR, real-time streaming with SSE and WebSocket, and P2P communication with WebRTC. Deliver superlative TCP, UDP, and TLS performance Speed up network performance over 3G/4G mobile networks Develop fast and energy-efficient mobile applications Address bottlenecks in HTTP 1.x and other browser protocols Plan for and deliver the best HTTP 2.0 performance Enable efficient real-time streaming in the browser Create efficient peer-to-peer videoconferencing and low-latency applications with real-time WebRTC transports

With the scope and frequency of attacks on valuable corporate data growing enormously in recent years, a solid understanding of cryptography is essential for anyone working in the computer/network security field. This timely book delivers the hands-on knowledge you need, offering comprehensive coverage on the latest and most-important standardized cryptographic techniques to help you protect your data and computing resources to the fullest. Rather than focusing on theory like other books on the market, this unique resource describes cryptography from an end-user perspective, presenting in-depth, highly practical comparisons of standards and techniques.

Protocols for authentication and key establishment are the foundation for security of communications. The range and diversity of these protocols is immense, while the properties and vulnerabilities of different protocols can vary greatly. This is the first comprehensive and integrated treatment of these protocols. It allows researchers and practitioners to quickly access a protocol for their needs and become aware of existing protocols which have been broken in the literature. As well as a clear and uniform presentation of the protocols this book includes a description of all the main attack types and classifies most protocols in terms of their properties and resource requirements. It also includes tutorial material suitable for graduate students.