
Acsac

Advancing Embedded Systems and Real-Time Communications with Emerging Technologies

The Hospitaller Knights of Saint John, 1523-1565

Detection of Intrusions and Malware, and Vulnerability Assessment

Security Engineering

16th Annual Computer Security Applications Conference (ACSAC '00)

Electronic Healthcare Information Security

Online Harassment

Advances in Computer Systems Architecture

Department of Defense Appropriations for ...

Secure Data Management

Computational Intelligence in Security for Information Systems

Computer Security -- ESORICS 2015

Building Secure Defenses Against Code-Reuse Attacks

Entity-Relationship Approach - ER '93

Telecommunications, Command and Control Programs

Advances in Computer Systems Architecture

Department of Defense Appropriations for 1980: Telecommunications, command and control programs. Research, development, test and evaluation

The Department of the Army Manual

Department of the Army

Network and System Security

Army

Advances in Swarm and Computational Intelligence

High Performance Cloud Auditing and Applications

Cyberspace Safety and Security

Recent Advances in Intrusion Detection

Research in Attacks, Intrusions, and Defenses
Proceedings of the 34th Annual Computer Security Applications Conference
Department of the Army Historical Summary
Department of Defense Appropriations for 1981: Operation and maintenance, Air Force
Recent Advances in Intrusion Detection
Advances in Computer Systems Architecture
Mobile Platform Security
Research in Attacks, Intrusions, and Defenses
Proceedings of the First International Conference on Computational Intelligence and Informatics
Signals
Computer Security Applications Conference (Acsac 98) 14th Annual
Security and Privacy in Communication Networks
Department of Defense appropriations for 1980
Emerging IT/ICT and AI Technologies Affecting Society
Department of Defense Sponsored Information Security Research

Acsac

Downloaded from <ftp.wtvq.com> by guest

ROSA ESTHER

Advancing Embedded Systems and Real-Time Communications with Emerging Technologies Springer

Nature

This book constitutes the refereed proceedings of the 4th International Symposium on Cyberspace Safety and Security (CSS 2012), held in Melbourne, Australia, in December 2012. The 30 revised full papers presented together with 7 invited talks were carefully reviewed and selected from 105 submissions. The papers cover the following topics: mobile security, cyberspace attacks and defense, security application and systems, network

and cloud security, wireless security, security protocols and models.

The Hospitaller Knights of Saint John, 1523-1565 Springer Science & Business Media

Covers the Hospitaller Knights' relocation to Malta, their operations, and the Great Siege of 1565. The sequel to The Hospitaller Knights of Saint John at Rhodes 1306-1522, this volume covers the period 1523-1565. This volume opens with the relocation from Rhodes to Malta during the years following the Order's heart-rending loss of Rhodes to Ottoman Sultan Suleiman. This loss was also that of 4,000 non-belligerent Christians choosing to abandon their homes and livelihoods and to accompany the Order in its search for a new home. Volume II

further deals with the first thirty-five years of Hospitaller residence at Malta including operations from there along the coast of North Africa, with major sieges of Tripoli, Tunis, and Algiers, with penetrating exposés of corsair admirals such as Kheir-ed-Din Barbarossa and Dragut, and with giants of Christian history such as Andrea Doria. Finally, this volume deals with the Ottoman Empire's 1565 attempt to eradicate the Order with that year's Great Siege of Malta. The author draws on the work of the Order's official historians, Giacomo Bosio and his successor Bartolomeo dal Pozzo. He transcribes their writings for the modern reader, while also presenting new information revealed in the 400 years of scholarship since Bosio's death in 1627. While initial chapters focus on Philippe Villiers de l'Isle-Adam, 44th Grand Master of the Hospitaller Knights of Saint John, this history also brings to light the contributions of properly identified lieutenants, allies and opponents. This volume is believed to be the only continuous history since Bosio of the Hospitallers during the period 1523 through 1565, and is certainly the only such history in English.

Detection of Intrusions and Malware, and Vulnerability Assessment Springer

This book provides an in-depth look at return-oriented programming attacks. It explores several conventional return-oriented programming attacks and analyzes the effectiveness of defense techniques including address space layout randomization (ASLR) and the control-flow restrictions implemented in security watchdogs such as Microsoft EMET. Chapters also explain the principle of control-flow integrity (CFI), highlight the benefits of CFI and discuss its current weaknesses. Several improved and

sophisticated return-oriented programming attack techniques such as just-in-time return-oriented programming are presented. Building Secure Defenses against Code-Reuse Attacks is an excellent reference tool for researchers, programmers and professionals working in the security field. It provides advanced-level students studying computer science with a comprehensive overview and clear understanding of important runtime attacks.

Security Engineering Springer Science & Business Media
This book mainly focuses on cloud security and high performance computing for cloud auditing. The book discusses emerging challenges and techniques developed for high performance semantic cloud auditing, and presents the state of the art in cloud auditing, computing and security techniques with focus on technical aspects and feasibility of auditing issues in federated cloud computing environments. In summer 2011, the United States Air Force Research Laboratory (AFRL) CyberBAT Cloud Security and Auditing Team initiated the exploration of the cloud security challenges and future cloud auditing research directions that are covered in this book. This work was supported by the United States government funds from the Air Force Office of Scientific Research (AFOSR), the AFOSR Summer Faculty Fellowship Program (SFFP), the Air Force Research Laboratory (AFRL) Visiting Faculty Research Program (VFRP), the National Science Foundation (NSF) and the National Institute of Health (NIH). All chapters were partially supported by the AFOSR Information Operations and Security Program extramural and intramural funds (AFOSR/RSL Program Manager: Dr. Robert Herklotz). Key Features: · Contains surveys of cyber threats and security issues in cloud computing and presents secure cloud

architectures · Presents in-depth cloud auditing techniques, federated cloud security architectures, cloud access control models, and access assured information sharing technologies · Outlines a wide range of challenges and provides solutions to manage and control very large and complex data sets

16th Annual Computer Security Applications Conference (ACSAC '00) Springer

This book constitutes the refereed proceedings of the 12th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2015, held in Milan, Italy, in July 2015. The 17 revised full papers presented were carefully reviewed and selected from 75 submissions. The papers are organized in topical sections on attacks, attack detection, binary analysis and mobile malware protection, social networks and large-scale attacks, Web and mobile security, and provenance and data sharing.

Electronic Healthcare Information Security Springer

This volume constitutes the thoroughly refereed post-conference proceedings of the 11th International Conference on Security and Privacy in Communication Networks, SecureComm 2015, held in Dallas, TX, USA, in October 2015. The 29 regular and 10 poster papers presented were carefully reviewed and selected from 107 submissions. It also presents 9 papers accepted of the workshop on Applications and Techniques in Cyber Security, ATCS 2015. The papers are grouped in the following topics: mobile, system, and software security; cloud security; privacy and side channels; Web and network security; crypto, protocol, and model.

Online Harassment Springer

The book covers a variety of topics which include data mining

and data warehousing, high performance computing, parallel and distributed computing, computational intelligence, soft computing, big data, cloud computing, grid computing, cognitive computing, image processing, computer networks, wireless networks, social networks, wireless sensor networks, information and network security, web security, internet of things, bioinformatics and geoinformatics. The book is a collection of best papers submitted in the First International Conference on Computational Intelligence and Informatics (ICCI 2016) held during 28-30 May 2016 at JNTUH CEH, Hyderabad, India. It was hosted by Department of Computer Science and Engineering, JNTUH College of Engineering in association with Division V (Education & Research) CSI, India.

Advances in Computer Systems Architecture Springer
Nature

This book constitutes the refereed proceedings of the 4th International Conference on Computational Intelligence in Security for Information Systems, CISIS 2011, held in Torremolinos-Málaga, in June 2011 as a satellite event of IWANN 2011, the International Work-conference on Artificial and Natural Neural Networks. The 38 revised full papers presented were carefully reviewed and selected from a total of 70 submissions. The papers are organized in topical sections on machine learning and intelligence, network security, cryptography, securing software, and applications of intelligent methods for security.

Department of Defense Appropriations for ... Springer

This book constitutes the refereed proceedings of the 17th International Conference on Network and System Security, NSS 2023, held in Canterbury, UK, August 14-16, 2023. The 12 full

and 9 short papers presented together with 2 invited talks in this book were carefully reviewed and selected from 64 submissions. They focus on Attacks and Malware, Blockchain, Security through Hardware, Machine learning and much more.

Secure Data Management Springer

The refereed proceedings of the 12th Asia-Pacific Computer Systems Architecture Conference are presented in this volume. Twenty-six full papers are presented together with two keynote and eight invited lectures. Collectively, they represent some of the most important developments in computer systems architecture. The papers emphasize hardware and software techniques for state-of-the-art, multi-core and multi-threaded architectures.

Computational Intelligence in Security for Information Systems Springer

This book constitutes the refereed proceedings of the 10th Asia-Pacific Computer Systems Architecture Conference, ACSAC 2005, held in Singapore in October 2005. The 65 revised full papers presented were carefully reviewed and selected from 173 submissions. The papers are organized in topical sections on energy efficient and power aware techniques, methodologies and architectures for application-specific systems, processor architectures and microarchitectures, high-reliability and fault-tolerant architectures, compiler and OS for emerging architectures, data value predictions, reconfigurable computing systems and polymorphic architectures, interconnect networks and network interfaces, parallel architectures and computation models, hardware-software partitioning, verification, and testing of complex architectures, architectures for secured computing,

simulation and performance evaluation, architectures for emerging technologies and applications, and memory systems hierarchy and management.

Computer Security -- ESORICS 2015 Springer Science & Business Media

Now that there's software in everything, how can you make anything secure? Understand how to engineer dependable systems with this newly updated classic *In Security Engineering: A Guide to Building Dependable Distributed Systems*, Third Edition Cambridge University professor Ross Anderson updates his classic textbook and teaches readers how to design, implement, and test systems to withstand both error and attack. This book became a best-seller in 2001 and helped establish the discipline of security engineering. By the second edition in 2008, underground dark markets had let the bad guys specialize and scale up; attacks were increasingly on users rather than on technology. The book repeated its success by showing how security engineers can focus on usability. Now the third edition brings it up to date for 2020. As people now go online from phones more than laptops, most servers are in the cloud, online advertising drives the Internet and social networks have taken over much human interaction, many patterns of crime and abuse are the same, but the methods have evolved. Ross Anderson explores what security engineering means in 2020, including: How the basic elements of cryptography, protocols, and access control translate to the new world of phones, cloud services, social media and the Internet of Things Who the attackers are – from nation states and business competitors through criminal gangs to stalkers and playground bullies What they do – from

phishing and carding through SIM swapping and software exploits to DDoS and fake news Security psychology, from privacy through ease-of-use to deception The economics of security and dependability - why companies build vulnerable systems and governments look the other way How dozens of industries went online - well or badly How to manage security and safety engineering in a world of agile development - from reliability engineering to DevSecOps The third edition of Security Engineering ends with a grand challenge: sustainable security. As we build ever more software and connectivity into safety-critical durable goods like cars and medical devices, how do we design systems we can maintain and defend for decades? Or will everything in the world need monthly software upgrades, and become unsafe once they stop?

Building Secure Defenses Against Code-Reuse Attacks Springer

The adoption of Information and Communication Technologies (ICT) in healthcare is driven by the need to contain costs while maximizing quality and efficiency. However, ICT adoption for healthcare information management has brought far-reaching effects and implications on the spirit of the Hippocratic Oath, patient privacy and confidentiality. A wave of security breaches have led to pressing calls for opt-in and opt-out provisions where patients are free to choose to or not have their healthcare information collected and recorded within healthcare information systems. Such provisions have negative impact on cost, efficiency and quality of patient care. Thus determined efforts to gain patient trust is increasingly under consideration for enforcement through legislation, standards, national policy

frameworks and implementation systems geared towards closing gaps in ICT security frameworks. The ever-increasing healthcare expenditure and pressing demand for improved quality and efficiency in patient care services are driving innovation in healthcare information management. Key among the main innovations is the introduction of new healthcare practice concepts such as shared care, evidence-based medicine, clinical practice guidelines and protocols, the cradle-to-grave health record and clinical workflow or careflow. Central to these organizational re-engineering innovations is the widespread adoption of Information and Communication Technologies (ICT) at national and regional levels, which has ushered in computer-based healthcare information management that is centred on the electronic healthcare record (EHR).

Entity-Relationship Approach - ER '93 Springer Science & Business Media

This book constitutes the refereed proceedings of the 9th Asia-Pacific Computer Systems Architecture Conference, ACSAC 2004, held in Beijing, China in September 2004. The 45 revised full papers presented were carefully reviewed and selected from 154 submissions. The papers are organized in topical sections on cache and memory, reconfigurable and embedded architectures, processor architecture and design, power and energy management, compiler and operating systems issues, application-specific systems, interconnection networks, prediction techniques, parallel architectures and programming, microarchitecture design and evaluation, memory and I/O systems, and others.

Telecommunications, Command and Control Programs John Wiley

& Sons

This book constitutes the refereed proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection, RAID 2008, held in Cambridge, MA, USA, in September 2008. The 20 revised full papers presented together with 16 revised poster papers were carefully reviewed and selected from 80 submissions. The papers are organized in topical sections on rootkit prevention, malware detection and prevention, high performance intrusion and evasion, Web application testing and evasion, alert correlation and worm detection, as well as anomaly detection and network traffic analysis.

Advances in Computer Systems Architecture Springer
Annotation Forty-four papers from the December 2000 conference address challenges in the field of information security. The main areas of discussion are intrusion detection, security policy, public key infrastructure, access control, security architecture, e-commerce, and cryptography. Topics include extending Java for package-based access control, policy mediation for multi-enterprise environments, binding identities and attributes using digitally signed certificates, using operating system wrappers to increase the resiliency to commercial firewalls, calculating costs for quality of security service, and the Chinese Remainder Theorem and its application in a high-speed RSA crypto chip. No subject index. Annotation copyrighted by Book News, Inc., Portland, OR.

Department of Defense Appropriations for 1980: Telecommunications, command and control programs. Research, development, test and evaluation Springer

This book constitutes the refereed proceedings of the 8th

International Symposium on Recent Advances in Intrusion Detection held in September 2005. The 15 revised full papers and two practical experience reports were carefully reviewed and selected from 83 submissions. The papers are organized in topical sections on worm detection and containment, anomaly detection, intrusion prevention and response, intrusion detection based on system calls and network-based, as well as intrusion detection in mobile and wireless networks.

The Department of the Army Manual Springer

Online Harassment is one of the most serious problems in social media. To address it requires understanding the forms harassment takes, how it impacts the targets, who harasses, and how technology that stands between users and social media can stop harassers and protect users. The field of Human-Computer Interaction provides a unique set of tools to address this challenge. This book brings together experts in theory, socio-technical systems, network analysis, text analysis, and machine learning to present a broad set of analyses and applications that improve our understanding of the harassment problem and how to address it. This book tackles the problem of harassment by addressing it in three major domains. First, chapters explore how harassment manifests, including extensive analysis of the Gamer Gate incident, stylistic features of different types of harassment, how gender differences affect misogynistic harassment. Then, we look at the results of harassment, including how it drives people offline and the impacts it has on targets. Finally, we address techniques for mitigating harassment, both through automated detection and filtering and interface options that users control. Together, many branches of HCI come together to provide a

comprehensive look at the phenomenon of online harassment and to advance the field toward effective human-oriented solutions.

Department of the Army IEEE Computer Society Press

This monograph is devoted to computational morphology, particularly to the construction of a two-dimensional or a three-dimensional closed object boundary through a set of points in arbitrary position. By applying techniques from computational geometry and CAGD, new results are developed in four stages of the construction process: (a) the gamma-neighborhood graph for describing the structure of a set of points; (b) an algorithm for constructing a polygonal or polyhedral boundary (based on (a)); (c) the flintstone scheme as a hierarchy for polygonal and polyhedral approximation and localization; (d) and a Bezier-triangle based scheme for the construction of a smooth piecewise cubic boundary.

Network and System Security Springer

This book and its companion volumes, LNCS volumes 9140, 9141 and 9142, constitute the proceedings of the 6th International Conference on Swarm Intelligence, ICSI 2015 held in conjunction with the Second BRICS Congress on Computational Intelligence,

CCI 2015, held in Beijing, China in June 2015. The 161 revised full papers presented were carefully reviewed and selected from 294 submissions. The papers are organized in 28 cohesive sections covering all major topics of swarm intelligence and computational intelligence research and development, such as novel swarm-based optimization algorithms and applications; particle swarm optimization; ant colony optimization; artificial bee colony algorithms; evolutionary and genetic algorithms; differential evolution; brain storm optimization algorithm; biogeography based optimization; cuckoo search; hybrid methods; multi-objective optimization; multi-agent systems and swarm robotics; Neural networks and fuzzy methods; data mining approaches; information security; automation control; combinatorial optimization algorithms; scheduling and path planning; machine learning; blind sources separation; swarm interaction behavior; parameters and system optimization; neural networks; evolutionary and genetic algorithms; fuzzy systems; forecasting algorithms; classification; tracking analysis; simulation; image and texture analysis; dimension reduction; system optimization; segmentation and detection system; machine translation; virtual management and disaster analysis.