Logic In Access Control

2.1 Web Application Vulnerabilities Many web application vulnerabilities havebeenwell documented andthemi- gation methods havealso beenintroduced [1]. The most common cause ofthose vulnerabilities isthe insu?cient input validation. Any data originated from o- side of the program code, forexample input data provided by user through a web form, shouldalwaysbeconsidered malicious andmustbesanitized before use.SQLInjection, Remote code execution orCross-site Scriptingarethe very common vulnerabilities ofthattype [3]. Below isabrief introduction toSQL- jection vulnerability though the security testingmethodpresented in thispaper is not limited toit. SQLinjectionvulnerabilityallowsanattackertoillegallymanipulatedatabase byinjectingmalicious SQL codes into the values of input parameters of http requests sentto the victim web site. 1: Fig.1. An example of a program written in PHP which contains SQL Injection v- nerability Figure 1 showsaprogram that uses the database query function mysql query togetuserinformationcorrespondingtothe userspeci?edby the GETinput- rameterusername andthen printtheresultto the clientbrowser.Anormalhttp request with the input parameter username looks like "http://example.com/ index.php?username=bob". The dynamically created database query at line2 is "SELECT @* FROM users WHERE username='bob' AND usertype='user'". Thisprogram is vulnerabletoSQLInjection attacks because mysql query uses the input value of username without sanitizingmalicious codes. A malicious code can be a stringthatcontains SQL symbols ork- words.Ifan attacker sendarequest with SQL code ('alice'-') - jected "http://example.com/index.php?username=alice'-", the query becomes "SELECT@* FROM users WHERE username='alice'--' AND usertype='user'"

This book constitutes the refereed proceedings of the Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2005, held in St. Petersburg, Russia in September 2005. The 25 revised full papers and 12 revised short papers presented together with 5 invited papers were carefully reviewed and selected from a total of 85 submissions. The papers are organized in topical sections on mathematical models, architectures and protocols for computer network security, authentication, authorization and access control, information flow analysis, covert channels and trust management, security policy and operating system security, threat modeling, vulnerability assessment and network forensics, and intrusion detection.

This book constitutes the thoroughly refereed post-conference proceedings of the 7th International Workshop on Security and Trust Management, STM 2011, held in Copenhagen, Denmark, in June 2011 - co-located with IFIPTM 2011, the 5th IFIP International Conference on Trust Management. The 12 revised full papers presented together with 4 invited papers were carefully reviewed and selected from 33 submissions. Focusing on high-quality original unpublished research, case studies, and implementation experiences, STM 2011 features submissions from academia, industry, and government presenting novel research on all theoretical and practical aspects of security and trust in information and communication technologies.

This book constitutes the refereed proceedings of the 12th European Symposium on Research in Computer Security, ESORICS

2007, held in Dresden, Germany in September 2007. The 39 revised full papers presented were carefully reviewed and selected from 164 submissions. ESORICS is confirmed as the European research event in computer security; it presents original research contributions, case studies and implementation experiences addressing any aspect of computer security - in theory, mechanisms, applications, or practical experience.

This two-volume set (CCIS 201 and CCIS 202) constitutes the refereed proceedings of the International Conference on Computer Science and Education, CSE 2011, held in Qingdao, China, in July 2011. The 164 revised full papers presented in both volumes were carefully reviewed and selected from a large number of submissions. The papers address a large number of research topics and applications: from artificial intelligence to computers and information technology; from education systems to methods research and other related issues; such as: database technology, computer architecture, software engineering, computer graphics, control technology, systems engineering, network, communication, and other advanced technology, computer education, and life-long education.

This book constitutes the refereed proceedings of the 13th International Conference on Security, Privacy, and Anonymity in Computation, Communication, and Storage, SpaCCS 2020, held in Nanjing, China, in December 2020. The 30 full papers were carefully reviewed and selected from 88 submissions. The papers cover many dimensions including security algorithms and architectures, privacy-aware policies, regulations and techniques, anonymous computation and communication, encompassing fundamental theoretical approaches, practical experimental projects, and commercial application systems for computation, communication and storage. SpaCCS 2020 is held jointly with the 11th International Workshop on Trust, Security and Privacy for Big Data (TrustData 2020), the 10th International Symposium on Trust, Security and Privacy for Emerging Applications (TSP 2020), the 9th International Symposium on Security and Privacy on Internet of Things (SPIoT 2020), the 6th International Symposium on Sensor-Cloud Systems (SCS 2020), the 2nd International Workshop on Communication, Computing, Informatics and Security (CCIS 2020), the First International Workshop on Intelligence and Security in Next Generation Networks (ISNGN 2020), the First International Symposium on Emerging Information Security and Applications (EISA 2020).

As part of the Syngress Basics series, The Basics of Information Security provides you with fundamental knowledge of information security in both theoretical and practical aspects. Author Jason Andress gives you the basic knowledge needed to understand the key concepts of confidentiality, integrity, and availability, and then dives into practical applications of these ideas in the areas of operational, physical, network, application, and operating system security. The Basics of Information Security gives you clear-non-technical explanations of how infosec works and how to apply these principles whether you're in the IT field or want to understand how it affects your career and business. The new Second Edition has been updated for the latest trends and threats, including new material on many infosec subjects. Learn about information security without wading through a huge textbook Covers both theoretical and practical aspects of information security Provides a broad view of the information security field in a concise manner All-new Second Edition updated for the latest information security trends and threats, including material on incident response,

social engineering, security awareness, risk management, and legal/regulatory issues
Access Control, Security, and TrustA Logical ApproachCRC Press
Electronic Access Control, Second Edition provides the latest advice on how to interface systems from multiple Electronic Access Control (EAC) manufacturers into a single cohesive system. The book shows how to provide integration, while also allowing building security managers to protect, control and manage their own users' card data. This second edition details advanced card data management and advanced system access level management. Readers will be better able to manage their systems to protect the privacy of their cardholders' private information, while providing much improved control over the security of their buildings. Like its highly regarded first edition, the book offers the complete picture on EAC for readers at any level of expertise. It provides comprehensive material on how to select, and interface to, the appropriate locking hardware, typically the most difficult responsibility for access control system designers, installers and end users. Provides a comprehensive understanding of Electronic Access Control (EAC) Systems to readers at any level, novices and experts alike Helps readers understand concepts for securing a facility, while providing transparent access to those who frequently, and legitimately, enter the facility Includes expanded information on system configurations, including user data security, access levels, access clearances and groups, and system interfaces Offers all new material on how to interface systems from multiple manufacturers into a single cohesive system
Presents an Cyber-Assurance approach to the Internet of Things (IoT) This book discusses the cyber-assurance needs of the IoT environment, highlighting key information assurance (IA) IoT issues and identifying the associated security implications. Through contributions from cyber-assurance, IA, information security and IoT industry practitioners and experts, the text covers fundamental and advanced concepts necessary to grasp current IA issues, challenges, and solutions for the IoT. The future trends in IoT infrastructures, architectures and applications are also examined. Other topics discussed include the IA protection of IoT systems and information being stored, processed or transmitted from unauthorized access or modification of machine-2-machine (M2M) devices, radio-frequency identification (RFID) networks, wireless sensor networks, smart grids, and supervisory control and data acquisition (SCADA) systems. The book also discusses IA measures necessary to detect, protect, and defend IoT information and networks/systems to ensure their availability, integrity, authentication, confidentially, and non-repudiation. Discusses current research and emerging trends in IA theory, applications, architecture and information security in the IoT based on theoretical aspects and studies of practical applications Aids readers in understanding how to design and build cyber-assurance into the IoT Exposes engineers and designers to new strategies and emerging standards, and promotes active development of cyber-assurance Covers challenging issues as well as potential solutions, encouraging discussion and debate amongst those in

the field Cyber-Assurance for the Internet of Things is written for researchers and professionals working in the field of wireless technologies, information security architecture, and security system design. This book will also serve as a reference for professors and students involved in IA and IoT networking. Tyson T. Brooks is an Adjunct Professor in the School of Information Studies at Syracuse University; he also works with the Center for Information and Systems Assurance and Trust (CISAT) at Syracuse University, and is an information security technologist and science-practitioner. Dr. Brooks is the founder/Editor-in-Chief of the International Journal of Internet of Things and Cyber-Assurance, an associate editor for the Journal of Enterprise Architecture, the International Journal of Cloud Computing and Services Science, and the International Journal of Information and Network Security.

This book constitutes the refereed proceedings of the 24th IFIP TC 11 International Information Security Conference, SEC 2009, held in Pafos, Cyprus, in May 2009. The 38 revised full papers presented were carefully reviewed and selected from 176 submissions. The papers are organized in topical sections on identification and authentication, threats and attacks, applications of cryptography and information hiding, trusted computing, security policies, validation, verification and evaluation, privacy protection and security assessment, role mining and content protection, security protocols, access control, and internet and Web applications security.

This volume contains the proceedings of the 24th International Conference on Logic Programming (ICLP 2008). The conference took place in Udine, Italy during December 9–13, 2008. The conference focuses on the foundations, dev-opments, and applications in the area of logic programming. The ICLP series of conferences is aimed at providing a technical forum for presenting and d- seminating innovative research results in the ?eld of logic programming. The conference features technical presentations, tutorials, invited speakers, and a number of co-located events, including: – The First Workshop on Answer Set Programming and Other Computing Paradigms (ASPOCP 2008) – The Annual Meeting of the ISO/IEC JTC1/SC22/WG17 working group on the standardization of Prolog – The Third International Workshop on Applications of Logic Programming to (Semantic) Web and Web Services (ALPSWS'08) – The18thWorkshoponLogic-basedMethodsin ProgrammingEnvironments (WLPE 2008) – The 8th Colloquium on Implementation of Constraint Logic Programming Systems (CICLOPS 2008) – The 15th RCRA Workshop on Experimental Evaluation of Algorithms for Solving Problems with Combinatorial Explosion ICLP 2008 also featured two special events. The ?rst was the 4th ICLP Doctoral Student Consortium, an event speci?cally organized to encourage p-ticipation and interaction between doctoralstudents working in the area of logic programming. The second event was a special session celebrating 20 years of Stable Model Semantics.

SmartData empowers personal data by wrapping it in a cloak of intelligence such that it now becomes the individual’s

virtual proxy in cyberspace. No longer will personal data be shared or stored in the cloud as merely data, encrypted or otherwise; it will now be stored and shared as a constituent of the binary string specifying the entire SmartData agent. This agent proactively builds-in privacy, security and user preferences, right from the outset, not as an afterthought. SmartData: Privacy Meets Evolutionary Robotics includes the advances made in the technology of simulating virtual worlds, together with the ideas emerging from fields of evolutionary robotics and embodied cognition within a framework of dynamical systems as an approach toward this ultimate goal. The book brings together top researchers in the field and addresses current personal data privacy challenges in the online-world.

This book contains a selection of the papers presented at the 19th International Workshop on Functional and Constraint Logic Programming, WFLP 2010, held in Madrid, Spain, in January 2010, as part of the ACM-SIGPLAN Principles of Programming Languages event, POPL 2010. From the 15 papers submitted, 12 were accepted for presentation at the workshop. The 8 regular papers presented in this volume were selected following a second round of reviewing, which took place after the event. They are complemented by a full-length invited talk by the workshop's guest speaker, Mariangiola Dezani-Ciancaglini. All current issues in the areas of functional and constraint logic programming are covered including foundational aspects, language design, implementation, transformation and analysis, software engineering, integration of paradigms, and applications.

Focuses mainly on communications and communication standards with emphasis also on risk analysis, ITSEC, EFT and EDI with numerous named viruses described. The dictionary contains extended essays on risk analysis, personal computing, key management, pin management and authentication.

Totally updated for 2011, here's the ultimate study guide for the CISSP exam Considered the most desired certification for IT security professionals, the Certified Information Systems Security Professional designation is also a career-booster. This comprehensive study guide covers every aspect of the 2011 exam and the latest revision of the CISSP body of knowledge. It offers advice on how to pass each section of the exam and features expanded coverage of biometrics, auditing and accountability, software security testing, and other key topics. Included is a CD with two full-length, 250-question sample exams to test your progress. CISSP certification identifies the ultimate IT security professional; this complete study guide is fully updated to cover all the objectives of the 2011 CISSP exam Provides in-depth knowledge of access control, application development security, business continuity and disaster recovery planning, cryptography, Information Security governance and risk management, operations security, physical (environmental) security, security architecture and design, and telecommunications and network security Also covers legal and regulatory investigation and compliance Includes two practice exams and challenging review questions on the CD Professionals seeking the CISSP

certification will boost their chances of success with CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition.

21 articles from the Security Awareness Bulletin which was made available exclusively to "cleared" employees in the U.S. defense industry. Covers: the foreign intelligence threat; espionage case studies; security policy and programs; computer and communications security (including "keeping tabs on the digital magicians"); and 68 summaries of recent espionage cases from 1975-1989. Supports security training and awareness programs in industry and government. Fascinating, spell-binding reading of actual national security cases. You won't be able to put this book down!

Developed from the authors' courses at Syracuse University and the U.S. Air Force Research Laboratory, Access Control, Security, and Trust: A Logical Approach equips readers with an access control logic they can use to specify and verify their security designs. Throughout the text, the authors use a single access control logic based on a simple pro

Artificial Intelligence and Security in Computing Systems is a peer-reviewed conference volume focusing on three areas of practice and research progress in information technologies: -Methods of Artificial Intelligence presents methods and algorithms which are the basis for applications of artificial intelligence environments. -Multiagent Systems include laboratory research on multiagent intelligent systems as well as upon their applications in transportation and information systems. -Computer Security and Safety presents techniques and algorithms which will be of great interest to practitioners. In general, they focus on new cryptographic algorithms (including a symmetric key encryption scheme, hash functions, secret generation and sharing schemes, and secure data storage), a formal language for policy access control description and its implementation, and risk management methods (used for continuous analysis both in distributed network and software development projects).

This three-volume set constitutes the refereed proceedings of the International Conference on Computational Science and its Applications. These volumes feature outstanding papers that present a wealth of original research results in the field of computational science, from foundational issues in computer science and mathematics to advanced applications in almost all sciences that use computational techniques.

This book constitutes the refereed proceedings of the 6th International Conference on Information Security, ISC 2003, held in Bristol, UK in October 2003. The 31 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 133 submissions. The papers are organized in topical sections on network security, public key algorithms, cryptographic protocols, protocol attacks, attacks on public key cryptosystems, block ciphers, authorization, water marking, software security, and codes and related issues.

Security and Access Control Using Biometric Technologies presents an introduction to biometrics or the study of recognizing individuals based on their unique physical or behavioral traits, as they relate to computer security. The book begins with the basics of biometric technologies and discusses how and why biometric systems are emerging in information security. An emphasis is directed towards authentication, authorization, identification, and access control. Topics covered include security and management

required to protect valuable computer and network resources and assets, and methods of providing control over access and security for computers and networks. Written for a broad level of readers, this book applies to information system and information technology students, as well as network managers, security administrators and other practitioners. Oriented towards the practical application of biometrics in the real world, Security and Access Control Using Biometric Technologies provides the reader with a realistic view of the use of biometrics in the ever-changing industry of information security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Have you been asked to perform an information systems audit anddon't know where to start? Examine a company's hardware, software,and data organization and processing methods to ensure qualitycontrol and security with this easy, practical guide to auditingcomputer systems--the tools necessary to implement an effective ISaudit. In nontechnical language and following the format of an ISaudit program, you'll gain insight into new types of securitycertifications (e.g., TruSecure, CAP SysTrust, CPA WebTrust) aswell as the importance of physical security controls, adequateinsurance, and digital surveillance systems. Order your copy today!

This book constitutes the refereed proceedings of the 20th International Conference on Automated Reasoning with Analytic Tableaux and Related Methods, TABLEAUX 2011, held in Bern, Switzerland, in July 2011.The 16 revised research papers presented together with 2 system descriptions were carefully reviewed and selected from 34 submissions. The papers cover many topics in the wide range of applications of tableaux and related methods such as analytic tableaux for various logics, related techniques and concepts, related methods, new calculi and methods for theorem proving in classical and non-classical logics, as well as systems, tools, implementations and applications; all with a special focus on hardware and software verifications, semantic technologies, and knowledge engineering.

This book constitutes selected papers from the 12th International Workshop on Rewriting Logic and Its Applications, WRLA 2020, held in Dublin, Ireland, in April 2020. Due to the COVID-19 pandemic the workshop took place virtually. The 11 full papers presented in this volume were carefully reviewed and selected from 16 submissions Rewriting logic is a natural model of computation and an expressive semantic framework for concurrency, parallelism, communication, and interaction. It can be used for specifying a wide range of systems and languages in various application fields.

This book describes a new model, Relation Based Access Control (RelBAC) to handle the dynamics with full features of a general sense access control system. It is organized as follows: Chapter 2 analyzes the new challenges of the Web 2.0 such as the great dynamics in subjects, objects and in permissions. Chapter 3 lists existing access control models as the state of the art. Chapter 4 describes the RelBAC model and logic. We show the reasoning power of RelBAC in chapter 5. In Chapter 6, the extendibility of RelBAC is studied. Chapters 7 and 8 show applications of two important techniques of Semantic Web, Lightweight Ontologies and Semantic Matching, on the model of RelBAC. We show some evaluation results in Chapter 9. The result of general sense purpose Decription Logic reasoners are not good enough and we are proceeding with research on more efficient reasoning in the near

future. Chapter 10 describes the framework for implementing a system based on RelBAC and DL reasoner. We conclude that RelBAC is a natural formal model for the access control problem of Web 2.0 in Chapter 11.

The 1st International Conference on “Applied Cryptography and Network Se- rity” (ACNS 2003) was sponsored and organized by ICISA (International C- munications and Information Security Association), in cooperation with MiAn Pte. Ltd. and the Kunming government. It was held in Kunming, China in - tober 2003. The conference proceedings was published as Volume 2846 of the Lecture Notes in Computer Science (LNCS) series of Springer-Verlag. The conference received 191 submissions, from 24 countries and regions; 32 of these papers were accepted, representing 15 countries and regions (acceptance rate of 16.75%). In this volume you will ?nd the revised versions of the - cepted papers that were presented at the conference. In addition to the main track of presentations of accepted papers, an additional track was held in the conference where presentations of an industrial and technical nature were given. These presentations were also carefully selected from a large set of presentation proposals. This new international conference series is the result of the vision of Dr. Yongfei Han. The conference concentrates on current developments that advance the - eas of applied cryptography and its application to systems and network security. The goal is to represent both academic research works and developments in - dustrial and technical frontiers. We thank Dr. Han for initiating this conference and for serving as its General Chair.

This comprehensive encyclopedia provides easy access to information on all aspects of cryptography and security. The work is intended for students, researchers and practitioners who need a quick and authoritative reference to areas like data protection, network security, operating systems security, and more.

This book constitutes the refereed proceedings of the 8th International Symposium on Functional and Logic Programming, FLOPS 2006, held in Fuji-Susono, Japan, in April 2006. The 17 revised full papers presented together with 2 invited contributions were carefully reviewed and selected from 51 submissions. The papers are organized in topical sections on data types, FP extensions, type theory, LP extensions, analysis, contracts, as well as Web and GUI.

This book constitutes the thoroughly refereed post-conference proceedings of the 8th International Workshop on Formal Aspects of Security and Trust, FAST 2011, held in conjunction with the 16th European Symposium on Research in Computer Security, ESORICS 2011, in Leuven, Belgium in September 2011. The 15 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 42 submissions. The papers focus on security and trust policy models; security protocol design and analysis; formal models of trust and reputation; logics for security and trust; distributed trust management systems; trust-based reasoning; digital assets protection; data protection; privacy and ID issues; information flow analysis; language-based security; security and trust aspects of ubiquitous computing; validation/analysis tools; web service security/trust/privacy; grid security; security risk assessment; and case studies.

This book constitutes the refereed proceedings of the Third International Conference on Principles of Security and Trust, POST 2014, held as part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, in

April 2014. The 15 papers presented in this volume were carefully reviewed and selected from 55 submissions. They are organized in topical sections named: analysis of cryptographic protocols; quantitative aspects of information flow; information flow control in programming languages; cryptography in implementations and policies and attacks.

Allowing access to resources, including data and hardware, without compromising their security is a fundamental challenge in computer science. Because of the number and complexity of authorization policies in access control systems, it is clear that ad hoc methods for specifying and enforcing policies cannot inspire a high degree of trust. Authorization logics have been proposed as a theoretically sound alternative. However, for an authorization logic to be useful in practice, it should be able to model most, if not all, naturally occurring policy features. One common feature is the time-dependency of authorizations. For example, a user may only be permitted to access a given resource on workdays. Surprisingly, of the numerous proposals for access control logics, we know of no logic that incorporates time internally. In an attempt to fill this void, this thesis develops a logic with explicit time that permits reasoning about complex, yet natural, time-dependent authorizations. The logic is then extended to account for authorizations that may be used only once. A careful study of the meta-theory of both logics is conducted, and the logics? rich expressive power is demonstrated through several examples. Finally, a proof checker for the latter logic is formalized and discussed.

This is the first commercially available book to offer CISA study materials The consulting editor, Ronald Krutz, is the co-author of The CISSP Prep Guide (0-471-26802-X) Provides definitions and background on the seven content areas of CISA Includes many sample test questions and explanations of answers More than 10,000 people registered for the CISA exam in 2002 CD-ROM contains annual updates to the exam so the book remains current for a number of years

Electronic Access Control introduces the fundamentals of electronic access control through clear, well-illustrated explanations. Access Control Systems are difficult to learn and even harder to master due to the different ways in which manufacturers approach the subject and the myriad complications associated with doors, door frames, hardware, and electrified locks. This book consolidates this information, covering a comprehensive yet easy-to-read list of subjects that every Access Control System Designer, Installer, Maintenance Tech or Project Manager needs to know in order to develop quality and profitable Alarm/Access Control System installations. Within these pages, Thomas L. Norman - a master at electronic security and risk management consulting and author of the industry reference manual for the design of Integrated Security Systems - describes the full range of EAC devices (credentials, readers, locks, sensors, wiring, and computers), showing how they work, and how they are installed. A comprehensive introduction to all aspects of electronic access control Provides information in short bursts with ample illustrations Each chapter begins with outline of chapter contents and ends with a quiz May be used for self-study, or as a professional reference guide

This book constitutes the thoroughly refereed post-conference proceedings of the 8th International Workshop on Security

and Trust Management, STM 2012, held in Pisa, Italy, in September 2012 - in conjunction with the 17th European Symposium Research in Computer Security (ESORICS 2012). The 20 revised full papers were carefully reviewed and selected from 57 submissions. The papers are organized into topical sections on policy enforcement and monitoring; access control; trust, reputation, and privacy; distributed systems and physical security; authentication and security policies.

This book is dedicated to Marek Sergot, Professor in Computational Logic at Imperial College London, on the occasion of his 60th birthday. Professor Sergot’s scientific contributions range over many different fields. He has developed a series of novel ideas and formal methods bridging areas including artificial intelligence, computational logic, philosophical logic, legal theory, artificial intelligence and law, multi-agent systems and bioinformatics. By combining his background in logic and computing with his interest in the law, deontic logic, action, and related areas, and applying to all his capacity to understand the subtleties of social interaction and normative reasoning, Professor Sergot has opened up new directions of research, and has been a reference, an inspiration, and a model for many researchers in the fields to which he has contributed. The Festschrift includes several reminiscences and introductory essays describing Professor Sergot's achievements, followed by a series of articles on logic programming, temporal reasoning and action languages, artificial intelligence and law, deontic logic and norm-governed systems, and logical approaches to policies.

This comprehensive new resource provides an introduction to fundamental Attribute Based Access Control (ABAC) models. This book provides valuable information for developing ABAC to improve information sharing within organizations while taking into consideration the planning, design, implementation, and operation. It explains the history and model of ABAC, related standards, verification and assurance, applications, as well as deployment challenges. Readers find authoritative insight into specialized topics including formal ABAC history, ABAC’s relationship with other access control models, ABAC model validation and analysis, verification and testing, and deployment frameworks such as XACML. Next Generation Access Model (NGAC) is explained, along with attribute considerations in implementation. The book explores ABAC applications in SOA/workflow domains, ABAC architectures, and includes details on feature sets in commercial and open source products. This insightful resource presents a combination of technical and administrative information for models, standards, and products that will benefit researchers as well as implementers of ABAC systems in the field.

This book presents tutorial lectures from three International Schools on Foundations of Security Analysis and Design, FOSAD 2007/2008/2009. Topics include cryptographic protocol analysis, identity management and electronic voting, and wireless security.

Government and companies have already invested hundreds of millions of dollars in the convergence of physical and logical security solutions, but there are no books on the topic. This book begins with an overall explanation of information security, physical security, and why approaching these two different types of security in one way (called convergence) is so critical in today's changing security landscape. It then details enterprise security management as it relates to incident detection and incident management. This is followed by detailed examples of implementation, taking the reader through cases addressing various physical security technologies such as: video surveillance, HVAC, RFID, access controls, biometrics, and more. This topic is picking up momentum every day with every new computer exploit, announcement of a malicious insider, or issues related to terrorists, organized crime, and nation-state threats The author has over a decade of real-world security and management expertise developed in some of the most sensitive and mission-critical environments in the world Enterprise Security Management (ESM) is deployed in tens of thousands of organizations worldwide

Developed from the authors' courses at Syracuse University and the U.S. Air Force Research Laboratory, Access Control, Security, and Trust: A Logical Approach equips readers with an access control logic they can use to specify and verify their security designs. Throughout the text, the authors use a single access control logic based on a simple propositional modal logic. The first part of the book presents the syntax and semantics of access control logic, basic access control concepts, and an introduction to confidentiality and integrity policies. The second section covers access control in networks, delegation, protocols, and the use of cryptography. In the third section, the authors focus on hardware and virtual machines. The final part discusses confidentiality, integrity, and role-based access control. Taking a logical, rigorous approach to access control, this book shows how logic is a useful tool for analyzing security designs and spelling out the conditions upon which access control decisions depend. It is designed for computer engineers and computer scientists who are responsible for designing, implementing, and verifying secure computer and information systems.