Computable Methods for System Assurance Properties (Postprint)

Authors: Guo Yunchuan, Yin Lihua, Liu Licai

Date: 2017-03-10T00:00:00+00:00

Abstract

Due to the increasing complexity of system operating environments, the diversity of users, and the undecidability of software correctness, ensuring that systems deliver services entirely as intended is extremely difficult. Consequently, security assessment methods and modeling techniques have become essential components and key supporting technologies in system assurance research, employed to address issues such as the locality and state explosion inherent in existing assessment methods, as well as the absence of content access control assessment methods for the Internet. This paper first surveys related work on security assessment, and then introduces our research contributions—control models and quantitative evaluation methods for information content security, and confidentiality and integrity models in hybrid detection.

Full Text

Preamble

Vol. 9 No. 3 Information Technology Letters Vol.9 No.3
Computational Methods for Properties in System Assurance
Guo Yunchuan, Yin Lihua, Liu Licai

Abstract

Ensuring that a system delivers services exactly as intended is exceedingly difficult due to the complexity of operational environments, diversity of users, and the undecidability of software correctness. Consequently, security evaluation methods and modeling techniques have become critical components and key enabling technologies in system assurance research, addressing limitations in existing evaluation approaches such as locality, state explosion, and the lack of assessment methods for internet content access control. This paper first provides an overview of related work on security evaluation, then introduces our

research on control models and quantitative evaluation methods for information content security, as well as confidentiality and integrity models in hybrid detection.

Keywords: system assurance; attribute computation model; quantitative evaluation; security properties

1 Introduction

The research community' s understanding of security has evolved through a progression from information security (IS) to information assurance (IA), from information assurance to software assurance (SwA), and from software assurance to system assurance (SysA). The transition from information security to information assurance signifies a shift from technology-centric to service-oriented approaches, moving from providing technical means to delivering security service capabilities. The evolution from information assurance to software assurance represents a movement from external to internal perspectives, transforming post-hoc supplementary measures into proactive defensive mechanisms that intercept threats at their source. The progression from software assurance to system assurance indicates a broadening from partial to holistic approaches, shifting from unilateral security concerns to comprehensive, system-wide considerations.

Fundamentally, system assurance ensures that hardware and software systems provide expected services when interacting with users in specific environments, while offering a reasonable level of confidence. Given the complexity of system environments, user diversity, and the undecidability of software correctness, guaranteeing that systems absolutely perform as intended is extremely challenging. Under these circumstances, system evaluation becomes paramount.

In recent years, researchers have proposed numerous models and methods for security analysis and evaluation. Currently, widely adopted approaches include rule-based evaluation and model-based evaluation. Rule-based evaluation extracts characteristics from known security issues and generalizes them into rule expressions, which are then matched against target systems to identify potential vulnerabilities. Model-based evaluation, conversely, constructs comprehensive system models to capture all possible behaviors and states, enabling system-wide security assessment through model analysis tools. However, these are generic methods that may deviate from specific user security requirements and lack precision. For instance, if a system only requires integrity protection and has no integrity violations but does have vulnerabilities affecting other security properties, generic methods analyzing all vulnerabilities will produce evaluations that diverge from user concerns, compromising result accuracy. Consequently, fixing irrelevant vulnerabilities incurs unnecessary costs.

We contend that the services provided by system assurance can be reduced to logical combinations of security properties such as confidentiality, authenticity, controllability, and availability of information or system components. Therefore,

security measurement of system and component services directly reduces to computational problems of the underlying security properties.

Accordingly, we have selected "Security Attribute Computation Models and Evaluation Methods for System Assurance" as our research focus. Building upon analysis of cutting-edge developments in security attribute models, theories, and technologies both domestically and internationally, and drawing from existing achievements in attribute analysis and security evaluation, we have developed evaluation models, methods, and technologies based on probabilistic calculation of security properties to enhance assessment capabilities for information content security and network access control. Specifically, the attribute-computable framework partitions security services from a security attribute perspective, studies hierarchical relationships among subsystems, distinguishes topological relationships between sub-services, evaluates subsystems' capabilities to provide sub-services, and ultimately calculates each layer' s ability to guarantee different security properties through probability propagation.

Compared to generic evaluation methods, the attribute-computable framework not only provides quantitative assessment of specific security services, effectively overcoming inaccuracies in generic approaches, but also offers refinement capabilities from different perspectives (security layers and security elements), enabling evaluation at various system levels and identifying deficiencies in existing technologies. Relative to qualitative analysis, the framework' s advantages are twofold: (1) it better identifies bottlenecks in security requirement fulfillment, thereby improving assurance capabilities; and (2) it provides more reasonable measurement—qualitative analysis typically yields binary results (secure or insecure), whereas maintaining absolute security is impossible in practice; security breaches need only be kept within acceptable limits. Attribute computation precisely measures security degrees, making the framework more aligned with practical requirements. Compared to other quantitative analyses, the attribute-computable framework examines capabilities from the perspective of indivisible sub-services, effectively reducing subjectivity in value assignments.

2 Related Research Overview

Implementing system evaluation based on attribute-computable thinking requires first establishing security models and analyzing relationships among attributes, then performing quantitative evaluation. This necessitates formal description of security properties. Therefore, we overview related work from three perspectives: formal description methods and correlation analysis of security properties, security models, and quantitative analysis methods.

2.1 Formal Description and Correlation Analysis of Security Properties

Formal description of security properties originated with J. Jacob [1], encompassing two main approaches: process algebra-based methods and epistemic

logic-based methods. Process algebra-based research on security properties further divides into two branches: information flow security property analysis and general security property analysis.

Information flow security property analysis based on process algebra primarily investigates how to analyze system interference and quantify information leakage in such interference. J. Goguen of the University of California first introduced the non-interference concept [2, 3]. Representative researchers analyzing information flow security properties include R. Focardi from Università Ca' Foscari di Venezia [4, 5] and A. Aldini from Università Degli Studi di Urbino Carlo Bo [6, 7]. Their work primarily employs non-interference methods to analyze conditions under which information leakage occurs. The general approach involves designing appropriate description frameworks, then analyzing when information flow constitutes no leakage (termed a property), and subsequently comparing relationships among properties under different conditions. Figures 1, 2, and 3 respectively present Venn diagrams of properties under non-deterministic, probabilistic, and temporal-probabilistic conditions [4,6,57]. In Figures 1-3: NNI—Non-deterministic Non-Interference, NDC —Non-Deducibility on Compositions, BNNI—Bisimulation NNI, SNNI—Strong NNI, BSNNI—Bisimulation Strong NNI, BNDC—Bisimulation NDC, SBSNN—Strong BSNNI, SBNDC—Strong BNDC, BSPNI—Strong Bisimulation Probabilistic Non-Interference, PBNDC—Probabilistic BNDC, SPSNDC—Strong PBNDC, TNI—Time Non-Interference, PTNI—Probabilistic TNI. While much of this work is titled "Security Properties," it discusses only implicit information leakage, essentially analyzing confidentiality, which is only one aspect of security properties.

In general security property analysis based on process algebra, representative work includes that of S. Schneider from University College London [8], who used Communicating Sequential Processes (CSP) to characterize and analyze security properties independently of systems (security protocols), covering confidentiality and message authentication. Another contribution by Focardi [9, 10] treats system attacks as interference actions, using traces to describe agreement properties, message-oriented authentication, and non-repudiation. The conclusion states that a system satisfies these security properties if and only if traces under attack are prefixes of traces without attack. This work effectively combines non-interference concepts with general security properties, though it analyzes only confidentiality, authentication, and non-repudiation.

M. Burrows et al. from Cambridge University pioneered the use of epistemic logic to describe security properties [11], aiming to analyze security protocols—this logic became known as BAN logic. BAN logic spawned numerous security protocol analysis logics, including GNY [12], AT [13], and VO [14]. Epistemic logic represents knowledge and belief through expressions like "principal knows ···" and "principal believes···," offering simplicity, intuitiveness, and flexibility. However, current epistemic logic methods cannot truly solve protocol security analysis problems and serve only as auxiliary tools for discovering vulnerabili-

ties, as many protocols "proven" secure by these logics were later found insecure. The fundamental reasons include lack of formal semantics, ambiguous interpretations, non-probabilistic axioms, and potentially unreliable logical rules [15].

Beyond process algebra and epistemic logic, other approaches exist, such as [16, 17]. S. Gürgens [16] also describes system properties as action traces, characterizing authentication and confidentiality, but this method is non-intuitive and makes reasoning about property relationships difficult. In security protocols, many methods describe security properties, such as linear temporal logic used by Xu Weiwen [18] and computation tree logic employed by M. Panti [19]. Additionally, B. Alpern and F. Schneider from Cornell University provided formal descriptions of Safety and Liveness [20], noting that every property is the intersection of Safety and Liveness. In 2008, M. R. Clarkson and F. Schneider introduced the concept of Hyperproperties [21].

The earliest confidentiality model is the BLP model [22], and the earliest integrity model is the Biba model [23]. These models' cores are "no read up, no write down" and "no write up, no read down," respectively, representing opposite policies. Both models have been extensively discussed in research and widely applied in engineering. Other models include RBAC, information flow models, non-interference models [2], DTE [24], Clark-Wilson [25], Chinese Wall, and UCON [26]. Each has strengths and weaknesses: RBAC offers simple structure and easy implementation but struggles to control users accessing systems with different identities; information flow models can address covert channels but some strict security conditions are undecidable; the Chinese Wall model addresses both confidentiality and integrity for business conflict resolution, performing well in finance; the Clark-Wilson model theoretically addresses integrity well but is difficult to implement. Overall, confidentiality and integrity models define conditions for security but do not support quantitative evaluation.

Most models for availability, reliability, and survivability employ graph theory and stochastic models. S. Jha et al. [52] applied state machine models, formal logic, and Bayesian analysis to system availability and survivability. Y. Liu et al. [53] provided a general survivability evaluation framework, assuming system failure times follow stochastic distributions to obtain Markov models of transmission networks and derive survivability metrics. Such queueing and reliability theory-based analysis has also been applied to ad-hoc networks [54]. J. McDermott et al. [55] used Stochastic Process Algebra to describe attacker and system behaviors, quantitatively evaluating system availability and survivability. M. Dacier et al. [56] used Stochastic Petri Nets (SPN) to analyze system security, converting atomic attacks into stochastic transitions in SPN and solving the model to obtain continuous-time Markov chains. Advanced stochastic models offer strong descriptive power for system resources and services during operation, significantly contributing to security design, but quantitative security analysis using these models suffers from state explosion problems.

2.3 Quantitative Evaluation of Security Properties

For information confidentiality, some research measures implicit leakage from an interference perspective. The earliest quantitative confidentiality work dates to 1982, when D. Denning [28] presented methods for detecting information leakage in programs. Subsequent research expanded significantly, with representative contributions including: J. Millen [29] in 1987 first studied the relationship between non-interference and mutual information, establishing connections between state machine models in information flow and Shannon entropy. J. McLean [30] and J. W. Gray III [31] distinguished non-deterministic and probabilistic information flows, presenting general models for probabilistic information flow. However, Denning and Millen' s approaches suffer from inaccurate measurement [32], and McLean' s work struggles to distinguish causal relationships between high and low security-level objects. Moreover, these approaches are Shannon entropy-based, yet G. Smith [33] noted in 2009 that a variable can have arbitrarily large Shannon entropy even if easily guessed, rendering Shannon entropy-based approaches potentially inaccurate. Smith consequently proposed Bayesian risk-based measures using Rényi min-entropy to quantify uncertainty for information leakage measurement. In 2005, Clarkson [34] used probability distributions to model attacker beliefs, applied Bayesian techniques to update these beliefs, and utilized relative entropy to quantify belief-based information flow. In 2010, S. Hamadou [35] argued that belief-based and Bayesian risk approaches for quantifying information flow were also inaccurate, proposing a hybrid metric. In 2008, A. Aldini et al. [36-38] employed probabilistic weak bisimulation to identify information leakage, measuring it through maximum probability differences of identical actions across different processes. However, our experiments demonstrate this measurement approach is inaccurate [39].

At the abstract interpretation level, H. Yasuoka [40] analyzed the difficulty and feasibility of entropy-based quantitative analysis, noting that for arbitrary k, existing methods are not k-safety and thus cannot quantify information leakage through self-composition. B. Köpf [41] used guessed entropy to measure side-channel attacks, quantifying information leakage bounds based on program execution counts.

This analysis reveals that while information flow quantification has been deeply studied, ensuring measurement accuracy remains challenging. Additionally, few works analyze information leakage bounds. More importantly, most information flow measurement research focuses on leakage, with little attention to information flow integrity. In 2010, Clarkson initiated quantitative evaluation for information flow integrity [42], using mutual information to distinguish contamination and suppression points for calculating integrity violation degrees. Although pioneering, this approach employs singular metrics without considering topology changes, propagation of contamination/suppression points, or potential differences, limiting its applicability.

B. Littlewood' s probabilistic quantitative methods for security properties [43]

address operational security and service availability, seeking similarities between dependability evaluation and security property assessment to provide probabilistic definitions for availability, reliability, and survivability metrics. However, dependability analysis assumes system failures result from random component faults, whereas security failures in actual networks and information systems stem from malicious attacks causing Byzantine faults, creating a gap between dependability and quantitative security evaluation. Graph theory, queueing theory, and stochastic model-based quantitative analysis methods [44] suffer from state explosion given current network systems' large scale and complexity, limiting applicability to local networks or small-scale systems without forming systematic, practical evaluation methods or implementation mechanisms, and exhibiting inconsistent and overlapping security property semantics.

3 Research Progress

Attribute computability for system assurance requires studying the computation of controllability, availability, authenticity, and confidentiality.

3.1 Internet Content Security Control Model ICCON and Evaluation

While access control theory and security evaluation have advanced significantly, control models and quantitative evaluation methods for information content security remain underexplored.

3.1.1 Reference Monitor Locations The reference monitor stores access control policies and decision rules, controlling subject access to objects based on these rules, making it the core component of access control. In information content security, three types of reference monitors exist: Server-side Reference Monitor (SRM), Client-side Reference Monitor (CRM), and Networked Reference Monitor (NRM), as shown in Figures 4 [Figure 4: see original paper] through 6 [Figure 6: see original paper]. SRM examines information flows from objects to subjects or operations performed by subjects on objects at the server side; CRM performs similar examinations at the client side; and NRM implements content security control from the network perspective.

3.1.2 Control Model Since harmful information disseminators will not voluntarily submit information to NRM for analysis, NRM must first obtain access information to control content. As acquired information may lack explicit attribute identifiers, authentication is required, followed by response to improper information flows. Consequently, the NRM control process comprises three phases: information acquisition, authentication, and response. The three fundamental elements of communication— "who communicates with whom," "how they communicate,"and "what content is communicated"—define the control process objects: identity, content, and behavior. Based on the information content security control process and objects, three fundamental models emerge: content-based control model (ICCONC), identity-based control model (ICCONI), and

behavior-based control model (ICCONB). The combination of these three models forms ICCON, as shown in Figure 7 [Figure 7: see original paper].

3.1.3 Evaluation Methods Evaluating information content security control capabilities represents a key research focus. Two evaluation approaches exist: social evaluation and technical evaluation. Social evaluation assesses control effectiveness from societal needs, measuring the gap between control results and social expectations. Technical evaluation assesses specific control techniques' effectiveness, reflecting the gap between actual and expected results under given conditions.

Two metrics are commonly employed: miss-control rate and false-control rate. Miss-control rate is the probability of failing to respond when a response is expected, while false-control rate is the probability of responding when no response is expected. Expectations may derive from social or technical perspectives, yielding four metric categories: social miss-control rate, social false-control rate, technical miss-control rate, and technical false-control rate. This work focuses on technical evaluation, transforming information content security capability evaluation into control process evaluation—assessing information acquisition, authentication, and response capabilities to ultimately evaluate overall information content security control capability.

3.2 Confidentiality and Integrity Model in Hybrid Detection

Confidentiality and integrity in mobile computing constitute core issues in computer security models. The earliest confidentiality model is BLP, and the earliest integrity model is Biba, with contradictory information flow directions. Synthesizing these models requires careful investigation. Literature [45] suggests merging integrity and confidentiality access classes to compose BLP and Biba. Literature [46] notes both models are lattice-based information flow models, allowing composition through the "direct product of lattices remains a lattice" property. However, lattice direct product approaches cannot resolve directional contradictions. Literature [47, 48, 49] proposes a new security model based on trusted subjects to compose BLP and Biba, though trusted subjects with excessive authority may compromise system security. Literature [50] divides information-accessing subjects into four categories: direct creators, direct readers, indirect creators, and indirect readers, protecting confidentiality through "read" operations and integrity through "write" operations. However, since both operations relate closely to both confidentiality and integrity models, whether single "read" or "write" operations can effectively protect confidentiality or integrity requires further study. Literature [51] provides unified confidentiality and integrity policies under downgrade strategies and program equivalence but does not address the BLP-Biba information flow contradiction.

The Hybrid Typed Security Pi (HTSPi) calculus approach leverages -calculus for modeling mobile concurrent system characteristics, borrowing variable assignment patterns from programming languages. This method uses static type

checking to ensure low-confidentiality information flows only to equal or higher confidentiality levels, and high-integrity information flows only to equal or lower integrity levels. For the contradictory flow directions in BLP and Biba models, dynamic checking provides adjustments. This approach organically integrates static and dynamic checking into a unified formal framework that ensures both confidentiality and integrity while enabling efficient static reasoning about system behavior.

4 Conclusion

System assurance aims to guarantee that hardware and software systems provide expected services when interacting with users in specific environments. Security evaluation is an extremely important component for ensuring such expected services. Among numerous security evaluation approaches, security attribute computability theory represents a significant method for assessing system security performance from different abstraction levels and perspectives. However, research in this direction remains in its initial stages, and we hope this work will attract more researchers to this field.

References

J. Jeremy. Security Specifications. Proceedings of the IEEE Symposium on Security and Privacy. 1988, 14-23

J. A. Goguen, J. Meseguer. Security Policies and Security Models. Proceedings of IEEE Symposium on Security and Privacy. 1982, 11-20

J. A. Goguen J. Meseguer. Inference Control and Unwinding. Proceedings of IEEE Symposium on Security and Privacy. 1984,75-86

R. Focardi, R. Gorrieri. Classification of Security Properties (Part I: Information Flow). Proceedings of Foundations of Security Analysis and Design. LNCS 2171. 2001

R. Focardi, R. Gorrieri and F. Martinelli. Classification of Security Properties (Part II: Network Security). Proceedings of Foundations of Security Analysis and Design II. LNCS 2946. 2004

[6] A. Aldini, M. Bravetti and R. Gorrieri. A Process-Algebraic Approach for the Analysis of Probabilistic Non-Interference. Journal of Computer Security. 2004, 12(2):191-245

[7] A. Aldini. Classification of Security Properties in a Linda-Like Process Algebra. Journal of Science of Computer Programming, Special Issue on Security Issues in Coordination Models, Languages and Systems. 2006,63(1):16-38

S. Schneider. Security Properties and CSP. Proceedings of IEEE Symposium on Security and Privacy. 1996,174-187

R. Focardi, F. Martinelli. A Uniform Approach for the Definition of Security Properties. Proceedings of Proceedings of the World Congress on Formal Methods in the Development of Computing Systems, LNCS 1708. 1999,794 - 813

[10] R. Focardi, R. Gorrieri and F. Martinelli. A Comparison of Three

Authentication Properties. Theoretical Computer Science. 2003,291(3):285 - 327
[11] M. Burrows, M. Abadi and R. M. Needham. A Logic of Authentication. ACM Transactions on Computer Systems. 1990, 8(1):18-36
[12] L. Gong, R. Needham and R. Yahalom. Reasoning About Belief in Cryptographic Protocols. Proceedings of Proceedings of the IEEE Symposium on Research in Security and Privacy. 1990,234-248
[13] M. Abadi, M. R. Tuttle. A Semantics for a Logic of Authentication. Proceedings of Annual ACM Symposium on Principles of Distributed Computing. 1991,201 -216
[14] PC. Van Oorschot. Extending Cryptographic Logics of Belief to Key Agreement Protocols. Proceedings of the ACM conference on Computer and communications security. 1994,232 -243
[15] 李益发. 密码协议安全性分析中的逻辑化方法—一种新的 ban 类逻辑. 解放军信息工程大学,
[16] Sigrid Gürgens, Peter Ochsenschläger and Carsten Rudolph. On a Formal Framework for Security Properties. Computer Standards & Interfaces. 2005,27(5):457-466
[17] A. Mana, G. Pujol, Towards Formal Specification of Abstract Security Properties. Proceedings of the Third International Conference on Availability, Reliability and Security 2008,80-87
[18] 陆鑫达, 徐蔚文. 身份认证协议的模型检测分析. 计算机学报. 2003, 26(2):195-201
[19] L. Spalazzi, M. Panti, S. Tacconi, Using the Nusmv Model Checker to Verify the Kerberos Protocol. Proceedings of Proceedings of the Collaborative Technologies Symposium 2002,230-236
[20] B. Alpern, F. B. Schneider. Defining Liveness. Information Processing Letters. 1985, 21(4):181-185
[21] M. Clarkson, F. Schneider. Hyperproperties. Proceedings of Computer Security Foundations Symposium. 2008,51-65
[22] D. E. Bell, L. J. Lapadula. Secure Computer Systems: A Mathematical Model. Hanscom AFB, Bedford, MA, Rep. FSD-TR- 73-278, vol. 1, ESD/AFSC. 1973
[23] K. J. Biba. Integrity Considerations for Secure Computer System. Technical Report ESD-TR-. 76-372, MTR-3153, The MITRE Corporation. 1977
[24] L. Badger, D. F. Sterne, D. L. Sherman, K. M. Walker, S. A. Haghighat. A Domain and Type Enforcement Unix Prototype. Proceedings of the Fifth USENIX UNIX Security Symposium. 1995,127-140
[25] D. D. Clark, D. R. Wilson. A Comparison of Commercial and Military Computer Security Policies. Proceedings of the IEEE Symposium on Security and Privacy. 1987, 184~194
J. Park, R. Sandhu. The UCONABC Usage Control Model. ACM Transactions on Information and System Security. 2004, 7(1):128 -174
J. K. Millen, Finite-State Noiseless Covert Channels. Proceedings of Proceedings of the Computer Security Foundations Workshop. 1989,81-86
[28] D. Denning, Cryptography and Data Security. Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA, 1982
J. K. Millen, Covert Channel Capacity. Proceedings of IEEE Symposium on

Research in Security and Privacy. 1987,60-66
J. Mclean, Security Models and Information Flow. Proceedings of IEEE Computer Society Symposium on Security and Privacy. 1990, 180-187
J. W. Gray III. Toward a Mathematical Foundation for Information Flow Security. Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy. 1991, 21-34
[32] D. Clark, S. Hunt, P. Malacaria. A Static Analysis for Quantifying Information Flow in a Simple Imperative Language. Journal of Computer Security，2007,15(3):321-371
[33] G. Smith. On the Foundations of Quantitative Information Flow. Lecture Notes in Computer Science. 2009,5504:288-302
[34] M. R. Clarkson, A. C. Myers, F. B. Schneider. Belief in Information Flow. Proceedings of Computer Security Foundations,(CSF05). 2005,31-45
[35] S. Hamadou, V. Sassone, C. Palamidessi. Reconciling Belief and Vulnerability in Information Flow. Proceedings of IEEE Symposium on Security and Privacy (SP). 2010,79-92
[36] A. Aldini, D. Pierro. A Quantitative Approach to Noninterference for Probabilistic Systems Electronic Notes in Theoretical Computer Science. 2004, 99(6):155-182
[37] A. Aldini, D. Pierro. Estimating the Maximum Information Leakage. International Journal of Information Security. 2008, 7(3):219-242
[38] Pierro A D, Hankin C, Wiklicky H. Approximate Non-Interference. Journal of Computer Security. 2004, 12:37-82
[39] G. YunChuan, Y. Lihua, Z. Yuan, L. Chao, G. Li, Simulation Analysis of Probability Timing Covert Channels. Proceedings of IEEE International Conference on Networking, Architecture, and Storage (NAS 2009) 2009,325-332
[40] H. Yasuoka, Terauchi T. Quantitative Information Flow-Verification Hardness and Possibilities. Proceedings of IEEE Computer Security Foundations Symposium (CSF),. 2010,15-27
[41] B. Kŏpf, D. Basin. An Information-Theoretic Model for Adaptive Side-Channel Attacks. Proceedings of the 14th ACM conference on Computer and communications security 2007, 286-296
[42] M. R. Clarkson, F. B. Schneider. Quantification of Integrity. Proceedings of IEEE Symposium on Computer Security Foundations. 2010,28-43
[43] B. Littlewood, S. Brocklehurst, N. Fenton, P. Mellor, S. Page, D. Wright, J. Dobson, J. McDermid, D. Gollmann. Towards Operational Measures of Computer Security. Journal of Computer Security, 1993,2:211-229
[44] L. Lamport, R. Shostak, M. Pease. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems. 1982, 4 (3):382-401
[45] M. Gasser. Building a Secure Computer System, 1988
[46] R. S. Sandhu. Lattice-Based Access Control Models. IEEE Computer. 1993, 26(11):9-19
[47] 郑志蓉，蔡谊，沈昌祥. 基于多级安全策略的二维标识模型. 计算机学报. 2004, 27(5):619-624
[48] 沈昌祥，李益发. 一种新的操作系统安全模型. 中国科学 (E 辑, 信息科学). 2006,

36(4):347~356
[49] 刘威鹏，张兴. 基于非传递无干扰理论的二元多级安全模型研究. 通信学报. 2009, 39(2):52-58
[50] N. Heintze, J. G. Riecke. The Slam Calculus: Programming with Secrecy and Integrity. Proceedings of the 25th ACM SIGPLAN-SIGACT symposium on Principles of programming languages. 1998,
[51] P. LI, S. Zdancewic. Unifying Confidentiality and Integrity in Downgrading Policies. Proceedings of the LICS' 05 Affiliated Workshop on Foundations of Computer Security (FCS). 2005,45-54
[52] S. Jha, R. Linger, T. Longstaff, J. Wing. Survivability Analysis of Network Specifications. Dependable Systems and Networks, New York, USA, IEEE Press, 2000:613~622
[53] Y. Liu, K. S. Trivedi. A General Framework for Network Survivability Quantification. the 12th GI/ITG Conference Measuring, Modeling and Evaluation of Computer and Communication Systems, Dresden, Germany, 2004,369~378
[54] D. Chen, S. Garg, K. S. Trivedi. Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc Networks. the 5th ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2002) , Atlanta, 2002,61~68
J. McDermott. Attack-Potential-based Survivability Modeling for High-Consequence Systems. the 3rd IEEE International Workshop on Infromation Assureance (IWIA' 05), Callege Park, Maryland, USA, 2005,119~130
[56] M. Dacier, Y. Deswarte, M. Kaaniche. Models and tools for quantitative assessment of operational security. Information systems security: facing the information society of the 21st century, 1996, 177 -
[57] R. Lanotte, A. Schettini, A. Troina. A Classification of Time and/or Probability Dependent Security Properties. Electronic Notes in Theoretical Computer Science.2006, 153(177-193)

Author Biographies

Guo Yunchuan: Ph.D. candidate, Information Security Research Center, Institute of Computing Technology, Chinese Academy of Sciences

Yin Lihua: Postdoctoral researcher, Information Security Research Center, Institute of Computing Technology, Chinese Academy of Sciences. Email: yinlihua@software.ict.ac.cn

Liu Licai: Ph.D. candidate, Information Security Research Center, Institute of Computing Technology, Chinese Academy of Sciences

Note: Figure translations are in progress. See original paper for figures.