2006 年 ACM Symposium on Information, Computer and Communications Security (資訊、電腦與通訊安全國際會議)

結案報告書

指導單位：行政院科技顧問室、國家資通安全會報

主辦單位:　**Association for Computing Machinery (ACM)**

共同主辦單位：國科會、教育部、交通大學、中央研究院、工研院、中華民國資訊安全學會

承辦單位: 國立交通大學、中央研究院、中華民國資訊安全學會、工業技術研究院

申請人：　中央研究院李德財所長/院士

國立交通大學資工系謝續平教授

聯絡地址: 新竹市大學路 1001 號　國立交通大學資工系

聯絡人:　交通大學資工系教授/國立交通大學資通安全研究與教學中心主任謝續平

聯絡電話: (03) 573-1876

E-mail: ssp@csie.nctu.edu.tw

目錄

一、會議前言

ACM 是全世界在資訊與電腦領域中最具權威的學術組織，而 ACM 資訊安全委員會（Special Interest Group on Security, Audit, and Control）轄下兩大資訊安全會議，其一即為本研討會。

2006 年 ACM 資訊、電腦與通訊安全國際會議於 2006 年 3 月 20 日到 3 月 24 日在台北國際會議中舉行。討論議題包括 Access control and authorization、Electronic privacy, anonymity、Authentication, biometrics, smartcards、Information flow、Watermarking and data hiding、Intrusion detection and survivability、Applied cryptography、Digital Right Management、Data integrity and audit、Mobile code and mobile agent security、Database security、Network security、Distributed systems security、Formal verification and testing、Wireless communications、Security protocols、E-commerce and mobile e-commerce 和 Viruses and other malicious code… 等。議程委員會收到 26 個國家將近兩百篇的論文，論文接受率只有 16%，在目前許多知名國際 ACM、IEEE 研討會中，為論文接受率極低者，能於本會報告之論文將會是國際資訊安全領域中相當傑出之作品。此外，本會並邀請國際資訊安全之六位相當知名國際學者來给大會進行演講，與國內資訊安全之先進交換研究心得。

預期可以達到以下成效

- 與會人員可以瞭解電腦通訊安全相關各領域理論及應用研究的最新進展。
- 與會人員可以交換研究果成經驗與心得。
- 國內相關研究成果可以讓國際人士瞭解。
- 國外知名專家提供新觀念與技術指導。
- 國外學者專家與會可了解國內電腦通訊安全發展情形，提昇國際知名度。

二、ACM 簡介

Association for Computing Machinery (簡稱 ACM)成立於 1947 年，是世界上第一個也是最富盛名與學術聲望的資訊領域學術組織，全球約有 80000 名會員。ACM 的研究領域包含 computers, information technology, communications、computer networks、network standard 等，其下有許多 Special Interest Group(簡稱 SIG)分別在探討各個相關領域的研究，每個 Special Interest Group 下轄數個重要 Conferences。每個 Conference 每年都會公開徵求世界各地的相關研究，經過評審審核後發表，並舉辦座談會讓全球的會員們交流意見，另外也會固定發行期刊各 Conference 最新的 paper。

ACM 共有下列 Special Interest Groups

SIGACCESS	Accessibility and Computing
SIGACT	Algorithms and Computation Theory
SIGAda	Ada Programming Language
SIGAPL	APL Programming Language
SIGAPP	Applied Computing
SIGARCH	Computer Architecture
SIGART	Artificial Intelligence
SIGBED	Embedded Systems
SIGCAS	Computers and Society
SIGCHI	Computer-Human Interaction
SIGCOMM	Data Communication
SIGCSE	Computer Science Education
SIGDA	Design Automation
SIGDOC	Systems Documentation
SIGecom	Electronic Commerce
SIGGRAPH	Computer Graphics
SIGGROUP	Groupware
SIGIR	Information Retrieval
SIGITE	Information Technology Education
SIGKDD	Knowledge Discovery in Data
SIGMETRICS	Measurement and Evaluation
SIGMICRO	Microprogramming/Microarchitecture
SIGMIS	Management Information Systems
SIGMM	Multimedia
SIGMOBILE	Mobility of Systems, Users, Data & Computing
SIGMOD	Management of Data
SIGOPS	Operating Systems
SIGPLAN	Programming Languages

SIGSAC	Security, Audit & Control
SIGSAM	Symbolic and Algebraic Manipulation
SIGSIM	Simulation & Modeling
SIGSOFT	Software Engineering
SIGUCCS	University & College Computing Services
SIGWEB	Hypertext, Hypermedia and Web

其中 SIGSAC 的研究重點在於發展電腦、通訊、網路和資訊安全，包含電腦存取控制、認證方法、密碼學、入侵檢測系統、風險分析、和安全協定，另外一個大方向是系統安全，包括作業系統、資料庫、分散式系統、網路系統以及中介軟體…等。下轄國際知名期刊 ACM Transactions on Information and System Security，與主要兩個國際知名頂級學術 conferences：

ACM Conference on Computer and Communications Security
ACM Symposium on Information, Computer and Communications Security

ACM Symposium on Information, Computer and Communications Security 即為本次在台舉辦會機。

三、會議目的

主要提供一個公開討論的場合, 充分交換研究成果, 以提昇電腦通訊安全相關領域理論研究及應用研究。參與會議的成員來自國內外大學教授、學術界知名學者及科技研究單位。今年會議主題涵蓋 Access control and authorization、Electronic privacy, anonymity、Authentication, biometrics, smartcards、Information flow、Watermarking and data hiding、Intrusion detection and survivability、Applied cryptography、Digital Right Management、Data integrity and audit、Mobile code and mobile agent security、Database security、Network security、Distributed systems security、Formal verification and testing、Wireless communications、Security protocols、E-commerce and mobile e-commerce 和 Viruses and other malicious code… 等相關領域。藉著本國際性會議的舉辦不僅可以達到上述促進國際學術交流、提昇密碼學相關領域研究應用、促進國際學術交流的目的，對國內學術提昇有具體貢獻外，亦可展現國內學術研究成果。

四、舉辦日期、地點

日期：民國九十五年三月二十日(星期一)至三月二十四日(星期五) 共五天
地點：台北君悅飯店

五、指導單位

行政院科技顧問室、國家資通安全會報

六、主辦單位

Association for Computing Machinery (ACM)

七、共同主辦單位

教育部、國科會、中央研究院、交通大學、工研院、中華民國資訊安全學會

八、籌備委員會

大會榮譽主席	行政院林逢慶政務委員	
大會主席	李德財，中研院院士暨資訊所所長 林寶樹，工研院電通所所長	
議程主席	謝續平 交通大學、中華民國資安學會 S. Jajodia, GMU (ACM SIGSAC chair)	確認整個會議議程的內容與進行方式，含 Call-for-Paper，Paper review，篩選邀請各 Session Speakers & Panelists 等。 提供出版委員會主席整個會議進行的內容。
Treasurer Chairs	劉培文，資策會 彭仁剛，國安局 吳宗成，台灣科技大學 何全德，研考會	提出募款計畫書，負責找到支援 ACM 各項活動的贊助者，包含與預期的贊助者簽定合約、贊助保證邀約書。 維持及傳遞各種募款記錄資料、適時的轉交發票資料給財務長。
Local arrangement chairs	鄭仁傑，工研院 雷欽隆，台灣大學、葉義雄，交通大學	主要負責相關會議室、宴會廳、展示室、委員會議室、旅館等預訂及 ACM 所有活動的安排。 ACM 活動期間，須負責櫃檯運作及財務安全，並確保櫃檯服務時間，服務人員盡忠職守。 負責會議參加報名、及協助財務做帳及財務報表。 預估 ACM 各項活動的參加人數予大會主席。 安排 Local Tour。 會場架設 ADSL 無線上網。
Public relation chairs	李惠慈，工研院 黃育綸，交通大學 陳榮傑，交通大學	負責 ACM 舉辦前或進行中各項活動的協調與宣傳。 負責新聞發佈／媒體宣傳。 偕同 Organizer、出版委員會主席一起推銷 ACM 於產、學、研、政、各界。 寄印海報
Publication	曾慧琦，中研院	負責協調、編輯校訂、出版、及分配銷售

chairs	曾文貴，交通大學	相關會議印刷品（Final Program, Proceedings & Rump Session）等事宜，其他委員會主席及相關人員可適時協助。 議程委員會接受通過的稿件，不論是邀稿或是自行投稿，都應在會議議程中被刊登。 所有的印刷物須有特定公司提供會議出版的商定支援。 提供參加者即時的會議資訊及會議議程。
Registration Chairs	黃世昆，交通大學 王秋鳳，中研院	網頁維護、設計 註冊系統、自動回覆系統、收據列印 Travel Guide 可放上網頁
Secretariat Chairs	楊明豪，交通大學 許騰尹，交通大學 彭文志，交通大學	負責籌辦期間籌備會召開、會議記錄整理。 預算編列與掌控。 負責協調財務會計控制預算及支出。 負責協調、編輯校訂、刊載、及所有相關 ACM 所有委員會網頁。

九、指導委員

Virgil Gligor（U of Maryland,USA）
Li Gong (Sun Microsystems, USA)
Pradeep Khosla (Carnegie Mellon University)
Shankar Sastry (University of California at Berkeley)
呂學錦（中華電信公司）
杜紫軍（商業司）
林進燈（交通大學）
林勤經 (國防部資源司)
吳重雨 (交通大學)
紀國忠 (國科會)
柯志昇 (資策會)
陳昭義（工業局）
陳文村（台灣聯大、清華大學）
陳俊麟 (行政院研考會)
黃重球（技術處）
黃磊　（國安局）
張俊彥 (交通大學)
張進福（暨南大學）
張真誠（逢甲大學）
賴溪松（成功大學）
簡仁德 (電信總局)

十、推動委員會(Steering Committee)

Virgil Gligor, University of Maryland, College Park, USA
Sushil Jajodia, GMU,USA
Pierangela Samarati, U of Milano, Italy
Robert Deng, SMU, Singapore
Shiuhpyng Shieh, National Chiao Tung University, Taiwan (Chair)
Hiroshi Imai, Department of Computer Science University of Tokyo

十一、議程委員會(Program Committee)

1. Vijay Atluri, Rutgers U, USA
2. Aditya Bagchi, ISI, India
3. Hao Chen, UC Davis, USA
4. Kefei Chen, Shanghai Jiaotung U, PRC
5. Tsuhan Chen, CMU, USA
6. Ed Dawson, QUT, AU
7. Robert Deng, SMU, Singapore
8. Yvo Desmedt,UCL&FSU, UK
9. Wenliang Du, Syracuse U, USA
10. Simon Foley, U College Cork, Ireland
11. Virgil Gligor, U of Maryland, USA
12. Dieter Gollmann, TUHH, Germany
13. Ravi Iyer, UIUC, USA
14. Pradeep Khosla, CMU, USA
15. Kwangjo Kim, ICU, Korea
16. Michiharu Kudoh, IBM Tokyo Lab, Japan
17. Chi-Sung Laih, ChenKung U, Taiwan
18. Kwok-Yan Lam, Tsinghua U, PRC
19. Chin-Laung Lei, Taiwan U, Taiwan
20. Peng Liu, Penn State U, USA
21. Sharad Mehrotra UC Irvine, USA
22. Jonathan Millen, MITRE, USA
23. Peng Ning, NC State U, USA
24. Eiji Okamoto, U of Tsukuba, Japan
25. Jean-Jacques Quisquater, UCL, Belgium
26. Mike Reiter, CMU, USA
27. Rei Safavi-Naini, U Wollogong, AU
28. Pierangela Samarati, U of Milano, Italy
29. Ravi Sandhu, GMU, USA

30. R. Sekar, Stony Brook U, USA
31. Hovav Shacham, Standford U, USA
32. Sean Smith, Dartmouth, USA
33. Dawn Song, CMU, USA
34. Michael Steiner, IBM, Germany
35. Wen-Guey Tzeng, Chiao Tung U, Taiwan
36. Doug Tygar, UC Berkerley, USA
37. Vijay Varadharajan, UWS, AU
38. Huaxiong Wang, Macquarie U, AU
39. Victor Wei, Chinese U of HK, HK
40. Felix Wu, UC Davis, USA
41. Tzong-Chen Wu, NTUST, Taiwan
42. Moti Yung, Columbia U, USA

十二、參加對象及國家

此會議 ACM Symposium on Information, Computer and Communications Security 由 ACM Conference Computer and Communication Security 所衍生新成立,，依 ACM Conference Computer and Communication Security 過去經驗來預測，此會議參與人員，國外人士有大約 160 人參加，包括來自歐洲、美洲、亞洲地區等二十餘國學者專家，國家計有法國、英國、美國、加拿大、日本、比利時、中國大陸、丹麥、新加坡、韓國、印度、波蘭、捷克、義大利、西班牙、瑞士、德國、奧地利、芬蘭、瑞典、以色列、香港、馬來西亞、紐西蘭、澳州等國從事資訊安全相關研究之專家學者，而國內與會人員大約有 150 人，將包括各大學院校、研究機構及軍方從事相關領域之教授、研究生及研究人員等，預估全部有超過 300 人與會(含未報名者)。下表為參加本次會議的國家各國人數統計：

日本	23	台灣	150
紐西蘭	4	韓國	24
法國	9	新加坡	6
英國	5	瑞士	3
比利時	1	德國	4
美國	17	義大利	3
印度	2	泰國	2
加拿大	2	中國大陸	7
澳洲	15	以色列	5
丹麥	5	波蘭	4
捷克	3	西班牙	3
奧地利	4	芬蘭	2
瑞典	2	香港	9

十三、會議議程

會議議程簡表

Date		
3/20/2006 (Monday)	7:00-9:00pm	Registration and reception at the Grand Hotel, Taipei, Taiwan
3/21/2006 (Tuesday)	8:30- 9:00am	Registration and welcome drinks and nibbles at the Grand Hotel, Taipei, Taiwan
	9:00- 9:20	Opening remarks (Minister Lin, general chairs, program chairs)
	9:20-10:10	Distinguish Lecture by Virgil Gligor (簡歷如附件五)
	10:10-10:30	Coffee Break
	10:30-12:10	Session 1 (4 papers)
	12:10-1:10	Lunch
	1:10-2:50	Session 2 (4 papers)
	2:50- 3:10	Coffee Break
	3:10- 4:30	Session 3 (3 papers)
	4:30-5:00	Break (moving to the Taipei 101 for rump session)
	5:00-6:40	Rump Session (20 Fast Abstract)
	7:00-9:00	Reception
3/22/2006 (Wednesday)	8:30-9:20	Invited Talk (1) by Prof. Doug Tygar (簡歷如附件四)
	9:20-10:10	Session 4 (2 papers)
	10:10-10:30	Coffee Break
	10:30-12:10	Session 5 (4 papers)
	12:10-1:10	Lunch
	1:10-2:00	Invited Talk (2) Prof. Michael Reiter (簡歷如附件三)
	2:00-2:50	Session 6 (2 papers)
	2:50- 3:10	Coffee Break
	3:10- 4:50	Session 7 (4 papers)
	6:00-9:00	Banquet
3/23/2006 (Thursday)	8:30-9:20	Invited Talk (3) Ravi Sandhu (簡歷如附件二)
	9:20-10:10	Session 8 (2 papers)
	10:10-10:30	Coffee Break
	10:30-11:20	Invited Talk (4) Prof. S. Jajodia (簡歷如附件一)

	11:20-12:10	Session 9 (2 papers)
	12:10-1:10	Lunch
	1:10-1:50	Session 10 (2 papers)
	1:50-2:40	Invited Talk (4) Jeannette Wing (簡歷如附件六)
	2:40- 3:00	Coffee Break
	3:00- 4:50	Session 12 (4 papers)
3/24/2006 (Friday)	8:30am – 5:00pm	Excursion to National Palace Museum, Science Park, III, ITRI

十四、會議籌備過程

年度	日期	預定之工作
2004	12 月	確定會議地點並預訂場地
		籌備會前會議
2005	2 月	組成籌備委員會
	3 月	第一次籌備會議
	4/1	Call For Paper
		線上投稿系統完成
	5/1	網站正式上線
	7/1	議程委員會 (共 42 位委員), 並陸續邀請中
	8/1	線上審稿系統完成
	10/1	投稿截止
	11/1	線上註冊系統
	11/20	通知論文審查結果, 開始受理註冊
	12/10	論文集排版完成
2006	2/20	早期註冊截止
	2/28	議程確定
	3/20	完成場地佈置
	3/21	會議開始
	3/25	會議期間
	7/30	處理會後相關事宜，報帳相關事宜
	9/30	召開檢討會議，準備繳交會議成果相關資料給 ACM
	11/10	參加 ACM SIGSAC 年會，繳交報告，報告會議成果
	12/31	計畫結案

十五、執行成效

ACM 是世界上第一個也是最富盛名的資訊領域的國際組織，此次相當難得可以爭取到 ACM 於資訊安全最重要之兩個研討會之一的 ACM Symposium on Information, Computer and Communications Security 來台舉辦，使國內資訊安全學者可以有機會不必出國即可參與國際一流之學術研討會。目前議程委員會已收到 25 個國家將近兩百篇的論文，論文接受率只有 16%，在目前許多知名國際 ACM、IEEE 研討會中，為論文接受率極低者，能於本會報告之論文將會是國際資訊安全領域中相當傑出之作品。此外，本會並邀請國際資訊安全之六位相當知名學者來给大會進行演講，與國內資訊安全之先進交換研究心得。

預期可以達到以下成效

- 與會人員可以瞭解電腦通訊安全相關各領域理論及應用研究的最新進展。
- 與會人員可以交換研究果成經驗與心得。
- 國內相關研究成果可以讓國際人士瞭解。
- 國外知名專家提供新觀念與技術指導。
- 國外學者專家與會可了解國內電腦通訊安全發展情形，提昇國際知名度。

十六、議會過程簡介

3/20 各項工作人員於下午約 1:30 抵達會場進行準備工作。

於晚間 6:30 工作準備就緒，7:00 正式接受 Pre-registration。

3/21 本日為 conference 第一日，許多著名國內、外學者齊聚一堂，盛況空前。

8:00 於台北君悅大飯店，開始接受 registration。

9:00 由林寶樹 所長(Minister Lin)、李德財 院士(General Chair)、謝續平教授(Program Chair)、Sushil Jajodia(Program Chair)等人發表開場演說。

9:20 由 ACM SIGSAC 主席暨 2005 年 Information Security Award 得主－Virgil D. Gligor 發表著名的演說，題目為”Emergent Properties in Ad-Hoc Networks: A Security Perspective”。

10:00 Coffee Break

10:20 Session 1 在會議主席－Wenke Lee 的主持下正式開始，這個 Session 主要談論與 Security Protocols 相關的議題，包括：

1. ”Improving Secure Server Performance by Re-balancing SSL/TLS Handshakes.”
2. ”Provably Secure Password-Based Authentication in TLS”
3. ”Certified Mailing Lists.”
4. ”Designated Group Credentials.”

12:00 午餐招待

13:00 Invited Talk 在 Pierangela Samarati 的主持下開始，由前 ACM SIGSAC 主席－Ravi Sandhu 帶來一場精采的演講，題目為”Secure Information Sharing Enabled by Trusted Computing and PEI Models”.

13:40 Session2 在會議主席－Pierangela Samarati 主持下開始，這個 Session 主要討論與 Database Security 相關的議題，包括：

1. “Privacy-preserving Semantic Interoperation and Access Control of Heterogeneous Databases”
2. “Publicly Verifiable Ownership Protection for Relation Databases”

14:30 Coffee Break

14:50 Session3 在會議主席－Rei Safavi-Naini 的主持下開始，這個 Session 主要討論與 Intrusion Detection and Modeling 相關的議題，包括：

1. “Measuring Intrusion Detection Capacity: An Information-Theoretic Approach”
2. “Time Series Modeling for IDS Alert Management”
3. “Augmenting Storage with an Intrusion Response Primitive to Ensure the Security of Critical Data”
4. “Design Space and Analysis of Worm Defense Strategies”

16:30 由台北君悅大飯店移動到台北 101 的會場，沿途有專人指示行走路徑。

17:00 Fast Abstract Session 於台北 101 正式舉行，會議主席為 Robert Deng，

這個會議總共有四個主題，討論與 Multimedia Security、Network Security、Digital Signature、Cryptosystem 相關的議題，包括：

- Multimedia Security：
  1. “Digital Invisible lnk: Revealing True Secrets via Attacking”
  2. “Quadtree based Perceptual Watermarking Scheme”
  3. “Continuous Fingerprint Classification By Symmetrical Filters ”
- Network Security：
  1. “A General Design Towards Secure Ad-Hoc Collaboration”
  2. “A Distributed Key Assignment Protocol For Multicast Based on Proxy Cryptography”
  3. “An Efficient Secure Communication Between Set-top Box and Smart card in DTV Broadcasting”
  4. “Forgery Attack on the RPC Incremental Unforgeable Encryption Scheme”
  5. “A Control Flow Obfuscation Method to Discourage Malicious Tampering of Software Codes”
  6. “Problems on the MR Micropayment Schemes”
  7. “Design and Implementation of a Reconfigurable Hardware for Secure Embedded Systems”
- Digital Signature：
  1. “Democratic Group Signatures”
  2. “Analysis of Traceability Attack on Camenisch et al.’s Blind Signature Scheme”
  3. “Restricted Message Signing”
- Cryptosystem：
  1. “Policy-based Encryption Schemes from Bilinear Pairings”
  2. “A Refined Look at Bernstein’s AES Side-Channel Analysis”

19:00 於台北 101 享用晚餐.

21:00 結束第一日的會議行程

3/22 本日為 conference 第二日。

8:30 於君悅飯店，開始接受 registration。

9:00 Session 4 正式開始，主題為 P2P& Ad Hoc Networks, 會議主席為 Jean-Pierre Seifert，其中內容包含：

1. “Self-Organized Group Key Management for Ad Hoc Networks”
2. “Lightweight, Pollution-Attack Resistant Multicast Authentication Scheme” 進行演講。

9:50 邀請 Jean-Pierre Seifert 進行 invited talk，題目為 ” TRUST: In Cyberspace and Beyond” 。

10:30 Coffee Break

10:50 Session 5 正式開始，由 Wen-Guey Tzeng 主持，主題為：Digital Rights Management and Watermarking, 內容有：

1. “An Attack-Localizing Watermarking Scheme for Natural Language Documents”
2. ”Tamper Proofing and Attack Identification of Corrupted Image by using Semi-fragile Multiple-watermarking Algorithm”
3. “Image-Adaptive Watermarking Based in Perceptually Shaping Watermark Blockwise”
4. “Finding the Original Point Set Hidden among Chaffs”

12:30 Lunch

13:15 進行 Invited talk，由 Bao Feng 發表 “Attack graph Generation and Analysis” 演說。

13:55 Session 6 正式開始，主題為 Software security, 議會主席為 Bao Feng，討論內容有：

1. “Software Integrity Protection Using Timed Executable Agents”
2. “Application Security Support in the Operating System Kernel”

14:45 Coffee Break

15:05 Session 7 正式開始,由 Hiroaki Kikuchi 主持,主題為 Access Control and Authentication,題目有：

1. “Supporting Location-Based Conditions in Access Control Policies”
2. ”A Secure System for Data Access Based in Anonymous Authentication and Time-Dependent Hierarchical Keys”
3. “Approvability”
4. “Safety Analysis of Usage Control Authorization Models”.

18:00 Banquet

3/23 本日為 conference 第三日。

8:30 於君悅飯店，繼續接受 registration。

9:00 Session 8 正式開始，會議主席為 Bodo Moller，討論主題為 Authentication and Biometrics， 內容包括：

1. “Fortifying Passwrod Authentication in Integrated Healthcare Delivery Systems”
2. “Collusion Secure Convolutional Fingerprinting Information Codes”

9:20 開始 Invited Talk 由 Bodo Moller 主持，由 Ravi lyer 講解 “Security Vulnerability: From Measurements to Design”

10:30 Coffee Break

10:50 Session 9 正式開始，主題為 Cryptosystem and Analysis，由 Tzong-Chen Wu 擔任主席，內容包括：

1. “Sridharan Anand Present “Periodicity, Complementarity and

Complexity of 2-adic FCSR Combiner Generators”

2. “Cryptanalysis of The Grain Family of Stream Ciphers”
3. “Addressing the Shortcomings of One-Way Chains”
4. “Ring Signature without Random Oracles”

12:30 午餐時間

13:15 開始 Invited Talk 在 Masahiro Mambo 主持下，由 Prof. Doug Tygar 發表 ”Can Machine Learning Be Secure?" 演說。

13:55 Session 10 正式開始，主題為 Wireless Sensor Networks，議會主席為 Masahiro Mambo，內容有：

1. “An Efficient Key Establishment Scheme for Secure Aggregating Sensor Networks”
2. “An Efficient Broadcast Authentitation Scheme in Wireless Sensor Networks”

14:45 Coffee Break;

15:05 Session 11 在 Peng Liu 主持下，正式開始主題為 Secure Routing and Firewall，討論內容有：

1. “Identity-Based Registry for Secure Interdomain Routing”
2. “Dynamic Rule-ordering Optimization or High-speed Firewall Filtering”
3. “Digitally Signed Document Sanitizing Scheme Based On Bilinear Maps”

16:20 由謝續平教授(Program Chair)及 Sushil Jajodia(Program Chair) 等人為研討會圓滿落幕，發表 Closing Remarks，並宣布下屆 ACM Symposium on Information, Computer and Communications Security 將在新加坡舉行。

3/24 此日為 Free tour 分成 half day tour 與 one day tour，由二位工作人員帶領許多外國學者參觀我國「故宮博物館」、「新竹工業技術研究院」以及「新竹科學園區」等等。

十七、與會名單統計資料

◆ 與會人員統計

1. 事前報名人數：220 人
2. 現場報名人數： 13 人
3. 現場應到人數：233 人
4. 現場實到人數：209 人，出席率：90%

◆ 各天報到狀況

ACM 各天報到狀況			
現場應到人數	233	實到人數	209
	人數	比率	
3 月 20 日報到者	18	9%	
3 月 21 日報到者	157	74%	
3 月 22 日報到者	16	8%	
3 月 23 日報到者	18	9%	
總人數	209		

十八、經費開銷

支出大項	支出項目	總額	細目	金額	備註
人事費用	人事費	1,142,000			
			專任助理	700,000	
			臨時工資	300,000	
			大會臨時工作人員	110,000	
			主持人費用	32,000	2,000/場*16
	合計	1,142,000			

支出大項	支出項目	總額	細目	金額	備註
業務費	印刷費	748,000			
			論文集	400,000	
			海報(大)	90,000	
			Call For Paper 印刷	30,000	30 元/張*1,000 張
			Call For Participation	48,000	
			大會手冊	90,000	150 元/份*600 份
			Final Program Brochure	90,000	
	餐飲費	2,709,000			

			晚宴(含飲料，服務費)	264,000	8,800 元/桌(10 人)*30 桌
			晚餐(Rump Session)(含飲料，服務費)	440,000	22,000 元/桌(12 人)*20 桌
			場地租用費(含服務費、午餐及每日兩次點心及稅金	1,980,000	300 人*2,200*3 天
			SIGSAC 技術委員會議場地費	25,000	
業務費	場地器材租用費	300,000			
			記錄費(含照相.錄影.音控等)	80,000	2,000 元/天*4 天
			麥克風喇叭 NB 租借費	100,000	
			場地佈置費	120,000	
	旅運費	200,000			
			國外差旅費	120,000	
			國內差旅費	80,000	
	耗材費	270,000			
			影印及印刷費	200,000	
			光碟片、磁片	20,000	
			碳粉匣等	30,000	
			消費性器材	20,000	
	交通費與膳雜宿費	1,798,000			

			受邀海外來賓生活費	420,000	10,000 元/人*6 人*7 天
			受邀海外傑出學者機票費 (商務艙)	1,200,000	(Dr. S. Jajodia, former Chair of ACM SIGSAC & Prof. Of GMU; Dr. Doug Tygar, Prof. Of UC Berkeley & Chair of the Defense Department's ISAT Study Group on Security with Privacy; Dr. Michael Reiter, Prof. Of CMU & Editor in-Chief of ACM TISSEC; Dr. Ravi Sandhu, Prof. Of GMU & former Editor-in-Chief of ACM TISSEC & ACM & IEEE fellows; Virgil Gligor, newly elected ACM SIGSAC chair & Prof. Of Univ. of Maryland; Jeannet Wing, IEEE fellow & Prof. & Chair Of CMU) 200,000 元/人*6 人
			國內專家受邀演講費	18,000	6,000/人*3 人
			國內交通費（遊覽車）	160,000	10,000 元*4*4 天
業務費	工作會	660,000			
			籌備會	360,000	20,000 元/次*18 次
			檢討會	300,000	
	大會網站製作與維護費	450,000			
			網站維護費	150,000	
			網頁製作費	150,000	

			程式設計費	150,000	
	郵電、文具	237,500			
			郵電費(含海外聯繫費)	65,000	
			文具、紙張	172,500	
	紀念品	500,000			
			紀念品	500,000	紀念品 1000 元/人份*500 份
	晚宴表演費	300,000			
			表演費	300,000	
業務費	參觀景點費（認識台灣）	390,000			參觀故宮、科學園區，增進國外人士認識台灣的文化與科技發展
			參觀費	390,000	1,500 元/人*260 人 (餐費及當天導遊費用)
	補助國外學者費	200,000			
			補助貧困地區國外優秀作者（學生或學者）前來發表論文	200,000	20,000 元/人*10 人
	補助國內學生費	840,000			
			由於 ACM 國際會議報名費較高，國內學生較難負擔，故補助國內學生報名費，以鼓勵學生參加難得在台灣舉辦的國際會議。	840,000	12,000 元/人*70 人（約 20 個學校，每個學校 3-4 名學生參加）
	最佳論文獎金	100,000			

			補助最佳論文獎得主費用	100,000	50,000 元/人*2 人
	雜支	250,000			
	給 ACM 費用	600,000	依 ACM 規定，支付 ACM 相關費用	600,000	
	合計	10,552,500			

總計	11,694,500

十九、擬請補助經費明細表

支出項目	細目	金額	備註
人事費	補助人事費	222,000	由教育部補助款支出，單據留存備查(部分補助)
業務費	交通費與膳雜宿費(邀請國外知名 invited speaker 費用)	810,000	(商務艙機票 200,000＋生活費 70,000)＊3 人，由教育部補助款支出，單據留存備查(部分補助)
	補助國內學生(由於 ACM 國際會議報名費較高,國內學生較難負擔,故補助國內學生報名費,以鼓勵學生參加難得在台灣舉辦的國際會議。)	840,000	補助國內各大學研究所碩博士班學生，每人 12000＊70 人，由教育部補助款支出，單據留存備查
	最佳論文獎補助	100,000	由教育部補助款支出，單據留存備查
	大會網站製作與維護費	250,000	由教育部補助款支出，單據留存備查(部分補助)
	郵電、文具	168,000	由教育部補助款支出，單據留存備查(部分補助)
	場地租用費	350,000	由教育部補助款支出，單據留存備查(部分補助)
合計		2,740,000	

二十、研討會發表論文之審稿制度

論文審查程序依照國際慣例由本研討會所組成之議程委員會以匿名審查方式，每篇論文將會指定三位審查委員審視所有投稿文章，並由議程委員會開會討論審查意見後決定接受發表之論文。

二十一、活動剪影

1. 註冊與研討會實況







Taipei, Taiwan
acm
SIGSAC
ACM Symposium on InformAtion, Computer
and Communications Security (ASIACCS'06)


acm
SIGSAC
ACM Symposium on

2.餐宴與活動實況


SIGSAC


acm
SIGSAC


acm
SIGSAC
Taipei, Taiwan
ium on InformAtion, Computer
cations Security (ASIACCS'06)
Banquet
Sponsored by


acm
SIGSAC
Taipei, Taiwan


acm
SIGSAC
Taipei, Taiwan
Symposium on InformAtion, Computer

二十二、主講/持人學經歷及著作一覽表

附件(一) Sushil Jajodia

Sushil Jajodia is BDM International Professor of Information Technology and the director of Center for Secure Information Systems at the *George Mason University*, Fairfax, Virginia. He served as the chair of the Department of Information and Software Engineering during 1998-2002. He joined GMU after serving as the director of the Database and Expert Systems Program within the Division of Information, Robotics, and Intelligent Systems at the *National Science Foundation.* Before that he was the head of the Database and Distributed Systems Section in the Computer Science and Systems Branch at the *Naval Research Laboratory,* Washington and Associate Professor of Computer Science and Director of Graduate Studies at the *University of Missouri, Columbia.* He has also been a visiting professor at the *University of Milan* and *University of Rome "La Sapienza", Italy* and at the Isaac Newton Institute for Mathematical Sciences, *Cambridge University, England.*

Dr. Jajodia received his PhD from the University of Oregon, Eugene. His research interests include information security, temporal databases, and replicated databases. He has authored five books, edited twenty two books, and published more than 250 technical papers in the refereed journals and conference proceedings. He received the 1996 Kristian Beckman award from IFIP TC 11 for his contributions to the discipline of Information Security, and the 2000 Outstanding Research Faculty Award from GMU's School of Information Technology and Engineering.

Dr. Jajodia has served in different capacities for various journals and conferences. He is the founding editor-in-chief of the *Journal of Computer Security* and on the editorial boards of *ACM Transactions on Information and Systems Security*, *International Journal of Cooperative Information Systems,* and *International Journal of Information and Computer Security*. He is the consulting editor of the *Kluwer International Series on Advances in Information Security*. He also serves as the chair of the *ACM Special Interest Group on Security, Audit, and Control (SIGSAC)* and the *IFIP WG 11.5 on Systems Integrity and Control.* He has been named a Golden Core member for his service to the IEEE Computer Society, and received International Federation for Information Processing (IFIP) Silver Core Award "in recognition of outstanding services to IFIP" in 2001. He is a past chairman of the IEEE Computer Society Technical Committee on Data Engineering. He is a senior member of the IEEE and a member of IEEE Computer Society and Association for Computing Machinery. The URL for his web page is http://csis.gmu.edu/faculty/jajodia.html.

List of Publications 1999 and beyond

AUTHORED BOOKS

1. Peng Ning, Sushil Jajodia, X. Sean Wang, Intrusion Detection in Distributed Systems: An Abstraction-based Approach, ISBN 1-4020-7624-X, Kluwer Academic Publishers, Boston, 2003, 156 pages.
2. Peng Liu, Sushil Jajodia Trusted Recovery and Defensive Information Warfare, ISBN 0-7923-7572-6, Kluwer Academic Publishers, Boston, 2002, 152 pages.
3. Neil F. Johnson, Zoran Duric, Sushil Jajodia, Information Hiding: Steganography and Watermarking - Attacks and Countermeasures, ISBN 0-7923-7204-2 Kluwer Academic Publishers, Boston, 2001, 137 pages.
4. Claudio Bettini, Sushil Jajodia, X. Sean Wang, Time Granularities in Databases, Data Mining, and Temporal Reasoning, ISBN 3-540-66997-3, Springer-Verlag, Berlin, July 2000, 226 pages.
5. Vijay Atluri, Sushil Jajodia, Binto George, Multilevel Secure Transaction Processing, ISBN 0-7923-7702-8, Kluwer Academic Publishers, Boston, November 1999, 144 pages.

EDITED BOOKS

1. Daniel Barbara, Sushil Jajodia, Applications of Data Mining in Computer Security, ISBN 1-4020-7054-3, Kluwer Academic Publishers, Boston, 2002, 252 pages.
2. Paul Ammann, Bruce H. Barnes, Sushil Jajodia, Edgar H. Sibley, eds., Computer Security, Dependibility, and Assurance: From Needs to Solutions , ISBN 0-7695-0337-3, IEEE Computer Society Press, Los Alamitos (1999), 224 pages.

EDITED PROCEEDINGS

1. Sushil Jajodia, Leon Strous, eds., Integrity and Internal Control in Information Systems VI, ISBN 1-4020-7900-1, Kluwer Academic Publishers, Boston, 2004, 272 pages.

2. Yves Deswarte, Frederic Cuppens, Sushil Jajodia, Lingyu Wang, Security and Protection in Information Processing Systems, ISBN 1-4020-8142-1, Kluwer Academic Publishers, Boston, 2004, 562 pages.
3. Yves Deswarte, Frederic Cuppens, Sushil Jajodia, Lingyu Wang, Information Security Management, Education, and Privacy, ISBN 1-4020-8144-8, Kluwer Academic Publishers, Boston, 2004, 328 pages.
4. Hideko S. Kunii, Sushil Jajodia, Arne Solvberg, eds., Conceptual Modeling - ER 2001, Springer Lecture Notes in Computer Science, Volume 2224, ISBN 3-540-42866-6, Springer, Berlin (2001), 614 pages. 2001.
5. Sushil Jajodia and Pierangela Samarati, eds., Proc. 7th ACM Conf. on Computer and Communications Security, ISBN 1-58113-203-4, ACM Press, New York, November 2000, 256 pages.
6. Sushil Jajodia, ed., Database Security XII: Status and Prospects, Kluwer Academic Publishers, Boston, 1999, 320 pages.

JOURNAL ARTICLES

1. Alberto Ceselli, Ernesto Damiani, Sabrina De Capitani di Vimercati, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati, "Modeling and assessing inference exposure in encrypted databases, *ACM Trans. on Information and System Security,* To appear.
2. Claudio Bettini, X. Sean Wang, sushil Jajodia, "Information release control: A learning-based architecture," *Journal on Data Semantics*, To appear.
3. Lingyu Wang, Duminda Wijesekera, Sushil Jajodia, “Cardinality-based inference control in data cubes,” *Journal of Computer Security,* Vol. 12, No. 5, 2004, pages 655-692.
4. Claudio Bettini, Sushil Jajodia, X. Sean Wang, Duminda Wijesekera, “Reasoning with advanced policy rules and its application to access control,” *International Journal on Digital Libraries,* Vol. 4, No. 3, November 2004, pages 156-170.
5. Kenneth Smith, Sushil Jajodia, Vipin Swarup, Jeffery Hoyt, Gail Hamilton, Donald Faatz, Todd Cornett, “Enabling the sharing of neuroimaging data through well-defined intermediate levels of visibility,” *NeuroImage,* Vol. 22, No. 4, August 2004, pages 1646-1656.
6. Duminda Wijesekera, Sushil Jajodia, Francesco Parisi-Presicce, Asa Hagstrom, “Removing permissions in the Flexible Authorization Framework,” *ACM Trans. on Database Systems,* Vol. 28, No. 3, September 2003, pages 209-229.

7. Alessandro Mei, Luigi V. Mancini, Sushil Jajodia, “Secure dynamic fragment and replica allocation in large-scale distributed file systems,” *IEEE Trans. on Parallel and Distributed Systems,* Vol. 14, No. 9, September 2003, pages 885-896.
8. Claudio Bettini, Sushil Jajodia, X. Sean Wang, Duminda Wijesekera, “Provisions and obligations in policy rule management,” *Journal of Network and Systems Management*, Vol. 11, No. 3, September 2003, pages 351-372.
9. Daniel Barbara, Rajni Goel, Sushil Jajodia, “A checksum-based corruption detection techniques,” *Journal of Computer Security,* Vol. 11, No. 3, 2003, pages 315-329.
10. Duminda Wijesekera, Sushil Jajodia, ``A propositional policy algebra for access control," *ACM Trans. on Information and System Security,* Vol. 6, No. 2, May 2003, pages 286-325.
11. Yingjiu Li, Peng Ning, X. Sean Wang, Sushil Jajodia, ``Discovering calendar-based temporal association rules," *Data and Knowledge Engineering,* Vol. 4, No. 2, 2003, pages 193-218.
12. Roberto Di Pietro, Luigi V. Mancini, Sushil Jajodia, "Providing secrecy in key management protocols for large wireless sensor networks," *Ad Hoc Networks,* Vol. 1, No. 4, 2003, pages 455-468.
13. Claudio Bettini, X. Sean Wang, and Sushil Jajodia, ``Solving multi-granularity temporal constraint networks," *Artificial Intelligence*, Vol. 140, No. 1/2, 2002, pages 107-152.
14. Paul Ammann, Sushil Jajodia, Peng Liu, ``Recovering from malicious transactions," *IEEE Trans. on Knowledge and Data Engineering,* Vol. 14, No. 5, September/October 2002, pages 1167-1185.
15. Sanjeev Setia, Sencun Zhu, Sushil Jajodia, ``A comparative performance analysis of reliable group rekey transport protocols for secure multicast, *Performance Evaluation,* Vol. 49, No. 1-4, September 2002, pages 21-41.
16. Claudio Bettini, Sushil Jajodia, X. Sean Wang, ``Temporal reasoning in workflow systems," *Distributed and Parallel Databases*, Vol. 11, No. 3, May 2002, pages 269-306.
17. Peng Ning, X. Sean Wang, Sushil Jajodia, ``An algebraic representation of calendars," *Annals of Mathematics and Artificial Intelligence,* Vol. 36, No. 1-2, September 2002, pages 5-38.
18. Yingjiu Li, Ningning Wu, Sushil Jajodia, X. Sean Wang, ``Enhancing profiles for anomaly detection using time granularities," *Jour. of Computer Security*, Vol. 10, No. 1/2, 2002, pages 137-157.
19. Peng Ning, Sushil Jajodia, X. Sean Wang, ``Design and implementation of a decentralized prototype system for detecting distributed attacks," *Computer Communications*, Vol. 25, No. 15, September 2002, pages 1374-1391.

20. Susan Chapin, Don Faatz, Sushil Jajodia, Amgad Fayad, ``Consistent policy enforcement in distributed systems using mobile policies," *Data & Knowledge Engineering,* Vol. 43, No. 3, December, 2002, pages 261-280.
21. Sushil Jajodia, Pierangela Samarati, Maria Luisa Sapino, V. S. Subrahmanian, ``Flexible support for multiple access control policies," *ACM Trans. on Database Systems*, Vol. 26, No. 2, June 2001, pages 214-260.
22. Peng Ning, Sushil Jajodia, Xiaoyang Sean Wang, ``Abstraction-based intrusion detection in distributed environments," *ACM Trans. on Information and System Security,* Vol. 4, No. 4, November 2001, pages 407-452.
23. Pierangela Samarati, Michael K. Reiter, Sushil Jajodia, ``An authorization model for a public key management service," *ACM Trans. on Information and System Security,* Vol. 4, No. 4, November 2001, pages 453-482.
24. Peng Liu, Peng Ning, Sushil Jajodia, ``Avoiding loss of fairness owing to failures in fair data exchange systems," *Decision Support Systems*, Vol. 31, No. 3, 2001, pages 337-350.
25. Sushil Jajodia, Vijaylakshmi Atluri, Thomas F. Keefe, Catherine D. McCollum, Ravi Mukkamala, ``Multilevel secure transaction processing," *Jour. of Computer Security*, Vol. 9, No. 3, 2001, pages 165-195.
26. Alexander Brodsky, Csilla Farkas, Sushil Jajodia, ``Secure databases: Constraints, inference channels, and monitoring disclosures," *IEEE Trans. on Knowledge and Data Engineering,* Vol. 12, No. 6, November/December 2000, pages 900-919.
27. I. Ray, L. V. Mancini, S. Jajodia, E. Bertino, ``ASEP: A secure and flexible commit protocols for MLS distributed database systems," *IEEE Trans. on Knowledge and Data Engineering*, Vol. 12, No. 6, November/December 2000, pages 880-899.
28. Indrakshi Ray, Paul Ammann, Sushil Jajodia, ``Using semantic correctness in multidatabases to achieve local autonomy, distribute coordination, and maintain global integrity," *Information Sciences,* Vol. 129, No. 1-4, December 2000, pages 155-195.
29. Peng Liu, Sushil Jajodia, Catherine D. McCollum, ``Intrusion confinement by isolation in information systems," *Jour. of Computer Security*, Vol. 8, No. 4, 2000, 243-279.
30. Peng Ning, X. Sean Wang, Sushil Jajodia, ``Modeling requests among cooperating intrusion detection systems," *Computer Communications*, Vol. 23, No. 17, November 2000, pages 1702-1715.
31. Luigi V. Mancini, Indrajit Ray, Sushil Jajodia, and Elisa Bertino, ``Flexible transaction dependencies in database systems," *Distributed and Parallel Databases*, Vol. 8, No. 4, October 2000, pages 399-446.

32. Peng Liu, Paul Ammann, and Sushil Jajodia, ``Rewriting histories: Recovering from malicious transactions," *Distributed and Parallel Databases*, Vol. 8, No. 1, January 2000, pages 7-40.
33. Chunru Zhang, Kwok-Yan Lam, Sushil Jajodia, ``Scalable threshold closure," *Theoretical Computer Science*, Vol. 226, 1999, pages 185-206.
34. S. Jajodia, P. Ammann, C. D. McCollum, ``Surviving information warfare attacks," *IEEE Computer*, Vol. 32, No. 4, April 1999, pages 57-63.
35. Sushil Jajodia, Catherine D. McCollum and Paul Ammann, ``Trusted recovery," *Communications of the ACM,* Vol. 42, No. 7, July 1999, pages 71-75.
36. E. Bertino, S. Jajodia, and P. Samarati, ``A flexible authorization mechanism for relational data management systems," *ACM Trans. on Information Systems*, April 1999, Vol. 17, No. 2, April 1999, pages 101-140.

ARTICLES IN REFEREED CONFERENCE AND WORKSHOP PROCEEDINGS

1. Lingyu Wang, Sushil Jajodia, Duminda Wijesekera, “Securing OLAP data cubes against privacy breaches,” *Proc. IEEE Symp. On Security and Privacy,* Oakland, CA, May 2004, pages 161-175 (Acceptance ratio 19/186).
2. Sencun Zhu, Sanjeev Setia, Sushil Jajodia, Peng Ning, “An interleaved hop-by-hop authentication scheme for filtering false data injection in sensor networks,” *Proc. IEEE Symp. On Security and Privacy,* Oakland, CA, May 2004, pages 259-271 (Acceptance ratio 19/186).
3. Shiping Chen, Duminda Wijesekera, Sushil Jajodia, “Incorporating Dynamic Constraints in the Flexible Authorization Framework,” *Proc. 9th European Symp. on Research in Computer Security (ESORICS 2004), Springer Lecture Notes in Computer Science, Vol. 3193,* Sophia Antipolis, France, September 2004, pages 1-16 (Acceptance ratio 27/159).
4. Steve Noel, Sushil Jajodia, Eric Robertson, "Correlating intrusion events and building attack scenarios through attack graph distances," *Proc. 20th Annual Computer Security Applications Conference*, Tucson, Arizona, December 6-10, 2004, pages 350-359. PDF
5. Lingyu Wang, Duminda Wijesekera, Sushil Jajodia, "A logic-based framework for attribute based access control," *Proc. 2nd ACM Workshop on Formal Methods in Security Engineering (FMSE 2004),* October 2004, pages 45-55 (Acceptance ration 9/25). PDF

6. Steve Noel, Sushil Jajodia, "Managing attack graph complexity through visual hierarchical aggregation" *Proc. ACM Workshop on Visualization and Data Mining for Computer Security*, October 2004, pages109-118 (Acceptance ratio 13/36). PDF
7. Yingjiu Li, Huiping Guo, Sushil Jajodia, "Tamper detection and localization for categorical data using fragile watermarks," *Proc. ACM Workshop on Digital Rights Management*, Washington, DC, October 2004, pages 73-82 (Acceptance ratio 10/27). PDF
8. Claudio Bettini, X. Sean Wang, Sushil Jajodia, "Identifying Sensitive Associations in Databases for Release Control," *Proc. International Workshop on Secure Data Management in a Connected World, Springer Lecture Notes in Computer Science, Vol. 3178,* Willem Jonker and Milan Petkovic, eds., Toronto, Canada, August 2004, pages 187-201.
9. Yingjiu Li, Vipin Swarup, Sushil Jajodia, "Defending against additive attacks with maximal errors in watermarking relational databases," *Proc. 18th IFIP WG 11.3 Working Conference on Data and Application Security, Research Directions in Data and Applications Security XVIII,* Csilla Farkas and Pierangela Samarati, editors, Kluwer Academic Publishers, Boston, 2004, pages 81-94 (Acceptance ratio 23/49).
10. Shiping Chen, Duminda Wijesekera, Sushil Jajodia, "FlexFlow: A flexible flow control policy specification framework," in *Data and Applications Security XVII: Status and Prospects,* Sabrina De Capitani di Vimercati, Indrakshi Ray, and Indrajit Ray, eds., Kluwer Academic Publishers, Boston, 2004, pages 358-371 (Acceptance ratio 26/59).
11. Sencun Zhu, Sanjeev Setia, Shouhuai Xu, Sushil Jajodia, "GKMPAN: An efficient group rkeying scheme for secure multicast in ad-hoc networks," *Proc. First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2004)*, Boston, MA, August 22-25, 2004, pages 42-51.
12. Claudio Bettini, X. Sean Wang, Sushil Jajodia, "A learning-based approach to information release control," in *Integrity and Internal Control in Information Systems VI*, Sushil Jajodia, Leon Strous, eds., Kluwer Academic Publishers, Boston, 2004, pages 83-105.
13. Sencun Zhu, Sushil Jajodia, "Scalable group rekeying for secure multicast: A survey," *Proc. 5th International Workshop on Distributed Computing, Springer Lecture Notes in Computer Science, Vol. 2918* (Samir R. Das and Sajal K. Das, editors), 2004, pages 1-10.
14. Sushil Jajodia,Duminda Wijesekera, "A flexible authorization framework for E-commerce," *Proc. First International Conference on Distributed Computing*

and Internet Technology, Springer Lecture Notes in Computer Science, Vol. 3347 (R. K. Ghosh and H. Mohanty, eds.), 2004, pages 336-345.

15. Kaushal Sarda, Duminda Wijesekera, Sushil Jajodia "Implementing consistency checking in correlating attacks," *Proc. First International Conference on Distributed Computing and Internet Technology, Springer Lecture Notes in Computer Science, Vol. 3347* (R. K. Ghosh and H. Mohanty, eds.), 2004, pages 379-384.
16. Sencun Zhu, Sanjeev Setia, Sushil Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," *Proc. 10th ACM Conf. On Computer and Communications Security*, Washington, DC, October 27-31, 2003, pages 62-72 (Acceptance ratio 36/252).
17. Ernesto Damiani, Sabrina De Capitani di Vimercati, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati, "Balancing confidentiality and efficiency in untrusted Relational DBMSs," *Proc. 10th ACM Conf. On Computer and Communications Security*, Washington, DC, October 27-31, 2003, pages 93-102 (Acceptance ratio 36/252).
18. *Yingjiu Li, Vipin Swarup, Sushil Jajodia, "*Constructing a virtual primary key for fingerprinting relational data, *Proc. ACM Workshop on Digital Rights Management*, Washington, DC, October 2003, pages 133-141 (Acceptance ratio 13/30).
19. Lingyu Wang, Yingjiu Li, Duminda Wijesekera, Sushil Jajodia, "Precisely answering multidimensional range queries without privacy breach," *Proc. 8th European Symposium on Research in Computer Security (ESORICS 2003), Springer Lecture Notes in Computer Science, Volume 2808,* October 2003, pages 100-115 (Acceptance ratio 19/114).
20. Steve Noel, Sushil Jajodia, Brian O'Berry, Mike Jacobs, "Efficient minimum-cost network hardening via exploit dependency graphs," *Proc. 19th Annual Computer Security Applications Conference*, Las Vegas, Nevada, December 8-12, 2003, pages 86-95.
21. *Yingjiu Li, Vipin Swarup, Sushil Jajodia, "*A robust watermarking scheme for relational data," *Proc. 13th Workshop on Information Technology and Systems (WITS'03),* Seattle, Washington, December 2003, pages 195-200.
22. S. Zhu, S. Xu, S. Setia, S. Jajodia, "Establishing pair-wise keys for secure communication networks: a probabilistic approach," *Proc. 11th IEEE International Conference on Network Protocols,* Atlanta, Georgia, November 4-7, 2003 (Acceptance ratio 30/230).
23. E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, P. Samarati, M. Finetti, S. Jajodia, "Implementation of a storage mechanism for untrusted DBMSs," *Proc. IEEE Second International IEEE Security in Storage Workshop (SISW 2003),* Washington, DC, October 31, 2003, pages 38-46.

24. Sencun Zhu, Sanjeev Setia, Sushil Jajodia, “Performance optimizations for group key management schemes for secure multicast,” *Proc. IEEE 23rd Int’l. Conf. On Distributed Computing Systems,* Providence, Rhode Island, May 19-22, 2003 (Acceptance ratio 72/406).
25. Sencun Zhu, Sanjeev Setia, Sushil Jajodia, “Adding reliable and self-healing key distribution to the subset difference group rekeying method for secure multicast,” Fifth International Workshop on Networked Group Communications (NGC'03), Munich, Germany, September 16-19, 2003 (Acceptance ratio 17/51).
26. Sencun Zhu, Shouhuai Xu, Sanjeev Setia and Sushil Jajodia, “LHAP: A lightweight hop-by-hop authentication protocol for ad-hoc networks,” *Proc. International Workshop on Mobile and Wireless Networks (MWN 2003),* May 2003 (Acceptance ratio 30/60).
27. Douglas E. Williams, Amgad Fayad, Sushil Jajodia, Daniel Calle, “A user friendly guard with mobile post-release access control policy,” in *Security and Privacy in the Age of Uncertainty,* Dimitris Gritzalis, Sabrina De Capitani di Vimercati, Pierangela Samarati, Sokratis Katsikas, eds., Kluwer Academic Publishers, Boston, 2003, pages 265-276 (Acceptance ratio 33/121).
28. Lingyu Wang, Duminda Wijesekera, Sushil Jajodia, ``Towards secure XML federations," in *Research Directions in Data and Applications Security,* Ehud Gudes, Sujeet Shenoi, eds., Kluwer Academic Publishers, Boston, 2003, pages 117-131 (Acceptance ratio 25/50).
29. Daniel Barbara, Rajni Goel, Sushil Jajodia, ``Mining malicious data corruption with hidden markov models," in *Research Directions in Data and Applications Security,* Ehud Gudes, Sujeet Shenoi, eds., Kluwer Academic Publishers, Boston, 2003, pages 175-189 (Acceptance ratio 25/50).
30. Daniel Barbará, Yi Li, Jia-Ling Lin, Sushil Jajodia, Julia Couto, “Bootstrapping a data mining intrusion detection system,” *Proc. ACM Symp. on Applied Computing (SAC),* Melbourne, FL, March 2003, pages 421-425.
31. Kenneth Smith, Vipin Swarup, Sushil Jajodia, Donald B. Faatz, Todd Cornett, Jeffery Hoyt, “Securely sharing neuroimagery,” *Proc. ACM International Conference on Information and Knowledge Management,* New Orleans, Louisiana, November 2-8, 2003, pages 375-377.
32. Claudio Bettini, Sushil Jajodia, Sean Wang, Duminda Wijesekera, ``Provisions and obligations in policy rule management and security applications," *Proc. 28th International Conference on Very Large Data Bases*, Hong Kong, China, August 2002, pages 502-513 (Acceptance ratio 69/432).
33. Duminda Wijesekera, Sushil Jajodia, ``Policy Algebras for Access Control - The predicate Case," *Proc. 8th ACM Conference on Computer and*

Communications Security, Washington, DC, November 17-22, 2002, pages 171-180 (Acceptance ratio 27/161).

34. Lingyu Wang, Duminda Wijesekera, Sushil Jajodia, ``Cardinality-based inference control in sum-only data cubes," *Proc. 7th European Symposium on Research in Computer Security (ESORICS 2002), Lecture Notes in Computer Science, Vol. 2502,* Zurich, Switzerland, October 14-16, 2002, pages 55-71 (Acceptance ratio 16/83).
35. Peng Liu, Sushil Jajodia, Paul Ammann, Jie Li, ``Can-follow concurrency control," *Proc. IASTED Int'l. Conf. on Networks, Parallel and Distributed Processing, and Applications, Tsukuba,* Japan, October 1-4, 2002.
36. Yingjiu Li, Senchun Zhu, Lingyu Wang, Sushil Jajodia, ``A privacy-enhanced microaggregation method," *Proc. 2nd Int'l. Symp. on Foundations of Information and Knowledge Systems (FoIKS 2002), Springer-Verlag Lecture Notes in Computer Science, Vol. 2284 (T. Eiter and K.-D. Schwe, eds)*, February 2002, pages 148-159. (Acceptance ratio 15/55).
37. Yingjiu Li, Lingyu Wang, X. Sean Wang, Sushil Jajodia, ``Auditing interval-based inference," *Proc. 14th Conf. on Advanced Information Systems Engineering (CAiSE'02)*, *Springer-Verlag Lecture Notes in Computer Science, Vol. 2348 (A. Banks Pidduck, J. Mylopoulos, C. C. Woo, M. Tamer Ozsu, eds.)*, May 2002, pages 553-568 (Acceptance ratio 42/173).
38. Yingjiu Li, Lingyu Wang, Sushil Jajodia, ``Preventing interval-based inference by random data perturbation," *Proc. Workshop on Privacy Enhancing Technologies,* San Francisco, CA, April 2002 (Acceptance ratio 16/47).
39. Claudio Bettini, Sushil Jajodia, X. Sean Wang, Duminda Wijesekera, ``Obligation monitoring in policy management," *Proc. 3rd International Workshop on Policies for Distributed Systems and Networks (POLICY 2002),* Monterey, CA, IEEE Computer Society, June 2002, pages 2-12 (Acceptance ratio 17/67).
40. Sushil Jajodia, Duminda Wijesekera, ``Recent advances in access control models," in *Database and Application Security XV,* Martin S. Olivier and David L. Spooner, eds., Kluwer Academic Publishers, Boston, 2002, pages 3-15.
41. Jackie Yang, Duminda Wijesekera, Sushil Jajodia, ``Subject switching algorithms for access control in federated databases," in *Database and Application Security XV,* Martin S. Olivier and David L. Spooner, eds., Kluwer Academic Publishers, Boston, 2002, pages 61-74.
42. Ravi Mukkamala, Sushil Jajodia, ``A novel approach to certificate revocation management," in *Database and Application Security XV,* Martin S. Olivier and David L. Spooner, eds., Kluwer Academic Publishers, Boston, 2002, pages 225-238.

43. Roberto Di Pietro, Luigi V. Mancini, Sushil Jajodia, ``Efficient and secure keys management for wireless mobile communications,'' *Proc. 2nd ACM Int'l. Workshop on Mobile Computing,* Toulouse, France, October 2002, pages 66-73.
44. Roberto Di Pietro, Luigi V. Mancini, Sushil Jajodia, ``Secure selective exclusion in ad hoc wireless network," in *Security in the information Society: Visions and Perspectives,* M. Adeeb Ghonaimy, Mahmoud T. El-Hadidi, Heba K. Aslan, eds., Kluwer Academic Publishers, Boston, 2002, pages 423-434.
45. Ken Smith, Don Faatz, Amgad Fayad, Sushil Jajodia, ``Propagating modifications to mobile policies," in *Security in the information Society: Visions and Perspectives,* M. Adeeb Ghonaimy, Mahmoud T. El-Hadidi, Heba K. Aslan, eds., Kluwer Academic Publishers, Boston, 2002, pages 573-584.
46. Duminda Wijesekera, Sushil Jajodia, ``Policy Algebras for Access Control - The Propositional Case," *Proc. 8th ACM Conference on Computer and Communications Security,* Philadelphia, PA, November 5-8, 2001, pages 38-47 (Acceptance ratio 27/153).
47. Daniel Barbara, Ningning Wu, Sushil Jajodia, ``Detecting novel network intrusions using bayes estimators," *Proc. 1st SIAM International Conference on Data Mining (SDM 2001),*, Chicago, IL, April 2001.
48. Asa Hagstrom, Sushil Jajodia, Francesco Parisi-Presicce, Duminda Wijesekera, ``Revocations - a classification," *Proc. 14th IEEE Computer Security Foundations Workshop*, Nova Scotia, Canada, June 2001, pages 44-58.
49. Peng Liu, Sushil Jajodia, ``Multi-phase damage confinement in database systems for intrusion tolerance," *Proc. 14th IEEE Computer Security Foundations Workshop*, Nova Scotia, Canada, June 2001, pages 191-205.
50. Yingjiu Li, Peng Ning, X. Sean Wang, Sushil Jajodia, ``Discovering calendar-based temporal association rules," *Proc. 8th Int'l. Symp. on Temporal Representation and Reasoning (TIME 2001)*, Cividale del Fruily, Italy, June 2001, pages 111-118.
51. Amgad Fayad, Sushil Jajodia, Don Faatz, Vinti Doshi, ``Going beyond MAC and DAC using mobile policies," in *Trusted Information - The New Decade Challenge* (Michel Dupuy and Pierre Pardinas, editors), Kluwer Academic Publishers, Boston, June 2001, pages 245-260.
52. Yingjiu Li, X. Sean Wang, Sushil Jajodia, ``Discovering temporal patterns in multiple granularities," *Proc. Int'l. Workshop on Temporal, Spatial, and Spatio-Temporal Data Mining, Springer-Verlag Lecture Notes in Artificial Intelligence, Vol. 2007* , 2001, pages 5-19.
53. Daniel Barbara, Rajni Goel, and Sushil Jajodia, ``Protecting file systems against corruption using checksums," in *Data and Applications Security: Developments and Directions,* Bhavani Thuraisingham, Reind van de Riet,

Klaus R. Dittrich, Jahir Tari, eds. Kluwer Academic Publishers, Boston, 2001, pages 113-124.

54. Susan Chapin, Don Faatz, Sushil Jajodia, ``Distributed policies for data management making policies mobile," in *Data and Applications Security: Developments and Directions,* Bhavani Thuraisingham, Reind van de Riet, Klaus R. Dittrich, Jahir Tari, eds. Kluwer Academic Publishers, Boston, 2001, pages 63-75.
55. Daniel Barbara, Julia Couto, Sushil Jajodia, Leonard Popyack, Ningning Wu, ``ADAM: Detecting intrusions by data mining," *Proc. IEEE Workshop on Information Assurance and Security,* West Point, NY, June 2001, pages 11-16.
56. Sanjeev Setia, Samir Koussih, Sushil Jajodia, Eric Harder, ``Kronos: A scalable group re-keying approach for secure multicast," *Proc. IEEE Symp. on Security and Privacy*, Oakland, CA, May 2000 (Acceptance ratio 18/137).
57. Daniel Barbará, Rajni Goel, and Sushil Jajodia, ``Using checksums to detect data corruption," *Proc. Conf. on Extending Database Technology, Springer Lecture Notes in Computer Science, Vol. 1777* Konstanz, Germany, March 2000, pages 136-149 (Acceptance ratio 30/180).
58. Yingjiu Li, Ningning Wu, Sushil Jajodia, X. Sean Wang, ``Enhancing profiles for anomaly detection using time granularities," *Proc. 1st Workshop on Intrusion Detection Systems*, Athens, Greece, November 2000.
59. Vinti Doshi, Amgad Fayad, Sushil Jajodia, Roswitha MacLean, ``Using attribute certificates with mobile policies in electronic commerce applications," *Proc. 16th Annual Computer Security Applications Conf.,* New Orleans, LA, December 2000, pages 298-307.
60. Paul Ammann and Sushil Jajodia, ``The integrity challenge," *Integrity and Internal Controls in Information Systems: Strategic View on the Need for the Control*, (Margaret E. van Biene-Hershey and Leon Strous, eds.), Kluwer, Boston, 2000, pages 59-69.
61. Jiahai Yang, Peng Ning, X. Sean Wang, Sushil Jajodia, ``CARDS: A distributed system for detecting coordinated attacks," in *Information Security For Global Information Infrastructures: IFIP TC11 Sixteenth Annual Working Conference on Information Security,* (Sihan Qing and Jan H.P. Elof eds.), Kluwer, Boston, August 2000, pages 171-180 (Acceptance ratio 50/180).
62. Claudio Bettini, X. Sean Wang, Sushil Jajodia, ``Free schedules for free agents in workflow systems," *Proc. 7th Int'l. Symp. on Temporal Representation and Reasoning (TIME 2000)*, Nova Scotia, Canada, July 2000, pages 31-37.
63. Peng Ning, X. Sean Wang, Sushil Jajodia, ``An algebraic representations of calendars," *Proc. AAAI Workshop on Spatial and Temporal Granularity*, Austin, TX, June 2000, pages 1-8.

64. Sushil Jajodia, Michiharu Kudo, V. S. Subrahmanian, ``Provisional authorizations," *Proc. 1st Workshop on Security and Privacy in E-Commerce*, Athens, Greece, November 2000.
65. Peng Liu, Peng Ning, Sushil Jajodia ``Avoiding loss of fairness owing to process crashes in fair data exchange protocols," *IEEE Workshop on Dependability despite Malicious Faults*, In *Proc. IEEE Int'l. Conf. on Dependable Systems and Networks,* New York, NY, June 2000, pages 631-640.
66. Neil F. Johnson, Zoran Duric, Sushil Jajodia, ``Recovery from watermarks on distorted images." *Proc. 3rd Workshop on Information Hiding, Springer-Verlag Lecture Notes in Computer Science, Vol. 1768* , 2000, pages 318-332.
67. Peng Ning, X. Sean Wang, Sushil Jajodia, ``A query facility for common intrusion detection framework," *Proc. 23rd National Information Systems Security Conf.,* Baltimore, MD, October 2000.
68. Peng Liu, Sushil Jajodia and Catherine D. McCollum, ``Intrusion confinement by isolation in information systems," *Research Advances in Database and Information Systems Security,* Vijay Atluri and John Hale, editors, Kluwer Publishers, Boston, 2000, pages 3-18.
69. Ravi Mukkamala, Jason Gagnon, and Sushil Jajodia, ``Integrating data mining techniques with intrusion detection," *Research Advances in Database and Information Systems Security,* Vijay Atluri and John Hale, editors, Kluwer Publishers, Boston, 2000, pages 33-46.
70. Peng Liu, Paul Ammann, Sushil Jajodia, ``Incorporating transaction semantics to reduce reprocessing overhead in replicated mobile data applications," *IEEE Int'l. Conf. on Distributed Computing Systems,* 1999, pages 414-423 (Acceptance ratio 57/173).
71. Amgad Fayad, Sushil Jajodia, Catherine D. McCollum, ``Application-level isolation using data inconsistency detection," *Proc. 15th Annual Computer Security Applications Conf.,* Phoenix, AZ, December 1999, pages 119-126.
72. Sushil Jajodia, Peng Liu, Paul Ammann, ``A fault tolerance approach to survivability," *Symp. on Protecting NATO Information Systems in the 21st Century,* Washington, DC, October 1999.
73. Neil F. Johnson, Zoran Duric, Sushil Jajodia, ``On ``fingerprinting" images for recognition," *Proc. 5th Int'l. Workshop on Multimedia Information Systems,* Palm Springs Desert, CA, October 1999.

BOOK CHAPTERS

1. Sushil Jajodia, Steve Noel, Brian O'Berry, "Topological analysis of network attack vulnerability," in *Managing Cyber Threats: Issues, Approaches and Challenges*, Vipin Kumar, Jaideep Srivastava and Aleksandar Lazarevic, eds., Kluwer Academic Publishers, Boston, 2004, To appear.
2. Sushil Jajodia, "Database security and privacy," in *Computer Science Handbook, 2nd edition*, Allen B. Tucker, Jr., ed., CRC Press, Boca Raton, FL, June 2004.
3. Anoop Singhal, Sushil Jajodia, "Data mining for intrusion detection," in *Data Mining and Knowledge Discovery Handbook: A Complete Guide for Practitioners and Researchers,* Oded Maimon and Lior Rokach, eds., Kluwer Academic Publishers, Boston, 2004, To appear.
4. Mohamed Eltoweissy, Sushil Jajodia, Ravi Mukkamala, "Secure multicast for mobile commerce applications: Issues and challenges," in *Advances in Security and Payment Methods for Mobile Commerce,* Wen Chen Hu, Chung-Wei Lee, and Weidong Kou, eds., Idea Group Publishing, Hershey, PA, 2004, pages 164-190.
5. Duminda Wijesekera, Sushil Jajodia, "A flexible authorization framework," in *Information Security: Policies and Actions in Modern Integrated Systems*, Marigrazia Fugini and Carlo Bellettini, eds. Idea Group Publishing, Hershey, PA, 2004, pages 149-176.
6. Peng Ning, Sushil Jajodia, "Intrusion Detection Systems Basics," in *Handbook of Information Security*, Hossein Bidgoli, ed., John Wiley, 2004.
7. Peng Ning, Sushil Jajodia, "Intrusion Detection Techniques," in *The Internet Encyclopedia*, Hossein Bidgoli, ed., John Wiley, ISBN 0-471-22201-1, December 2003.
8. Daniel Barbara, Julia Couto, Sushil Jajodia, Ningning Wu, ``An architecture for anomaly detection," in Applications of Data Mining in Computer Security, Daniel Barbara, Sushil Jajodia, eds., ISBN 1-4020-7054-3, Kluwer Academic Publishers, Boston, 2002, pages 63-76.
9. Yingjiu Li, Ninging Wu, X. Sean Wang, and Sushil Jajodia, ``Enhancing profiles for anomaly detection using time granularities," in *Intrusion Detection*, Deborah Frincke, ed., IOS Press, Amsterdam, 2002, pages 137-157.
10. Sushil Jajodia, Michiharu Kudo, V. S. Subrahmanian, ``Provisional authorizations," in *E-Commerce Security and Privacy*, Anup Ghosh, ed., Kluwer Academic Publishers, Boston, 2001, pages 133-159.
11. Sabrina Di Capitani di Vimercati, Pierangela Samarati, Sushil Jajodia, ``Database Security," in *Encyclopedia of Software Engineering, 2nd edition,* John Marciniak, ed., John Wiley, New York, 2001.
12. Paul Ammann, Sushil Jajodia, Peng Liu, ``A fault tolerance approach to survivability," in *Computer Security, Dependibility, and Assurance: From*

Needs to Solutions , P.Ammann, B. H. Barnes, S. Jajodia, E. H. Sibley, eds., IEEE Computer Society Press, Los Alamitos (1999), pages 204-212.
13. Pierangela Samarati and Sushil Jajodia, ``Data Security," in *Wiley Encyclopedia of Electrical and Electronics Engineering, Volume 4*, John G. Webster, ed., John Wiley, NY, (1999) pages 743-759.

OTHER ARTICLES

1. Csilla Farkas and Sushil Jajodia, ``The Inference problem: A survey,'' *ACM SIGKDD Explorations,* Vol. 4, No. 2, 2003, pages 6-11.
2. Daniel Barbara, Julia Couto, Sushil Jajodia, Ningning Wu, ``ADAM: A testbed for exploring the use of data mining in intrusion detection," *ACM SIGMOD Record*, Vol. 30, No. 4, December 2001, pages 15-24.
3. Sushil Jajodia, Duminda Wijesekera, ``Security in Federated Database Systems," *Information Security Technical Report*, Vol. 6, No. 2, 2001, pages 69-79.
4. Paul Ammann and Sushil Jajodia, ``Computer security, fault Tolerance, and software assurance," *IEEE Concurrency*, Vol. 7, No. 1, January-March 1999, pages 4-6.

附件(二) Ravi Sandhu

Ravi Sandhu

Professor of Information and Software Engineering, GMU, Fairfax, VA
Co-founder and Chief Scientist, SingleSignOn.Net, Reston, VA

CONTACT

Ravi Sandhu, ISE Department-MS4A4, George Mason University, Fairfax, VA, 22030 Voice: 703 993 1659, Facsimile: 703 993 1638, Voice (SSN): 703 796 0965 Email: sandhu@gmu.edu or rsandhu@singlesignon.net, URL: www.list.gmu.edu

CITIZENSHIP

US citizen since 1991

DEGREES

Degree	Major University	Year
Ph.D.	Computer Science Rutgers University, New Jersey	1983
M.S.	Computer Science Rutgers University, New Jersey	1980
M.Tech.	Computer Technology Indian Institute of Technology, New Delh	1976
B.Tech.	Electrical Engineering Indian Institute of Technology, Bombay	1974

CAREER OBJECTIVES

My ambition is to pursue a high impact research, development and education program in information and system security. The ability to build and operate large-scale secure systems amidst rapid technological change is critical for our information-based society. This requires continued advances in basic technology, applied research and development, and education. My goal is to play a lead role in this effort.

RESEARCH ACTIVITIES

My research activities focus on information and system security, with emphasis on access control models and systems, distributed systems, electronic commerce and the Internet. I am the founder and director of the Laborator y for Information Security Technology (LIST) established at GMU.

ENTREPRENEURIAL ACTIVITIES

I am the Co-Founder and Chief Scientist of an Internet Security start-up called SingleSignOn.Net. The company's novel Secure Identity ApplianceTM is the only product in the market that in a single appliance offers multiple solutions encompassing Password Authentication Systems, Secure Vault, Single Sign-On, PKI,

Wireless Authentication, Network Wallet and VPN Authentication. The cryptographic protocols, security architecture and role-based access control features have been largely designed by me.

CAREER SYNOPSIS

George Mason University, 1989 onwards

- 1995 onwards, Full Professor
- 1989-1995, Associate Professor

SingleSignOn.Net, 2000 onwards

- Co-founder and Chief Scientist

Ohio State University, 1982-89

- 1983-1989, Assistant Professor
- 1982-1983, Instructor

Prior Years, 1975-82

- 1978-1982, Graduate Assistant, Rutgers University, New Brunswick, New Jersey
- 1977-1978, Systems Engineer, Hindustan Computers Limited, New Delhi, India
- 1975-1977, Graduate Assistant, Indian Institute of Technology, New Delhi, India

PUBLICATIONS

I have authored over 140 technical papers in refereed journals, conferences and collections, mostly available at www.list.gmu.edu. Some of the more significant and influential papers are listed below.

- D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn and R. Chandramouli. "Proposed NIST Standard for Role-Based Access Control." ACM TISSEC, Volume 4, Number 3, August 2001.
- J. Park, R. Sandhu and G. Ahn. "Role-Based Access Control on the Web." ACM Transactions on Information and System Security (TISSEC), Volume 4, Number 1, February 2001, pages 37-71.
- G. Ahn and R. Sandhu. "Role-Based Authorization Constraints Specification." ACM Transactions on Information and System Security (TISSEC), Volume 3, Number 4, November 2000, pages 207-226
- J. Park & R. Sandhu, "Secure Cookies on the Web." IEEE Internet Computing, 4(4):36-45, July 2000.
- S. Osborn, R. Sandhu and Q. Munawer. "Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies." ACM TISSEC, 3(2):85-106, May 2000.
- R. Sandhu, V. Bhamidipati and Q. Munawer. "The ARBAC97 Model for Role -Based Administration of Roles." ACM TISSEC, Volume 2, Number 1, February 1999, pages 105-135.
- R. Sandhu & F. Chen, "The Multilevel Relational Data Model." ACM TISSEC,

1(1):93-132, Nov 1998.

- R. Sandhu, "Role-Based Access Control." Advances in Computers, Vol. 46, pages 237-286, 1998.
- R. Thomas & R. Sandhu, "Task-based Authorization Controls (TBAC)." Database Security XI: Status and Prospects, (T.Y. Lin and Shelly Qian, editors), Chapman & Hall 1998, pages 262-275.
- R. Sandhu, E. Coyne, H. Feinstein and C. Youman, "Role -Based Access Control Models." IEEE Computer, Volume 29, Number 2, February 1996, pages 38-47.
- R. Thomas and R. Sandhu, "A Secure Trusted Subject Architecture for Multilevel Object-Oriented Databases." IEEE TKDE, Volume 8, Number 1, February 1996, pages 16-31.
- R. Sandhu, "Lattice-Based Access Control Models." IEEE Computer, 26(11):9-19, Nov. 1993.
- R. Sandhu, "The Typed Access Matrix Model." IEEE Symposium on Research in Security and Privacy, Oakland, California, May 1992, pages 122-136.
- R. Sandhu, "Undecidability of Safety for SPM with Cyclic Creates." JCSS, 44(1):141-159, Feb 1992.
- R. Sandhu, "Transaction Control Expressions for Separation of Duties , Dec. 1988, 282-286.
- R. Sandhu, "The NTree." ACM TOCS, Volume 6, Number 2, May 1988, pages 197-222.
- R. Sandhu, "The Schematic Protection Model (SPM)." JACM, 35(2):404-432, April 1988.

SPONSORED RESEARCH

Primary funding has come from: NSF, NSA, NRO, NIST, DARPA, Sandia Laboratories, Naval Research Laboratory, Lockheed Martin, SETA Corporation and TASC.

PROFESSIONAL POSITIONS

- Founding Editor-in-Chief of the ACM Transaction on Information and Systems Security (TISSEC)
- Chairman, Special Interest Group on Security Audit and Control of the ACM (SIGSAC)
- Member Editorial Board of IEEE Internet Computing
- Founder & Steering Committee Chair of ACM Conference on Computer & Communications Security
- Founder & Steering Committee Chair of ACM Symposium on Access Control Models & Technologies
- Member Steering Committee of IEEE Computer Security Foundations Workshop

- Program and General Chair of numerous security conferences on various occasions

CONSULTING ACTIVITIES

- I have served as a security consultant to numerous organizations including AT&T, Lucent Technologies, Network Associates, SETA Corporation, NIST, IRS, State Department and Verizon
- I have taught professional courses on Information and System Security all over the world including USA, Canada, India, Australia, Singapore, Korea, Malaysia and New Zealand.

HONORS

- Fellow of ACM and Fellow of IEEE.
- Best paper award in 1998 and 1992 at National Information Systems Security Conference

附件(三) Shankar Sastry

Contact information

Director, Center for Information Technology Research in the Interest of Society
NEC Distinguished Professor of Engineering
Departments of Electrical Engineering and Computer Sciences and Bioengineering
University of California, Berkeley
Office: 284 HMMB, 514 Cory Hall
Phone: (510) 643-2200, (510) 642-1857
Fax: (510) 643-2356

Email: sastry@eecs.berkeley.edu

Professional Biography

S.Shankar Sastry became Chair, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley in January, 2001, and held that position until 2004. prior to that, he served as Director of the Information Technology Office at DARPA. From 1996-1999, he was the Director of the Electronics Research Laboratory at Berkeley, an organized research unit on the Berkeley campus conducting research in computer sciences and all aspects of electrical engineering. During his directorship from 1996-1999, extra-mural funding of the laboratory grew from $29M to $50M. Prof. Sastry also holds a joint professorship in the Departments of Electrical Engineering and Computer Sciences and Bioengineering.

Prof. Sastry served as associate editor for numerous publications, including: IEEE Transactions on Automatic Control; IEEE control Magazine; IEEE Transactions on Circuits and Systems; the Journal of Mathematical Systems, Estimation and Control; IMA Journal of Control and Information; the International Journal of Adaptive Control and Signal processing; and the Journal of Biomimetic Systems and Materials.

Research Interests

- Hybrid and Embedded Control and Systems
- Software Enabled Control
- Networked Embedded Systems
- Cybersecurity and Critical Infrastructure Protection
- Millirobotics for Minimally-Invasive surgery
- Computer Vision

- Generalized Principal Component Analysis and Unsupervised Learning
- Berkeley AeroRobots: flying aircraft and rotorcraft.
- Engineering Applications of Exterior Differential Systems. See parking movies on Dawn Tilbury's home page
- Adaptation and Learning in Biological and Artificial Systems

See also CML: Learning Complex Motor Tasks in Natural and Artificial Systems

- Air Traffic Management Systems

Major Research Projects

- TRUST: Team for Research in Ubiquitous Security Technologies NSF Science and Technology Center
- DETER: Cyberdefense Technology Evaluation and Research testbed , NSF and DHS Network Defense Testbed
- Foundations of Hybrid and Embedded Software and Systems An NSF ITR with Vanderbilt and Memphis
- Adaptive Coordinated Control of Intelligent Multi-Agent Teams (ACCLIMATE) An ARO MURI with U Penn and CMU
- Network Embedded Systems Technology DARPA, NSF.
- Berkeley Quantum Information and Computation Center NSF-ITR, DARPA.
- Minimally-Invasive Telesurgery Supported by NSF, ONR, NASA, ARO.
- Software Enabled Control , DARPA. Project Completed.
- Intelligent Control Architectures for Unmanned Air Vehicles , ARO, ONR, Project Completed.
- Air Traffic Management Systems supported by NASA, FAA. See also the homepage of NEXTOR
- CML: Learning Complex Motor Tasks in Natural and Artificial Systems, NSF KDI Program, Project Completed.

Recent Papers

A searchable index of recent papers is being compiled and papers being scanned at the current time to add to the home page: this page will be under construction for a bit: Please stay tuned!

- Stochastic Approximations for Hybrid Systems

by Abate, Ames and Sastry,
Proceedings of the American Control Conference, Portland, Oregon

- Stability Criteria for Stochastic Hybrid Systems

by Abate, Shi, Simic and Sastry,
Proceedings of the 16th International Symposium on the Mathematical Theory of

Networks and Systems, Leuven 2004.

- Joint Parametric Alignment for ANalyzing Spatial Gene Expression Patterns in Drosophila Imaginal Discs

by Ahammad, Harmon, Hammonds, Sastry and Rubin,
Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, San Diego, 2005.

附件(四) Doug Tygar

Doug Tygar is Professor of Computer Science and Information Management at UC Berkeley. He works in the areas of computer security, privacy, and electronic commerce. His current research includes strong privacy protections, security issues in sensor webs, and digital rights management. His awards include a National Science Foundation Presidential Young Investigator Award, an Okawa Foundation Fellowship, a teaching award from CMU, and invited keynote addresses at PODC, PODS, VLDB, and several other conferences. His newest book, *Secure Broadcast Communication in Wired and Wireless Networks* (with Adrian Perrig) was published in 2003 and a Japanese version will shortly appear. He designed cryptographic postage standards for the US Postal Service and has helped build a number of security and electronic commerce systems including: Strongbox, Dyad, Netbill, and Micro-Tesla. He serves as chair of the Defense Department's ISAT Study Group on Security with Privacy, and was a founding board member of ACM's Special Interest Group on Electronic Commerce. Dr. Tygar previously was tenured faculty at Carnegie Mellon University's Computer Science Department for many years (and retains an Adjunct Professor position there). He received his doctorate from Harvard and his undergraduate degree from Berkeley.

Publications

Books (authored):

1. Waiyādo/Waiyaresu Nettowōku ni Okeru Burōdokyasuto Tsūshin no Sekyuriti (ワイヤード/ワイヤレスネットワークにおけるブロードキャスト通信のセキュリティ). A. Perrig and J. D. Tygar. Translated by Fumio Mizoguchi and the Science University of Tokyo Information Media Science Research Group. Kyoritsu Shuppan, 2004. (Japanese translation of item 2 below, with additional material.)

2. Secure Broadcast Communication. A. Perrig and J. D. Tygar. Springer (Kluwer), 2003.

3. Trust in Cyberspace. National Research Council Committee on Information Systems Trustworthiness (S. Bellovin, W. E. Boebert, M. Branstad, J. R. Catoe, S. Crocker, C. Kaufman, S. Kent, J. Knight, S. McGeady, R. Nelson,

A. Schiffman, F. Schneider [ed.], G. Spix, and J. D. Tygar). National Academy Press, 1999.

Books (edited):

4. Computer Security in the 21st Century. Eds. D. Lee, S. Shieh, and J. D. Tygar. Springer, 2005 (to appear). (Note: This work will include a technical overview by me and other editors as well as a technical paper; see items 5-6 below.)

Book Chapters:

5. "Overview of Computer Security in the 21st Century." J. D. Tygar. In Computer Security in the 21st Century, eds. D. Lee, S. Shieh, and J. D. Tygar. Springer, 2005 (to appear, see item 4).

6. "Private matching." Y. Li, J. D. Tygar, J. Hellerstein. In Computer Security in the 21st Century., eds. D. Lee, S. Shieh, and J. D. Tygar. Springer, 2005 (to appear, see item 4). (Note: An early version of this paper appeared as Intel Research Laboratory Berkeley technical report IRB-TR-04-005, February, 2004.)

7. "Digital cash." J. D. Tygar. In Berkshire Encyclopedia of Human Computer Interaction, ed. W. Bainbridge. Berkshire Publishing, 2004, pp. 167-170.

8. "Spamming." J. D. Tygar. In Berkshire Encyclopedia of Human Computer Interaction, ed. W. Bainbridge. Berkshire Publishing, 2004, pp.673-675.

9. "Viruses." J. D. Tygar. In Berkshire Encyclopedia of Human Computer Interaction, ed. W. Bainbridge. Berkshire Publishing, 2004, pp. 788-791.

10. "Privacy in sensor webs and distributed information systems." J. D. Tygar. In Software Security, eds. M. Okada, B. Pierce, A. Scedrov, H. Tokuda, and A. Yonezawa. Springer-Verlag, 2003, pp. 84-95.

11. "Atomicity in electronic commerce." J. D. Tygar. In Internet Besieged, eds. D. Denning and P. Denning. ACM Press and

Addison-Wesley, 1997, pp. 389-406. (Note: a more detailed, earlier version of this paper was published as "Atomicity in electronic commerce," Proceedings of the Fifteenth Annual ACM Symposium on Principles of Distributed Computing PODC, Keynote paper, May 1996, pp. 8-26; and as CMU Computer Science technical report CMU-CS-96-112. See also item 26 below.)

12. "Cryptographic postage indicia." J. D. Tygar, B. Yee, and N. Heintze. In Concurrency and Parallelism, Programming, Networking, and Security, eds. J. Jaffar and R. Yap. Springer-Verlag, 1996, pp. 378-391. (Early versions appeared as CMU Computer Science technical reports CMU-CS-96-113, UCSD Computer Science technical report UCSD-TR-CS96-485 and in the 1996 Securicom Proceedings, Paris. See also item 80 below.)

13. "Dyad: A system for using physically secure coprocessors." J. D. Tygar and B. Yee. In Technological Strategies for the Protection of Intellectual Property in the Networked Multimedia Environment. Harvard University Press and the Interactive Multimedia Association, 1994, pp. 121-152. (An early version appeared as CMU Computer Science technical report CMU-CS-91-140R, 1991.)

14. "A system for self-securing programs." J. D. Tygar and B. Yee. In Carnegie Mellon Computer Science: A 25-Year Commemorative, ed. R. Rashid. ACM Press and Addison-Wesley, 1991, pp. 163-197. (Note: The first printing of this volume had incorrect text due to a production error.)

15. "Implementing capabilities without a trusted kernel." M. Herlihy and J. D. Tygar. In Dependable Computing for Critical Applications, eds. A. Avizienis and J. Laprie. Springer, 1991, pp. 283-300. (Note: An early version appeared in the (IFIP) Proceedings of the International Working Conference on Dependable Computing for Critical Applications, August 1989.)

16. "Strongbox." J. D. Tygar and B. Yee. In Camelot and Avalon: A Distributed Transaction Facility, eds. J. Eppinger, L. Mummert, and A. Spector. Morgan-Kaufmann, 1991, pp. 381-400.

17. "ITOSS: An Integrated Toolkit for Operating System Security." M. Rabin and J. D. Tygar. In Foundations of Data Organization, eds. W. Litwin and H.-J. Shek. Springer, 1990, pp. 1-15. (Note: Earlier, longer versions

appeared as Harvard University Aiken Computation Laboratory technical report TR-05-87R and my Ph.D. dissertation.)

18. "The semantics of Miro." M. Maimone, J. D. Tygar, and J. Wing. In Visual Languages and Visual Programming, ed. S. K. Chang. Plenum, 1990, pp. 97-116.
(Early version published n Proceedings of the 1988 IEEE Workshop on Visual Programming, pp. 45-51, and as CMU Computer Science technical report CMU-CS-88-173r.)

Journal Papers:

19. "Cyber defense technology networking and evaluation." Members of the DETER and EMIST Projects (R. Bajcsy, T. Benzel, M. Bishop, B. Braden, C. Brodley, S. Fahmy, S. Floyd, W. Hardaker, A. Joseph, G. Kesidis, K. Levitt, B. Lindell, P. Liu, D. Miller, R. Mundy, C. Neuman, R. Ostrenga, V. Paxson, P. Porras, C. Rosenberg, S. Sastry, D. Sterne, J. D. Tygar, and S. Wu). In Communcations of the ACM, 47:3, March 2004, pp. 58-61.

20. "Technological dimensions of privacy in Asia." J. D. Tygar. In Asia Pacific Review. 10:2, November 2003. pp. 120-145.

21. "SPINS: Security protocols for sensor networks." A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler. In ACM Journal of Wireless Networks, 8:5, September 2002, pp. 521-534. (An early version of this paper appears in the Proceedings of the 7th Annual International Conference on Mobile Computing and Networks (MOBICOM), pp. 189-199, July 2001.)

22. "The TESLA broadcast authentication protocol." A. Perrig, R. Canneti, J. D. Tygar, and D. Song. In CryptoBytes, 5:2, Summer/Fall 2002, pp. 2-13.

23. "SAM: A flexible and secure auction architecture using trusted hardware." A. Perrig, S. Smith, D. Song, and J. D. Tygar. In Electronic Journal on E-commerce Tools and Applications, Volume 1, Number 1, January 2002 (online journal). (An early version of this paper appeared in Proceedings of the 1st IEEE International Workshop on Internet Computing and Electronic Commerce, April 2001, pp. 1763-1773.)

24. "Why isn't the internet secure yet?" J. D. Tygar and A. Whitten. In ASLIB Proceedings, 52:3, March 2000, pp. 93-97.

25. "Multi-round anonymous auction protocols." H. Kikuchi, M. Harkavy, and J. D. Tygar. In Institute of Electronics, Information, and Communication Engineers Transactions on Information and Systems, E82-D:4, April 1999. (An early version appeared in the Proceedings of IEEE Workshop on Dependable and Real-Time E-Commerce Systems (DARE'98), June 1998, pp. 62-69.)

26. "Atomicity in electronic commerce." In ACM NetWorker, 2:2, April/May 1998, pp. 32-43. (Note, this is a revision of item 11 published together with new material: "An update on electronic commerce." In ACM NetWorker, Volume 2, Number 2, April/May 1998, pp. 40-41.)

27. "A model for secure protocols and their compositions." N. Heintze and J. D. Tygar. In IEEE Transactions on Software Engineering, 22:1, January 1996, pp. 16-30. (An expanded abstract appeared in Proceedings 1994 IEEE Symposium on Security and Privacy, May 1994, pp. 2-13 and CMU technical report CMU-CS-92-100.)

28. "NetBill: An Internet commerce system optimized for network-delivered services." M. Sirbu and J. D. Tygar. In IEEE Personal Communications, 2:4, August 1995, pp. 34-39. (An early version appeared in Proceedings of Uniforum '96, February 1996, pp. 205-226; and another early version appeared in Proceedings of 40th IEEE Computer Society International Conference, Spring 1995, pp. 20-25.)

29. "Optimal sampling strategies for quicksort." C. C. McGeoch and J. D. Tygar. In Random Structures and Algorithms, 7:4, 1995, pp. 287-300. (An early version appeared in Proceedings 28th Annual Allerton Conference on Communication, Control, and Computing, October 1990, pp 62-70.)

30. "Geometric characterization of series-parallel variable resistor networks." R. Bryant, J. D. Tygar, and L. Huang. In IEEE Transactions on Circuits and Systems 1: Fundamental Theory and Applications, 41:11, November 1994, pp. 686-698. (An early version appeared in Proceedings 1993 IEEE International Symposium on Circuits and Systems, May 1993, pp. 2678-2681.)

31. "Computability and complexity of ray tracing." J. Reif, J. D. Tygar, and A. Yoshida. In Discrete Computational Geometry, 11:3, 1994, pp. 265-287. (An early version appeared in Proceedings of the 31st Annual IEEE Symposium on Foundations of Computer Science, October 1990, pp. 106-114.)

32. "Specifying and checking Unix security constraints." A. Heydon and J. D. Tygar. In Computing Systems, 7:1, Winter 1994, pp. 91-112. (An early version appeared in Proceedings of the 3rd USENIX Security Symposium, October 1993, pp. 211-226.)

33. "Protecting privacy while preserving access to data." L. J. Camp and J. D. Tygar. In The Information Society, 10:1, January 1994, pp. 59-71.

34. "Miro: visual specification of security." A. Heydon, M. Maimone, J. D. Tygar, J. Wing, and A. Zaremski. In IEEE Transactions on Software Engineering, 16:10, October 1990, pp. 1185-1197. (An early version appeared as CMU Computer Science Department technical report CMU-CS-89-199.)

35. "Efficient parallel pseudo-random number generation." J. Reif and J. D. Tygar. In SIAM Journal of Computation, 17:2, April 1988, pp. 404-411. (An early version appeared in Proceedings CRYPTO-85, eds. E. Brickell and H. Williams, Springer, 1986.)

36. "Review of Abstraction and Specification in Program Development." J. D. Tygar. In ACM Computing Reviews, 28:9, September 1987, pp. 454-455.

Refereed Conference Papers (does not include items listed above)

37. "Image Recognition CAPTCHAs." M. Chew and J. D. Tygar. In Proceedings of the 7th International Information Security Conference (ISC 2004), September 2004, pp. 268-279. (A longer version appeared as UCB Computer Science Division technical report UCB/CSD-04-1333, June 2004.)

38. "Side effects are not sufficient to authenticate software." U. Shankar, M. Chew, and J. D. Tygar. In Proceedings of the 13th USENIX Security

Symposium, August 2004, pp. 89-101.

39. "Statistical monitoring + predictable recovery = Self-*." A Fox, E. Kiciman, D. Patterson, R. Katz, M. Jordan, I. Stoica and J. D. Tygar. In Proceedings of the 2nd Bertinoro Workshop on Future Directions in Distributed Computing (FuDiCo II), June 2004 (online proceedings).

40. "Distillation codes and their application to DoS resistant multicast authentication." C. Karlof, N. Sastry, Y. Li, A. Perrig, and J. D. Tygar. In Proceedings of the Network and Distributed System Security Conference (NDSS 2004), February 2004, pp. 37-56.

41. "Privacy and security in the location-enhanced World Wide Web." J. Hong, G. Boriello, J. Landay, D. McDonald, B. Schilit, and J. D. Tygar. In Proceedings of the Workshop on Privacy at Ubicomp 2003, October 2003 (online proceedings).

42. "The problem with privacy." J. D. Tygar. Keynote address. In Proceedings of the 2003 IEEE Workshop on Internet Applications, June 2003, pp. 2-10.

43. "Safe staging for computer security." A. Whitten and J. D. Tygar. In 2003 Workshop on Human-Computer Interaction and Security Systems, April 2003 (online).

44. "Expander graphs for digital stream authentication and robust overlay networks." D. Song, D. Zuckerman, and J. D. Tygar . In Proceedings of the 2002 IEEE Symposium on Security and Privacy, May 2002, pp. 258-270.

45. "ELK: A new protocol for efficient large-group key distribution." A. Perrig, D. Song, and J. D. Tygar. In Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001, pp. 247-262.

46. "Efficient and secure source authentication for multicast." A. Perrig, R. Canetti, D. Song, and J. D. Tygar. In Proceedings of the Internet Society Network and Distributed System Security Symposium (NDSS 2001), February 2001, pp. 35-46.

47. "Efficient authentication and signing of multicast streams over lossy channels." A. Perrig, R. Canetti, J. D. Tygar, and D. Song. In Proceedings

of the 2000 IEEE Symposium on Security and Privacy, May 2000, pp. 56-73.

48. "Why Johnny can't encrypt: A usability evaluation of PGP 5.0." A. Whitten and J. D. Tygar. In Proceedings of the 8th USENIX Security Symposium, August 1999. See also item 78.

49. "Flexible and scalable credential structures: NetBill implementation and experience." Y. Kawakura, M. Sirbu., I. Simpson, and J. D. Tygar In Proceedings of the International Workshop on Cryptographic Techniques and E-Commerce, July 1999, pp. 231-245.

50. "Open problems in electronic commerce." J. D. Tygar. In Proceedings of the 18th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS 1999), May 1999, p. 101.

51. "Electronic auctions with private bids." M. Harkavy, J. D. Tygar, and H. Kikuchi. In Proceedings of the 3rd USENIX Workshop on Electronic Commerce, September 1998, pp. 61-75.

52. "Atomicity vs. Anonymity: Distributed Transactions for Electronic Commerce." J. D. Tygar. In Proceedings of the 24th International Conference on Very Large Data Bases, August 1998, pp. 1-12.

53. "Smart cards in hostile environments." H. Gobioff, S. Smith, J. D. Tygar, and B. Yee. In Proceedings of the 2nd USENIX Workshop on Electronic Commerce, November 1996, pp. 23-28. (An early version appeared as CMU technical report CMU-CS-95-188.)

54. "Anonymous atomic transactions." L. J. Camp, M. Harkavy, and B. Yee. In Proceedings of the 2nd USENIX Workshop on Electronic Commerce, November 1996, pp. 123-133. (An early version appeared as CMU technical report CMU-CS-96-156.)

55. "Model checking electronic commerce protocols." N. Heintze, J. D. Tygar, J. Wing, and H. Wong. In Proceedings of the 2nd USENIX Workshop on Electronic Commerce, November 1996, pp. 147-164.

56. "WWW electronic commerce and Java Trojan horses." J. D. Tygar and A. Whitten. In Proceedings of the 2nd USENIX Workshop on Electronic

Commerce, November 1996, pp. 243-250.

57. "Building blocks for atomicity in electronic commerce." J. Su and J. D. Tygar. In Proceedings of the 6th USENIX Security Symposium, July 1996, pp. 97-104.

58. "Token and notational money in electronic commerce." L. J. Camp, M. Sirbu, and J. D. Tygar. In Proceedings of the 1st USENIX Workshop on Electronic Commerce, July 1995, pp. 1-12. (An early version was presented at the Telecommunications Policy Research Conference, October 1994.)

59. "NetBill security and transaction protocol." B. Cox, J. D. Tygar, and M. Sirbu. In Proceedings of the 1st USENIX Workshop on Electronic Commerce, July 1995, pp. 77-88.

60. "Secure coprocessors in electronic commerce applications." B. Yee and J. D. Tygar. In Proceedings of the 1st USENIX Workshop on Electronic Commerce, July 1995, pp. 155-170.

61. "Completely asynchronous optimistic recovery with minimal rollbacks." S. Smith, D. Johnson, and J. D. Tygar. In Proceedings of the 25th IEEE Symposium on Fault-Tolerant Computing, June 1995, pp. 361-370. (An early version appears as CMU technical report CMU-CS-94-130.)

62. "A fast off-line electronic currency protocol." L. Tang and J. D. Tygar. In CARDIS 94: Proceedings of the First IFIP Smart Card Research and Advanced Application Conference, October 1994, pp. 89-100.

63. "Security and privacy for partial order time." S. Smith and J. D. Tygar. In Proceedings 1994 Parallel and Distributed Computing Systems Conference, October 1994, pp. 70-77. (Early versions appeared as CMU Computer Science technical reports CMU-CS-93-116 and CMU-CS-94-135.)

64. "Certified electronic mail." A. Bahreman and J. D. Tygar. In Proceedings of the Network and Distributed Systems Security Conference (NDSS 1994), February 1994, pp. 3-19.

65. "Miro tools." A. Heydon, M. Maimone, A. Moormann, J. D. Tygar and J. Wing. In Proceedings 3rd ACM Workshop on Visual Languages, October 1989, pp. 86-91. (A preprint appeared as CMU Computer Science technical

reports CMU-CS-89-159.)

66. "Constraining pictures with pictures." A. Heydon, M. Maimone, A. Moormann, J. D. Tygar, and J. Wing. In Information Processing 89: Proceedings of the 11th World Computer Congress, August 1989, pp. 157-162. (An early version appeared as CMU Computer Science technical report CMU-CS-88-185.)

67. "Miro: A Visual Language for Specifying Security: abstract." M. Maimone, A. Moorman, J.D. Tygar, J. Wing. Proceedings of the (First) USENIX UNIX Security Workshop, August 1988, p. 49."

68. "StrongBox: Support for Self-Securing Programs: abstract." J. D. Tygar, B. Yee, and A. Spector. In Proceedings of the (First) USENIX UNIX Security Workshop, August 1988, p. 50.

69. "How to make replicated data secure." M. Herlihy and J. D. Tygar. In Proceedings of CRYPTO-87, ed. C. Pomerance, 1988, pp. 379-391. (An early version appeared as CMU Computer Science Technical Report CMU-CS-87-143.)

70. "Visual specification of security constraints." J. D. Tygar and J. Wing. In Proceedings 1st ACM Workshop on Visual Programming, 1987. (Another version appeared as CMU Computer Science Technical Report CMU-CS-87-122.)

71. "Efficient netlist comparison using hierarchy and randomization." J. D. Tygar and R. Ellickson. In Proceedings 22nd ACM/IEEE Design Automation Conference, Las Vegas, NV, July 1985, pp. 702-708.

72. "Hierarchical logic comparison," with R. Ellickson. In Proceedings MIDCON, 1984.

Other Conference Publications:

73. "Notes from the Second USENIX Workshop on Electronic Commerce." M. Harkavy, A. Meyers, A. Whitten, and H. Wong. In Proceedings of the 3rd

USENIX Workshop on Electronic Commerce, September 1998.

74. "How are we going to pay for this? Fee-for-service in distributed systems -- research and policy issues." C. Clifton, P. Gemmel, E. Means, M. Merges, J. D. Tygar. In Proceedings of the 15th International Conference on Distributed Computing Systems, May 1995, pp. 344-348.

Standards Documents:

75. TESLA: Multicast Source Authentication Transform Introduction. A. Perrig, R. Canetti, D. Song, B. Briscoe. Current version dated 1 August 2004.

76. Performance Criteria for Information-Based Indicia and Security Architecture for Closed IBI Postage Metering Systems (PCIBI-C) (Draft). United States Postal Service. January 1999. (Note: I was a major contributor to this document.)

77. Performance Criteria for Information-Based Indicia and Security Architecture for Open IBI Postage Evidence Systems (PCIBI-O) (Draft). United States Postal Service. February 2000. (Note: I was a major contributor to this document.)

78. "Production, Distribution, and Use of Postal Security Devices and Information Based Indicia." United States Postal Service. Federal Register 65:191, October 2, 2000, pp. 58682-58698. (Note: I was a major contributor to this document.)

Technical Reports (does not include items listed above)

79. Usability of Security: A Case Study. A. Whitten and J. D. Tygar. CMU Computer Science technical report CMU-CS-98-155, December 1998. (Note: this report partly overlaps item 48, but also includes substantial additional material not included in item 48.)

80. Security for Network Attached Storage Devices. H. Gobioff, G. Gibson and J. D. Tygar. CMU Computer Science technical report CMU-CS-97-185,

October 1997.

81. Cryptography: It's Not Just for Electronic Mail Anymore. J. D. Tygar and B. Yee. CMU Computer Science technical report CMU-CS-93-107, March 1993. (See also item 12 above.)

82. Median separators in d dimensions. J. Sipelstein, S. Smith, and J. D. Tygar . CMU Computer Science technical report CMU-CS-88-206, December 1988.

83. When are Best Fit and First Fit Optimal? C. McGeogh and J. D. Tygar. CMU Computer Science technical report CMU-CS-87-168, October 1987.

84. Display Manager User's Guide. J. D. Tygar. Valid Logic Systems engineering memorandum, VED-050682-1-JDT, May 1982.

85. Performance analysis of the DANTE Network. Bell Telephone Laboratories technical memorandum, August 1981.

Patents:

86. Anonymous certified delivery. L. J. Camp, J. D. Tygar, and M. Harkavy. US Patent 6,076,078, June 13, 2000.

87. Method and apparatus for purchasing and delivering digital goods over a network. M. Sirbu, J. D. Tygar, B. Cox, T. Wagner. US Patent 5,809,144, September 15, 1998.

Miscellaneous:

88. Security with Privacy. Information Science and Technology Study Group on Security and Privacy (chair: J. D. Tygar). December 2002

89. Expert Report of J. D. Tygar ... A&M Records et al v. Napster.... J. D. Tygar. (For Hearing) July 2000.

附件(五) Virgil D. Gligor

Professor
Department of Electrical and Computer Engineering
University of Maryland at College Park

Chair, ACM SIGSAC

Chairs of numerous conferences

Editors of number journals

2005 National Information Security Award, USA (the most prestigious award in security)

Mailing Address:

Virgil D. Gligor
Dept. of Electrical and Computer Engineering
University of Maryland
College Park, MD 20742
Phone: (301) 405-3647
gligor@eng.umd.edu
http://www.ee.umd.edu/~gligor

Education

- B.Sc ('72), M.Sc. ('73), Ph.D ('76), University of California, Berkeley

Teaching

- Security in Distributed Systems and Networks ENEE757

Research Interests

- Network and Distributed Systems Security
- Distributed systems

Recent Research

90. Security of Emergent Properties in Ad-Hoc Networks (.ps) (.pdf) (Proc. of the Security Protocols Workshop, Sidney Sussex College, Cambridge, UK, April, 2004. To appear in Lecture Notes in Computer Science, Springer-Verlag, 2005.)
91. Guaranteeing Access in Spite of Service-Flooding Attacks (.ps) (.pdf) (Proc. of the Security Protocols Workshop, Sidney Sussex College, Cambridge, UK, April 2-4, 2003. To appear in Lecture Notes in Computer Science, Springer-Verlag, 2004.)
92. A Key-Management Scheme for Distributed Sensor Networks (.ps) (Proc. of the 9th ACM Conference on Computer and Communication Security, Washington D.C., November 2002.)
93. Bootstrapping Security Associations for Routing in Mobile Ad-Hoc Networks (.ps) Institute for Systems Research, ISR Technical Report 2002-44, May 2002.(also available at http://bellatrix.isr.umd.edu/TechReports/ISR/2002/TR_2002-44/TR_2002-44.pdf)
94. On Trust Establishment in Mobile Ad-Hoc Networks (.ps) (Proc. of the Security Protocols Workshop, Cambridge, UK, April 2002. To appear in Lecture Notes in Computer Science, Springer-Verlag, 2003.)
95. Reasoning about Joint Administration of Access Policies for Coalition Resources (.pdf) (Proc. of IEEE Int. Conf. On Distr. Computing (ICDCS), pp. 429, Vienna, Austria, July 2002)
96. On Message Integrity in Symmetric Encryption (.ps) (unpublished manuscript) February 2002.
97. A Note on NSA's Dual Counter Mode of Encryption (.ps) (.pdf)
Specification of Dual Counter Mode (.pdf)
and NSA's response (.html)
98. On Message Integrity in Symmetric Encryption (.ps) (Presented at the NIST Workshop on AES Modes of Operation, Baltimore, Maryland, October 20, 2000)
99. Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes (.ps) (Presented at the 2nd NIST Workshop on AES Modes of Operation, Santa Barbara, CA, August 24, 2001)
100. On the Negotiation of Access Control Policies (.ps) (Proc. of the Security Protocols Workshop, Cambridge, UK, April 2001. Lecture Notes in Computer Science, Springer-Verlag, 2002.)
101. Enforcing Dependencies between PKI Certificates in ad-hoc Networks, (.ps) (IEEE International Conference on Telecommunications, Bucharest, Romania, June 2001, pp. 293-298.)

102. Review and Revocation of Access Privileges Distributed with PKI Certificates (.ps) (Proc. of the Security Protocols Workshop, Cambridge, UK, April 2000, Lecture Notes in Computer Science vol. 2133, Springer-Verlag, 2001.)
103. Application-Oriented Security Policies and their Composition (.ps) (Proc. of the Security Protocols Workshop, Cambridge, UK, April 1998, Lecture Notes in Computer Science vol 1550, Springer-Verlag 1999)

104. On the Formal Definition of Separation of Duty Policies and their Composition (.ps) (Proc. of the 1998 IEEE Symposium on Security and Privacy, Berkeley, CA. May 1998.)

附件(六) Jeannette M. Wing

President's Professor of Computer Science
Computer Science, Department Head, CMU

Contact Information

Address: Computer Science Department, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213
Phone: 412-268-3068 (office) 412-260-8926 (cell)
Fax: 412-268-5577
Email: wing@cs.cmu.edu

Research Interests

Software specification and verification, security, concurrent and distributed systems, programming languages, programming methodology.

Publications (complete list).

Selected Recent Publications

Security

1. Game Strategies in Network Security, Kong-wei Lye and Jeannette Wing, International Journal of Information Security, February 2005. Our shorter conference version, Proceedings of Foundations of Computer Security Workshop, July 26, 2002, Copenhagen, Denmark; our technical report CMU-CS-02-136, May 2002.
2. Measuring A System's Attack Surface, Pratyusa Manadhata and Jeannette Wing, CMU-TR-04-102, January 2004.
3. Tools for Generating and Analyzing Attack Graphs, Oleg Sheyner and Jeannette Wing, Proceedings of Formal Methods for Components and Objects, Lecture Notes in Computer Science, 2004, pp. 344-371.
4. Measuring Relative Attack Surfaces, Michael Howard, Jon Pincus, and Jeannette Wing, Proceedings of Workshop on Advanced Developments in Software and Systems Security, available as CMU-TR-03-169, August 2003.
5. Beyond the Horizon: A Call to Arms, Jeannette M. Wing, IEEE Security and Privacy. November/December 2003, pp. 62-67.

6. Verifiable Secret Redistribution for Archive Systems, Theodore M. Wong, Chenxi Wang, and Jeannette M. Wing, Proceedings of the First International Security in Storage Workshop, Maryland, December 2002. .ps version.
7. Verifiable Secret Redistribution for Threshold Sharing Schemes, Theodore M. Wong, Chenxi Wang, and Jeannette M. Wing. Earlier version available as CMU-CS-02-114 Technical Report, February 2002.
8. Minimization and Reliability Analyses of Attack Graphs, Somesh Jha, Oleg Sheyner, and Jeannette M. Wing. CMU-CS-02-109, February 2002. This is a detailed version of our paper in Proceedings of the Computer Security Foundations Workshop, Nova Scotia, June 2002, pp. 49-63.
9. Automated Generation and Analysis of Attack Graphs, Oleg Sheyner, Somesh Jha, and Jeannette M. Wing, Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 2002.
10. Survivability Analysis of Networked Systems, Somesh Jha and Jeannette M. Wing, Proceedings of the International Conference on Software Engineering, Toronto, May 2001. Earlier version available as CMU-CS-00-168, October 2000.
11. Composing Proofs of Security Protocols Using Isabelle/IOA, Oleg Sheyner and Jeannette M. Wing, Theorem Proving for Higher Order Logics Workshop, August 2000. Long version with proofs available as CMU-CS-00-106.
12. A Comparison and Combination of Theory Generation and Model Checking for Security Protocol Analysis, Nicholas J. Hopper, Sanjit A. Seshia, and Jeannette M. Wing, Workshop on Formal Methods and Security, July 2000.
13. Survivability Analysis of Network Specifications, Somesh Jha, Richard Linger, Tom Longstaff, and Jeannette Wing, Proceedings of the International Conference on Dependable Systems and Networks, Workshop on Dependability Despite Malicious Faults, New York City, NY, June 25-28, 2000.
14. Theory Generation for Security Protocols, Darrell Kindred and Jeannette M. Wing, July 1999. Work in progress.
15. Fast, Automatic Checking of Security Protocols, Darrell Kindred and Jeannette M. Wing, Proc. of the USENIX 1996 Workshop on Electronic Commerce, November 1996.

Distributed Systems, Fault Tolerance

16. A Nitpick Analysis of Mobile IPv6, Daniel Jackson, Yuchung Ng, and Jeannette Wing, Formal Aspects of Computing. Also available as CMU-CS-98-113, March 1998.
17. A Case Study in Model Checking Software Systems, Jeannette M. Wing and Mandana Vaziri-Farahani, Science of Computer Programming, vol. 28, 1997, pp. 273-299.
18. Avalon/C++, David L. Detlefs, Maurice P. Herlihy and Jeannette M. Wing, in Advanced Language Implementation: Recent Research at Carnegie Mellon University, P. Lee, editor, MIT Press, 1991.
19. The Avalon Language, Jeannette M. Wing et al., Part IV, Chapters 19-22, in Camelot and Avalon: A Distributed Transaction Facility, J. Eppinger, L. Mummert and A. Spector, editors, Morgan Kaufmann Publishers, Inc., 1991.

Subtyping, Interface Specifications

20. Respectful Type Converters, Jeannette M. Wing and John Ockerbloom, IEEE Transactions on Software Engineering, July 2000. Also CMU-CS-98-130.
21. Behavioral Subtyping Using Invariants and Constraints, Barbara H. Liskov and Jeannette M. Wing, Formal Methods for Distributed Processing: An Object Oriented Approach, H. Bowman and J. Derrick, editors, Cambridge University Press. Also CMU-CS-99-156, July 1999.
22. Respectful Type Converters For Mutable Types, Jeannette M. Wing and John Ockerbloom, Foundations of Component Based Systems, G. Leavens and M. Sitaraman, editors, Cambridge University Press. Also CMU-CS-99-142, June 1999.
23. Specification Matching Software Components, Amy Moormann Zaremski and Jeannette M. Wing, ACM Transactions on Software Engineering and Methodology, October 1997.
24. A Behavioral Notion of Subtyping, Barbara H. Liskov and Jeannette M. Wing, ACM Transactions on Programming Languages and Systems, November 1994.

Formal Methods (General)

25. Formal Methods: State of the Art and Future Directions, Edmund M. Clarke and Jeannette M. Wing, report by the Working Group on Formal Methods for the ACM Workshop on Strategic Directions in Computing Research, ACM Computing Surveys, vol. 28, no. 4, December 1996, pp. 626-643. Also CMU-CS-96-178.

26. Related talk: Formal Methods: Past, Present, and Future, Keynote Address at ASIAN'98, Manila, The Philippines, December 10, 1998; Distinguished Lecturer at DePaul University, October 2, 1998; Invited Speaker at the Fourth Software Reuse Symposium, August 19, 1998; Distinguished Lecturer at University of Washington, February 19, 1998.
27. A Symbiotic Relationship Between Formal Methods and Security, Jeannette M. Wing, Proceedings from Workshops on Computer Security, Fault Tolerance, and Software Assurance: From Needs to Solution, CMU-CS-98-188, December 1998.

Formal Methods (Education)

28. Mathematics in Computer Science Curricula (Abstract), Jeannette M. Wing, in Proceedings of the 6th International Conference, Mathematics of Program Construction 2002, Dagstuhl Castle, Germany, July 2002.
29. Weaving Formal Methods into the Undergraduate Computer Science Curriculum (Extended Abstract), Jeannette M. Wing, in Proceedings of the 8th International Conference on Algebraic Methodology and Software Technology (AMAST) 2000, pp. 2-7, May 2000. Slides of invited talk, for Education Day.
30. Hints to Specifiers, Jeannette M. Wing, in Teaching and Learning Formal Methods, Dean and Hinchey, editors, Academic Press, 1996, Chapter 5, pp. 57-77. Also available as CMU-CS-95-118R, May 1995.

附件(七) Ravishankar K. Iyer

255 Computer & Systems Research Laboratory
MC 228
1308 West Main Street
Urbana, IL 61801
Tel: (217) 333-7774
Fax: (217) 244-5686
Email: iyer@crhc.uiuc.edu

PROFESSIONAL EMPLOYMENT

Director, Coordinated Science Laboratory, University of Illinois , February 2000-present.
George and Ann Fisher Distinguished Professor of Electrical and Computer Engineering, University of Illinois,
1998-present.
Director, Motorola Center for Communication, 2000-present.
Professor of Electrical and Computer Engineering, Research Professor of Coordinated Science Laboratory, and
Professor of Computer Science, University of Illinois, 1989-present.
Honorary Professor, School of Information Technology and Electrical Engineering, University of Queensland,
Brisbane, Australia, November 2003 – December 2006.
Visiting Professor, University of New South Wales, Australia, August – December 2002.
Visiting Professor, University of Queensland, Brisbane, Australia, January – August 2002.
Acting Director, Coordinated Science Laboratory, University of Illinois, 1995-1996.
Co-Director, Center for Reliable and High-Performance Computing, University of Illinois, 1989-present.
Director and Principal Investigator, Multi-University (UIUC/Stanford/Texas A&M/UT-Austin) DARPA Project on
Design for Dependability, 1994-1998.
Co-Director, Illinois Computer Laboratory for Aerospace Systems and Software (ICLASS),
National Aeronautics and Space Administration (NASA) Center for Excellence in Aerospace Computing, 1985-1998.
Distinguished Visiting Professor, University of Queensland, Brisbane, Australia, August – December 1993.

Visiting Humboldt Foundation Professor, University of Erlangen-Nurnberg, Germany, 1992-1993.
Visiting Professor, University of Queensland, Brisbane, Australia, 1991.
Distinguished Visitor/Lecturer, Goethe University of Frankfurt, University of Kaiserslauten, West Germany, 1987.
Visiting Scientist, IBM Research Laboratory, Zurich, Switzerland, February-August 1987.
Visiting Professor, Laboratoire d'Automatique et d'Analyse des Systemes (LAAS-CNRS),
Toulouse, France, June 1987.
Associate Professor of Electrical and Computer Engineering,
Research Associate Professor of Coordinated Science Laboratory,
Associate Professor of Computer Science,
University of Illinois, 1985-1989.
Assistant Professor of Electrical and Computer Engineering,
Research Assistant Professor of Coordinated Science Laboratory,
University of Illinois, 1983-1985.
Computer Systems Laboratory, Stanford University, 1981-1983.
Acting Assistant Professor and Research Associate, Department of Electrical Engineering, Stanford University, 1980-
1983.
Visiting Scholar, Stanford University, October 1979-August 1980.
Royal Norwegian Council for Scientific and Industrial Research:
Research Fellow, Norwegian Institute of Technology, University of Trondheim, Norway, 1978-1979.
Tutor (Graduate Assistant) in Electrical Engineering, University of Queensland, 1973-1977.

AWARDS AND HONORS

IEEE Emanuel R. Piore Award “for fundamental contributions to measurement, evaluation, and design of reliable
computing systems ,” June 2001.
IBM Partnership Award, 1998.
American Institute of Aeronautics and Astronautics (AIAA) Information Systems Award and Medal “for fundamental
and pioneering contributions towards the design, evaluation, and validation of dependable aerospace computing
systems,” 1993.
Humboldt Foundation Senior Distinguished U.S. Scientist Award “in recognition of

scientific achievement in research
and teaching," 1991.
Fellow, Institute of Electrical and Electronics Engineers (IEEE), 1990.
Fellow, Association for Computing Machinery (ACM).
American Institute of Aeronautics and Astronautics (AIAA) Distinguished Service Certificate, 1997.
IEEE Computer Society 1995 commemorative volume highlighting the best papers of the past 25 years in fault-tolerant
computing:
- "A Statistical Load Dependency Model for CPU Errors at SLAC," R. K. Iyer and D. J. Rossetti (1982)
- "Simulation of Software Behavior under Hardware Faults," K. Goswami and R. K. Iyer (1993)

Best Paper Award for "FAMAS: Fault Modeling via Adaptive Simulation," H. Jin, R.K. Iyer, M.C. Hsueh, and M.
Covington, The Tenth International Conference on VLSI Design, 1997.
Best Paper Award for "Analyze-NOW—An Environment for Collection and Analysis of Failures in a Network of
Workstations," A. Thakur and R. K. Iyer, International Symposium on Software Reliability Engineering, 1996.
University of Illinois Engineering Council Excellence in Advising Award, 1994, 1996, 2001.
Listed in *Who's Who in America* and in *Who's Who in the World*.
Associate Fellow, AIAA, 1992.
Distinguished Visitor of the IEEE Computer Society, 1989-present.
Outstanding Contribution Award, 19th International Symposium on Fault-Tolerant Computing, June 1989.
Distinguished International Lecturer, International Computer Foundation, Japan, 1988.
Royal Norwegian Council for Scientific and Industrial Research Fellowship, 1977 (for work at the Norwegian Institute
of Technology, Trondheim; ten awards encompassing science and engineering).
Member, Sigma Xi Honor Society, 1980.
Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia Postdoctoral Research Award,
1978 (five or six awards encompassing mathematics, science, and engineering).
International prize and plaque for a graduate research paper, IEEE Student Paper Contest, 1977 (two prizes awarded
internationally).
Best Australian student paper, IEEE prize, 1977 (one prize awarded in Australia).

SELECTED PROFESSIONAL ACTIVITIES

IEEE Computer Society Fellow Evaluation Committee.
IEEE Reliability Society Fellow Evaluation Committee
Founding Chair, Steering Committee, IEEE International Performance and Dependability Symposium (IPDS), 1995.
Technical Program Chair, The Silver Jubilee (25th) International Symposium on Fault-Tolerant Computing (FTCS-25),
Toulouse, France, June 1995.
Executive Committee, IEEE Youth Forum in Computer Science and Engineering (YUFORIC), 1998-present.
Chair, IEEE Technical Committee on Fault -Tolerant Computing, 1996-1998.
General Chair, 2nd Annual IEEE International Computer Performance and Dependability Symposium (IPDS'96),
Urbana, Illinois, September 4-6, 1996.
Technical Chair, International Conference on Algorithms and Architectures for Parallel Processing, Brisbane,
Australia, April 19-21, 1995
Technical Program Chair, IEEE International Computer Performance and Dependability Symposium (IPDS'95),
Erlangen, Germany, April 24-26, 1995.
Technical Expert, NASA Space Station Advisory Council, 1990-1994.
Advisory Board, IEEE Technical Committee on Fault -Tolerant Computing, 1990-present.
Computer Science Accreditation Board (CSAB) and Accreditation Board for Engineering and Technology (ABET),
Program Evaluator.
Editorial Board, *IEEE Transactions on Parallel and Distributed Systems*, 1992-1996.
Editorial Board, *International Journal on Electronic Testing Theory and Applications (JETTA)*, 1992-1997.
Editorial Advisory Board, IFIP Series on Dependable Computing.
Chair, Bell-Canada, University Research Review Panel, 1990.
General Chair, 19th International Symposium on Fault-Tolerant Computing (FTCS-19), Chicago, Illinois, June 1989.
Program Committee, International Symposium on Fault-Tolerant Computing (FTCS), 1983-present.
Advisory Committee, Center for Excellence, Information Systems Engineering and Management, Tennessee State
University, 1991.
Technical Committee, International Federation for Information Processing (IFIP)

(WG 10.4) on Reliable and Fault-
Tolerant Computing, 1984-present.
Founding Member, AIAA Computer Systems Standards Committee, 1990.
Editor-In-Chief, *IEEE Transactions on Dependable and Secure Computing*, 2003-present.

LIST OF PUBLICATIONS

Books and Chapters in Books

1. R. K. Iyer and T. Downs, "A Variance Minimization Method of Reliability Design," Circuit Theory and
2. Design, C. S. Moschytz and J. Neirynck, Eds., Georgi Publishing Company, St. Saphorin, Switzerland, 1978.
3. J. A. Abraham, G. Metze, R. K. Iyer and J. H. Patel, "The Evolution of Fault -Tolerant Computing at the University of Illinois," The Evolution of Fault-Tolerant Computing, A. Avizienis, J.-C. Laprie, and H. Kopetz, Eds., Volume 1 in the series Dependable Computing and Fault-Tolerant Systems, Springer-Verlag: New York, pp. 271-288, 1987.
4. M.-C. Hsueh, R. K. Iyer and K. S. Trivedi, "A Measurement-Based Performability Model for a Multiprocessor System, " Mathematical Computer Performance and Reliability, G. Iazeolla , P.J. Courtois, and O.J. Boxma, Eds ., Elsevier Science Publishers B.V.: North Holland, pp. 337-352, 1988.
5. R. L. Llames and R. K. Iyer, "Memory Management and Usage in a Lisp System: A Measurement-Based
6. Study," Computers for Artificial Intelligence Processing, B. Wah and C. V. Ramamo orthy, Eds., John Wiley& Sons: New York, pp. 119 -170, 1990.
7. G. Choi, R. K. Iyer, R. Saleh and V. A. Carreno, "A Fault Behavior Model for an Avionic Microprocessor," Dependable Computing for Critical Applications, A. Avizienis and J. -C. Laprie, Eds., Volume 4 in the series Dependable Computing and Fault-Tolerant Systems, Springer-Verlag: New York, 1990.
8. R. K. Iyer, J. H. Patel, W. K. Fuchs, P. Banerjee and R. Horst, "Hardware and Software Fault Tolerance,"Encyclopedia of Microcomputers, Marcel Dekker: New York, 1991.
9. D. Tang and R. K. Iyer, "Impact of Correlated Failure s on Dependability in a VAXcluster System," Dependable Computing for Critical Applications 2 , J. F. Meyer and R. D. Schlichting, Eds., Volume 6 in the series Dependable Computing and Fault -Tolerant Systems, Springer-Verlag: New York, pp. 175 -194, 1992.

10. L. T. Young, R. K. Iyer, K. K. Goswami and C. Alonso, “A Hybrid Monitor Assisted Fault Injection Environment,” Dependable Computing for Critical Applications 3 , C. E. Landwehr, B. Randell, and L. Simoncini, Eds., Volume 8 in the series Dependable Computing a nd Fault-Tolerant Systems, Springer-Verlag: New York, pp. 281-318, 1993.
11. R. K. Iyer and D. Tang, “Measurement-Based Dependability Evaluation o f Operational Computer Systems,” Foundations of Ultradependable Computing: Volume II: System Design and Evaluation, G. M. Koob and C. G. Lau, Eds., Kluwer Academic Publishers, 1994.
12. R.K. Iyer and I. Lee “ Software Fault Tolerance in Computer Operating Systems,” Software Fault Tolerance , Michael Lyu, Ed., Volume 3 in the series Trends in Software, B. Krithnamurthy, Ed., Wiley, 1995.
13. W-L. Kao and R. K. Iyer, “ DEFINE: A Distributed Fault Inject ion and Monitoring Environment,” Fault- Tolerant Parallel and Distributed Systems, D. Pradhan and D. Avresky, Eds., IEEE Computer Society Press, 1995.
14. R. K. Iyer and I. Lee, “Measurement-Based Analy sis of Software Reliability,” McGraw-Hill Handbook of
15. Software Reliability Engineering, Chapter 8, M.R. Lyu, Ed., McGraw-Hill, pp. 303 -358, 1996.
16. 13. R. K. Iyer and D. Tang, “ Experimental Analysis of Computer System Dependability,” Fault-Tolerant
17. Computer System Design, second edition, D. K. Pradhan, Ed., Prentice Hall, 1996.
18. S. H. VanderLeest and R.K. Iyer, “ Heterogeneous I/O Contention in a Single -Bus Multiprocessor,” Input/Output in Parallel and Distributed Systems, R. Jain, J. Werth and J. C. Browne, Eds., Kluwer Academic Publishers, 1996.
19. R. K. Iyer, “Foolproof and Incapable of Error? Reliable Computing,” HAL's Legacy: 2001's Computer as
20. Dream and Reality, D. Stork, Ed., MIT Press, 1996. Japanese translation, 1997.
21. R. K. Iyer, M. Morganti, W. K. Fuchs and V. Gligor, Eds., “ Dependable Computing for Critical Applications
22. Dependable Computing and Fault-Tolerant Systems, Volume 10, IEEE Computer Society Press, 1998.
23. G. Ries and R. K. Iyer, “ Evaluating the Impact of Transient Faults on Software Behavior: Case Study of a Commercial, High-Speed Network,” Dependable Computing for Critical Applications 6 , M. Dal Cin, C. Meadows and W. H. Sanders, Eds., Volume 11 in the series Dependable Computing and Fault-Tolerant Systems, IEEE Computer Society Press, 1998.

24. R. K. Iyer, Z. Ka lbarczyk and M. Kalyanakrishnan, “Measurement-based Analysis of Networked System Availability,” Performance Evaluation: Origins and Directions, G. Haring, C. Lindemann and M. Reiser, Eds., Springer-Verlag, 1999.
25. R. K . Iyer, “Computer Equipment Testing," Encyclopedia of Electrical Engineering, John Wiley and Sons, 2001.