Xinwen Zhang, Ph.D.

Contact Information

Enterprise Security Group, Mobile Communication Lab
Samsung Research America
Mountain View, CA 94043

xinwenzhang@gmail.com
http://profsandhu.com/zhang

Professional Experience

Sr. Director of R&D, Samsung Research, Mountain View, CA 07/2013 – 05/2015
Sr. Staff Researcher, Huawei America Research Center, Santa Clara, CA 10/2010 – 07/2013
Staff Engineer, Samsung Information System America, San Jose, CA 09/2006 - 10/2010
Development Engineer, CE-Infosys Pte. Ltd., Singapore 05/2000 – 09/2000
Software Engineer, Yulong Communication Ltd., Shenzhen, China, 03/1998 – 06/1998

Expertise & Interests

System security policies, models, architectures, and mechanisms
Security enhanced Android platforms and mobile device management
Security and privacy in cloud computing
Security and privacy in Internet and future Internet architecture

Education

Ph.D., **George Mason University**, Fairfax, Virginia, USA 2001 - 2006

- Advisor: Prof. Ravi Sandhu
- Thesis: Formal Model and Safety Analysis of Usage Control Security Model

M. Eng., Nanyang Technological University, Singapore 1998 - 2000
B. Eng. & M. Eng., Huazhong University of Science & Technology, Wuhan, China 1991 - 1998

Honours & Awards

`President Technical Recognition Award`, Huawei Technologies (team award), 2011
`Best Paper Award`, Mobilware, 2010
`Best Paper Nominated`, ACM WiSec, 2010
`Best Paper Award`, Samsung Technological Conference, 2009
`Technical Recognition Award`, Samsung Information System America, 2008
`Inventor of Samsung`, Samsung Information System America, 2008

Industry & Research Projects

Secure Mobile Enterprise

Develop Samsung Knox platfrom for mobile device management (MDM) systems and enterprise application security. `https://www.samsungknox.com/` 2013 -

Internet Security

Trust, Security, and Privacy in Future Internet Architectures 2010 - 2013

Role: Security architect and leading prototype developer

Naming schema for information-centric network architectures (ICN), name-based trust management and security, secure neighbor discovery, secure device-to-device service discovery among mobile devices, encryption-based access control for data confidentiality, user access privacy protection. Large-scale information flow control in ICN. (***Partial results have been transferred to product team and deployed in a large operator's network***)

Internet Routing Security 2011 - 2013

Role: Security architect and leading researcher

Survey BGP security proposals (S*-BGP). Identity collaborative routing attacks by mulitple ASes that cannot be detected and prevented by current secure BGP protocols. Propose and develop packet watermark mechanism to detect routing attacks. Propose low complexity and lightweight trusted BGP protocol with transitive trust among AS routers.

Cloud and Web Service Security

Access Control as a Service for Enterprise Cloud 2012

Role: Security architect

Design service-oriented architecture for enforcing role-based access control (RBAC) policies for enterprises in public cloud environment. Extend Amazon Identity and Access Management (IAM) for RBAC-as-a-Service. Design general architecture for Authorization-as-a-Service model (support multiple types of access control models - e.g., MLS, RBAC).

Secure Data Storage and Sharing in Public Cloud 2010 - 2012

Role: Security architect and developer

Define security requirements for outsourcing data from enterprise IT to public cloud. Novel solutions for secure data storage and processing in public clouds. Policy-based encryption scheme for outsourcing data from enterprise to public cloud. delegated encryption and access control for secure data processing; proxy-based data encryption for secure content distribution and flexible data sharing between cloud customers.

Distributed Authorization Mechanisms for Web Applications 2009 - 2011

Role: Leading researcher and system architect Lead the design of authentication and authorization solutions for distributed web applications between client (mobile devices) and cloud platforms. Propose delegated authorization (DAuth) extended from OAuth for distributed web consumers with principle of least privilege. Propose flexible and user-centric authorization model (MAuth) for multi-mashup web applications. Lead the design and development of cross-domain access control and delegation framework (xDAuth) for web services.

Mobile Security

Android Permission Framework Extensions 2009

Role: Leading researcher

Extend Android permission framework to enable user selective permission control for Android applications downloaded from app stores. Flexible security policy can be defined for indiviaual apps to access system resources and phone functions. Develop an extra reference monitor layer to dynamic hook user/organizational access control policies into Android framework to augment pretermission control. Enable private model for Android platforms with mockable permissions.

Building Elastic Mobile Devices with Cloud Computing 2009 - 2010

Role: System architect and leading developer Design and develop middleware for smartphones to efficiently and seamlessly leverage elastic cloud computing resources. Lead security architecture design of elastic application and cloud-side infrastructure. Develop mobile applications on Android. Develop cloud platform and web applications with Amazon EC2.

Integrity Protection for Open Mobile Platforms 2007 - 2009

Role: Security architect and leading developer

Develop an integrity model based on open mobile operating system architecture and application behaviors, to confine the activities of untrusted codes from browser, Bluetooth, MMS, and MMC. Efficiently identify boundary between trusted and untrusted domains on mobile platforms to simplify security policy specification but still achieve high integrity assurance. Demonstrate effectiveness on malware prevention. The solution has been shipped with a commercially deployed Linux-based smartphone. (***Partial solution has been deployed on Samsung LiMo platforms***)

Towards Building Trusted Open Mobile Platforms 2006 - 2008

Role: Security architect and leading developer Design and deploy security model and reference monitor for next generation open mobile platform towards TCG Mobile Phone Reference Architecture. Extend traditional access control model with emerging trusted computing technology to build mandatory access control (MAC) mechanisms for Linux-based mobile devices. Build high assurance environment for mobile network provider and service providers. Design and develop security architecture and enforcement module for Linux Mobile (LiMo) platforms.

Security Foundations

Deploying Secure Distributed Systems using Trusted Computing Technology: Models, Architectures and Protocols 2004 - 2006
Sponsored by Intel Corporation *Role: Student Principal Investigator*
Participate as a student principal investigator of the cooperative project with Intel. Develop security model and trusted enforcement architecture for controlled information sharing and secure collaborations in distributed computing systems such as P2P, Grid, and Web Services. Investigate extending hardware-based root of trust to application level for security enforcement with mandatory access control and usage control models.

Formal Model and Safety Analysis of Access Control Models 2002 - 2005
Role: Research Assistant Define formal model and policy specification of UCON. Study the expressive power and safety properties of the authorization and obligation models in UCON. Investigate enforcement architecture and mechanisms of UCON in collaborative computing systems such as Grids and Web Services. Develop flexible administrative RBAC model under organization and enterprise environments. Develop permission-based delegation models for RBAC. Develop architecture and mechanisms for RBAC in distributed computing systems.

Teaching Experience

Instructor ISA767 Secure E-Commerce, `http://profsandhu.com/zhang/isa767` Fall 2005
Department of Information and Software Engineering, George Mason University

Teach Assistant, INFS766 Internet Security Protocols, INFS762 Information System Security
ISA767 Secure Electronic Commerce Fall 2001 - Spring 2004
Department of Information and Software Engineering, George Mason University

Academia Activities

PC Co-chair: IEEE CCNC Special Session, ACM STC 2012, TRUST 2012, ACM STC 2011
NSF Panel Review: 2012
Panelist: MobiCloud 2010 (with MobiCASE 2010)

PC Member: ACM TrustED 2014, IEEE ICC 2014, ACM CODASPY 2014, ACM CCS-SPSM 2013, ACM TrustED 2013, CANS 2013, IEEE TrustCom 2013, Sigcomm MCC 2013, TRUST 2013, DBSec 2013, IEEE MobileCloud 2013 HASP 2012, ACM SPSM 2012, ICNC 2013, CANS 2012, InTrust 2012, TrustCom 2012, ACM SACMAT 2012, ACM WiSec 2012, DBSec 2012, ACM CODASPY 2012, ICNC 2012, INTRUST 2011, TrustCom 2011, MSIS 2011, TRUST 2011, DBSec 2011, ACM WiSec 2011, ACM CODASPY 2011, ACM STC 2010, ICCIIS 2010, CollaboreteCom 2010, ChinaCom 2010, ACM SACMAT 2010, ACM STC 2009, ChinaCom 2009, ACM SACMAT 2009, MOTHIS 2008, ACM STC 2008, IS 2008, ACM SACMAT 2008, IEEE SUTC 2008, TRUST 2008, ACM STC 2007

Journal Review: IEEE Computer, IEEE Internet Computing, IEEE TDSC, IEEE TPDS, IEEE TMM, IEEE TMC, IEEE TSC, IEEE TSMC ACM TISSEC, Springer JNSM, IEICE Transactions on Information Systems, Elsevier Computer & Security, Springer Information Systems Frontiers Journal, Springer JONS, Wiley SCN

Publications

`https://scholar.google.com/citations?user=WyYnBkEAAAAJ&hl=en`

Referred Journal Articles and Book Chapters

1. Qi Li, Ravi Sandhu, Xinwen Zhang, and Mingwei Xu. Mandatory Content Access Control for Privacy Protection in Information Centric Networks. IEEE Transactions on Secure and Dependable Computing (TDSC) 14(5): 494-506 (2017).
2. Yacong Gu, Qi Li, Hongtao Zhang, Purui Su, Xinwen Zhang, Dengguo Feng, Direct Resource Hijacking in Android, Internet Computing, IEEE, 20(5):46-56, 2016.
3. Weiwen Zhang, Xinwen Zhang, and Yonggang Wen. Towards Virus Scanning as a Service in Mobile Cloud Computing: Energy-Efficient Dispatching Policy under N-Version

Protection. IEEE Transactions on Emerging Topics in Computing (TETC). Accepted.

4. Qi Li, Xinwen Zhang, Xin Zhang, and Purui Su. Invalidating Idealized BGP Security Proposals and Countermeasures. IEEE Transactions on Secure and Dependable Computing. Vol. 12, No. 3: 298-311, 2015.
5. Aziz Mohaisen, Hesham Mekky, Xinwen Zhang, Haiyong Xie, Yongdae Kim. Timing Attacks on Access Privacy in Information Centric Networks and Countermeasures. IEEE Transactions on Secure and Dependable Computing. 12(6): 675-687 (2015)
6. Qi Li, Xinwen Zhang, Qingji Zheng, Ravi Sandhu, Xiaoming Fu. LIVE: Lightweight Integrity Verification and Content Access Control for Named Data Networking. IEEE Transactions on Information Forensics and Security 10(2): 308-320 (2015)
7. Songqing Chen, Lei Liu, Xinyuan Wang, Xinwen Zhang, and Zhao Zhang. A Host-based Approach for Unknown Fast Spreading Worm Detection and Containment. ACM Transactions on Autonomous and Adaptive Systems (TAAS). Vol. 8, No. 4., 2014.
8. Ruoyu Wu, Xinwen Zhang, Gail-Joon Ahn, Hadi Sharifi, and Haiyong Xie. Design and Implementation of Access Control as a Service for IaaS Cloud. ASE Science Journal, Vol. 1, No. 3, 121-138 (2013).
9. Xingze He, Xinwen Zhang, and C.-C. Jay Kuo. A Distortion-Based Approach to Privacy-Preserving Metering in Smart Grids. IEEE Access. Vol 1: 67-78, 2013.
10. Xinwen Zhang, Jean-Pierre Seifert, and Onur Aciicmez. Design and Implementation of Efficient Integrity Protection for Open Mobile Platforms. IEEE Transactions on Mobile Computing (TMC). In Press.
11. Wenjuan Xu, Xinwen Zhang, Hongxin Hu, Gail-J. Ahn, and Jean-Pierre Seifert. Remote Attestation with Domain-based Integrity Model and Policy Analysis. IEEE Transactions on IEEE Transactions on Dependable and Secure Computing (TDSC). 9(3): 429-442 (2012).
12. Qi Li, Mingwei Xu, Jianping Wu, Xinwen Zhang, Patrick P. C. Lee, and Ke Xu. Enhancing the Trust of Internet Routing with Lightweight Route Attestation. IEEE Transactions on Information Forensics and Security (TIFS). 7(2): 691-703 (2012).
13. Hai Jin, Ge Cheng, Deqing Zou, and Xinwen Zhang. Cherub: Fine-grained Application Protection with On-demand Virtualization. Journal of Computers & Mathematics with Applications, Elsevier, March, 2012.
14. Xinwen Zhang, Anugeetha Kunjithapatham, Sangoh Jeong, and Simon Gibbs. Towards an Elastic Application Model for Augmenting the Computing Capabilities of Mobile Devices with Cloud Computing. ACM Springer Mobile Networks and Applications (MONET) Journal, Vol. 16, Num. 3, 270-284, 2011.
15. Min Xu, Duminda Wijesekera, and Xinwen Zhang. Runtime Administration of RBAC Profile for XACM. IEEE Transactions on Services Computing (TSC), 4(4): 286-299 (2011).
16. Jing Jin, Gail-J. Ahn, Hongxin Hu, Michael Covington, and Xinwen Zhang. Patient-centric Authorization Framework for Electronic Healthcare Services. Elsevier Journal of Computers & Security, 30(2-3): 116-127 (2011).
17. Masoom Alam, Xinwen Zhang, Mohammad Nauman, Tamleek Ali, and Patrick C.K. Hung. Behavioral Attestation for Business Processes. Journal of Web Services Research, 7(3): 52-72 (2010).
18. Ge Cheng, Hai Jin, Deqing Zou, and Xinwen Zhang. Building Dynamic and Transparent Integrity Measurement and Protection for Virtualized Platform in Cloud Computing. Journal of Concurrency and Computation: Practice and Experience, Wiley, 22(13): 1893-1910 (2010).
19. Qi Li, Xinwen Zhang, Mingwei Xu, and Jianping Wu. Towards Secure Dynamic Collaborations with Group-based RBAC Model. Elsevier Journal of Computers & Security (CompSec), Vol. 28, 2009: 260-275.

20. Xinwen Zhang, Masayuki Nakae, Michael J. Covington, and Ravi Sandhu. A Usage-based Authorization Framework for Collaborative Computing Systems. ACM Transactions on Information and System Security (TISSEC), 11(1), 2008.
21. Zhixiong Zhang, Xinwen Zhang, and Ravi Sandhu. Towards a Scalable Role and Organization Based Access Control Model with Decentralized Security Administration. Book chapter: Handbook of Research on Social and Organizational Liabilities in Information Security, published by IGI Global, ISBN: 978-1-60566-132-2. Nov. 2008.
22. Ravi Sandhu, Xinwen Zhang, Kumar Ranganathan, and Michael J. Covington, Client-side Security Enforcement Using Trusted Computing and PEI Models, Journal of High Speed Network, Special issue on Managing Security Polices: Modeling, Verification and Configuration, 15(3): 229-245, 2006.
23. Sejong Oh, Ravi Sandhu, and Xinwen Zhang. An Effective Role Administration Model Using Organization Structure. ACM Transactions on Information and System Security, (TISSEC), 9(2): 2006.
24. Xinwen Zhang, Songqing Chen, and Ravi Sandhu. Using Trusted Computing Technologies to Enhance Data Authenticity and Integrity in P2P Systems Using Trusted Computing. IEEE Internet Computing, Special Issue on Security for P2P/Ad Hoc Networks, 9(6), pp. 42-49, November/December, 2005.
25. Xinwen Zhang, Francesco Parisi-Presicce, Ravi Sandhu, and Jaehong Park, Formal Model and Policy Specification of Usage Control. ACM Transactions on Information and System Security (TISSEC), 8(4): 351-387, 2005.
26. Yingjiu Li and Xinwen Zhang. Securing Credit Card Transactions with One-Time Payment Scheme. Journal of Electronic Commerce Research and Applications (ECRA), Elsevier, 4, pp. 413-426, 2005.

Referred Conference, Symposium, and Workshop Papers

1. Ruowen Wang, William Enck, Douglas S. Reeves, Xinwen Zhang, Peng Ning, Dingbang Xu, Wu Zhou, Ahmed M. Azab: EASEAndroid: Automatic Policy Analysis and Refinement for Security Enhanced Android via Large-Scale Semi-Supervised Learning. USENIX Security 2015: 351-366.
2. Lei Xu, Xinwen Zhang, Xiaoxin Wu, Weidong Shi: ABSS: An Attribute-based Sanitizable Signature for Integrity of Outsourced Database with Public Cloud. CODASPY 2015: 167-169.
3. Su Zhang, Xinwen Zhang, Xinming Ou, Liqun Chen, Nigel Edwards, Jing Jin: Assessing Attack Surface with Component-Based Package Dependency. NSS 2015: 405-417
4. Su Zhang, Xinwen Zhang, and Xinming Ou. After We Knew It: Empirical Study and Modeling of Cost-effectiveness of Exploiting Prevalent Known Vulnerabilities Across IaaS. In Proc. of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2014.
5. Qingji Zheng, Wei Zhu, Jiafeng Zhu, and Xinwen Zhang. Improved Anonymous Proxy Re-encryption with CCA Security. In Proc. of 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2014.
6. Qi Li, Yih-Chun Hu, and Xinwen Zhang. Even Rockets Cannot Make Pigs Fly Sustainably: Can BGP be Secured with BGPsec? In NDSS Workshop on Security of Emerging Networking Technologies (SENT), 2014.
7. Ravishankar Ravindran, Xuan Liu, Asit Chakraborti, Xinwen Zhang, and Guoqing Wang. Towards Software Defined ICN based Edge-Cloud Services. In Proc. of IEEE CloudNet, 2013.
8. Ruoyu Wu, Xinwen Zhang, Gail-Joon Ahn, Hadi Sharifi, and Haiyong Xie. ACaaS: Access Control as a Service for IaaS Cloud. In Proc. of the 5th ASE/IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT), 2013.

9. Huijun Xiong, Qingji Zheng, Xinwen Zhang, and Danfeng Yao. CloudSafe: Securing Data Processing within Vulnerable Virtualization Environment in Cloud¡/a¿. In IEEE Conference on Communications and Network Security (IEEE-CNS), 2013.

10. Wu Zhou, Xinwen Zhang, and Xuxian Jiang. AppInk: Watermarking Android Apps for Repackaging Deterrence. In Proc. of the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2013.

11. Abedelaziz Mohaisen, Xinwen Zhang, Max Schuchard, Haiyong Xie, Yongdae Kim. Protecting Access Privacy of Cached Contents in Information Centric Networks. In Proc. of 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2013.

12. Ravishankar Ravindran, Trisha Biswas, Xinwen Zhang, Asit Chakraborti, and Guoqiang Wang. Information-centric Networking based Homenet. In Proc. of IFIP/IEEE International Workshop on Management of the Future Internet (ManFI), 2013 (co-located with IFIP/IEEE IM 2013).

13. Ravishankar Ravindran, Guoqiang Wang, Xinwen Zhang, and Asit Chakraborti. Supporting Dual-Mode Forwarding in Content-Centric Network. In Proc. of the 6th IEEE International Conference on Advanced Networks and Telecommunication Systems (ANTS), 2012.

14. Weidong Shi, Taeweon Suh, JongHyuk Lee, DongHyuk Woo, and Xinwen Zhang. Architectural Support of Multiple Hypervisors over Single Platform for Enhancing Cloud Computing Security. In Proc. of ACM International Conference on Computing Frontiers (CF'12), 2012.

15. Lei Xu, Xiaoxin Wu, and Xinwen Zhang. CL-PRE: a Certificateless Proxy Re-Encryption Scheme for Secure Data Sharing with Public Cloud. In Proc. of the 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2012.

16. Ravishankar Ravindran, Samantha Lo, Xinwen Zhang, and Guoqiang Wang. Supporting Seamless Mobility in Named-Data Networking. In Proc. of the Fifth International Workshop on the Network of the Future (co-located with ICC'12), 2012.

17. Yang Qin, Dijiang Huang, and Xinwen Zhang. VehiCloud: Cloud Computing Facilitating Routing In Vehicular Networks. In Proc. of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012.

18. Sokol Kosta, Andrius Aucinas, Pan Hui, Richard Mortier, and Xinwen Zhang. ThinkAir: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading. In IEEE INFOCOM 2012.

19. Huijun Xiong, Xinwen Zhang, Wei Zhu, and Danfeng Yao. End-to-End Content Protection in Cloud-based Storage and Delivery Services. In Second ACM Conference on Data and Application Security and Privacy (CODASPY), 2012.

20. Lei Liu, Xinwen Zhang, Guanhua Yan, and Songqing Chen. Chrome Extensions: Security Analysis and Countermeasures. In 19th Annual Network & Distributed System Security Symposium (NDSS), 2012.

21. Katharine Chang, Xinwen Zhang, Guoqiang Wang, and Kang G. Shin. TGIS: Booting Trust for Secure Information Sharing in Mobile Group Collaborations. In Proc. of Third IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT), 2011.

22. Lei Liu, Xinwen Zhang, and Songqing Chen. Botnet with Browser Extensions. In Proc. of Third IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT), 2011.

23. Xinwen Zhang, Katharine Chang, Huijun Xiong, Guangyu Shi, Guoqiang Wang, Kathleen Nichols, and Yonggang Wen. Towards Name-based Trust and Security for Content-centric Network. In Second International Workshop on Security & Trust in the Future Internet (FIST'11), co-located with ICNP 2011.

24. Huijun Xiong, Xinwen Zhang, Wei Zhu, and Danfeng Yao. CloudSeal: End-to-End Content Protection in Cloud-based Storage and Delivery Services. In the 7th International ICST Conference on Security and Privacy in Communication Network (SecureComm'11), 2011.

25. Yajin Zhou, Xinwen Zhang, Xuxian Jiang, and Vince Freeh. Taming Information-Stealing Smartphone Applications (on Android). In the 4th International Conference on Trust and Trustworthy Computing (TRUST), Pittsburgh, PA, June 2011.

26. Masoom Alam, Xinwen Zhang, Kamran Khan, and Gohar Ali. xDAuth: A Scalable and Lightweight Framework for Cross Domain Access Control and Delegation. In 16th ACM Symposium on Access Control Models and Technologies (SACMAT), 2011.

27. Qi Li, Mingwei Xu, Jianping Wu, Xinwen Zhang, Patrick P.C. Lee, and Ke Xu. Enhancing the Trust of Internet Routing with Lightweight Route Attestation. In Proc. of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2011.

28. Taeweon Suh, Jong Beom Lim, Dong Hyuk Woo, Weidong Shi, Xinwen Zhang, and Jong Hyuk Lee. PolyHype: Towards Poly-Hypervisor Platform for Cloud Computing. In Workshop on Micro Architectural Support for Virtualization, Data Center Computing, and Clouds, 2010. (in Conjunction with MICRO 2010).

29. Tamleek Ali, Mohammad Nauman, and Xinwen Zhang. On Leveraging Stochastic Models for Remote Attestation. In the Second International Conference on Trusted Systems (INTRUST), 2010.

30. Xinwen Zhang, Jean-Pierre Seifert, and Onur Aciicmez. SEIP: Simple and Efficient Integrity Protection for Open Mobile Platforms. In the 12th International Conference on Information and Communications Security (ICICS), 2010.

31. Guofu Xiang, Hai Jin, Deqing Zou, and Xinwen Zhang. VMDriver: A Driver-based Monitoring Mechanism for Virtualization. In the 29th IEEE Symposium on Reliable Distributed Systems (SRDS), 2010.

32. Wenjuan Xu, Gail-Joon Ahn, Hongxin Hu, Xinwen Zhang, and Jean-Pierre Seifert. DR@FT: Efficient Remote Attestation Framework for Dynamics Systems. In the 15th European Symposium on Research in Computer Security (ESORICS). 2010.

33. Xinwen Zhang, Won Jeon, Simon Gibbs, and Anugeetha Kunjithapatham. Elastic HTML5: Workload Offloading using Cloud-based Web Workers and Storages for Mobile Devices. In International Workshop on Mobile Computing and Clouds (MobiCloud, in conjunction with MobiCASE), 2010

34. Masoom Alam, Xinwen Zhang, Tamleek Ali, and Patrick C.K. Hung. MAuth: A Fine-grained and User-Centric Permission Delegation Framework for Multi-Mashup Web Services. In IEEE World Congress on Services (SERVICES), 2010.

35. Joshua Schiffman, Xinwen Zhang, and Simon Gibbs. DAuth: Fine-grained Authorization Delegation for Distributed Web Application Consumers. In IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), 2010.

36. Lei Liu, Xinwen Zhang, Guanhua Yan, and Songqing Chen. sePlugin: Towards Transparently Secure Plugins in Your Internet Explorers. In International Conference on Applied Cryptography and Network Security (ACNS), 2010.

37. Xinwen Zhang, Sangoh Jeong, Simon Gibbs, and Anugeetha Kunjithapatham. Towards an Elastic Application Model for Augmenting Computing Capabilities of Mobile Platforms. In the 3rd International ICST Conference on Mobile Wireless Middleware, Operating Systems, and Applications (MobileWare), 2010. (**Best Paper Award**)

38. Dijiang Huang, Xinwen Zhang, Myong Kang, and Jim Luo. MobiCloud: Building Secure Mobile Cloud Framework for Mobile Computing and Communication. In the 5th IEEE International Symposium on Service-Oriented System Engineering (SOSE), 2010.

39. Mohammad Nauman, Sohail Khan, Xinwen Zhang, and Jean-Pierre Seifert. Beyond Kernel-level Integrity Measurement: Enabling Remote Attestation for the Android Platform. In the 3rd International Conference on Trust and Trustworthy Computing (TRUST), 2010.

40. Liang Xie, Xinwen Zhang, Jean-Pierre Seifert, and Sencun Zhu. pBMDS: A Behavior-based Malware Detection System for Cellphone Devices. In ACM Conference on Wireless Network Security (WiSec), March 22-24, 2010, Hoboken, NJ, USA. (**Best paper Nominated**)

41. Mohammad Nauman, Sohail Khan, Masoom Alam, and Xinwen Zhang. Apex: Extending Android Permission Model and Enforcement with User-defined Runtime Constraints (short paper). In ACM Symposium on Information, Computer and Communications Security (ASIACCS), April 13-16, 2010, Beijing, China.

42. Simon Gibbs, Anugeetha Kunjithapatham, Sangoh Jeong, and Xinwen Zhang. Enabling Elastic Mobile Devices via Cloud Computing. In Samsung Technical Conference, 2009. (**Best Paper Award**)

43. Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapa, and Sangoh Jeong. Securing Elastic Applications on Mobile Devices for Cloud Computing. In the 1st ACM Cloud Computing Security Workshop (CCSW), Chicago, IL, USA, 13 November 2009.

44. Basel Katt, Xinwen Zhang, and Michael Hafner. Building Stateful Reference Monitor with Colored Petri Nets. In the 5th International Conference on Collaborative Computing (CollaborateCom'09), Crystal City, Washington D.C., USA, November 11-14, 2009.

45. Basel Katt, Xinwen Zhang, and Michael Hafner. A Usage Control Policy Specification with Petri Nets. In CollaborateCom Workshop on Trusted Collaboration (TrustCol), Crystal City, Washington DC, USA, 2009.

46. Lei Liu, Xinwen Zhang, Guanhua Yan, and Songqing Chen. Exploitation and Threat Analysis of Open Mobile Devices. In ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS'09), Princeton, New Jersey, USA, October 19-20, 2009.

47. Basel Katt, Xinwen Zhang, and Michael Hafner. A Usage Control Policy Specification with Petri Net Approach. In the 4th International Symposium on Information Security (IS'09), Vilamoura, Algarve-Portugal, Nov 02 - 03, 2009.

48. Ge Cheng, Hai Jin, Deqing Zou, Xinwen Zhang, Min Li, Chen Yu, and Guofu Xiang. Building Dynamic Integrity Protection for Multiple Independent Authorities in Virtualization-based Infrastructure. In the 10th IEEE/ACM International Conference on Grid Computing (GRID'09), Banff, Alberta, Canada, October 13 - 15, 2009.

49. Lei Liu, Guanhua Yan, Xinwen Zhang, and Songqing Chen. VirusMeter: Preventing Your Cellphone from Spies. In the 12th International Symposium on Recent Advances in Intrusion Detection (RAID'09), Saint-Malo, Brittany, France, September 23-25, 2009.

50. Liang Xie, Xinwen Zhang, Ashwin Chaugule, Trent Jaeger, and Sencun Zhu. Designing System-level Defenses against Cellphone Malware. In the 28th International Symposium on Reliable Distributed Systems (SRDS'09), Niagara Falls, New York, USA; September 27-30, 2009.

51. Min Xu, Duminda Wijesekera, Xinwen Zhang, and Deshan Cooray. Towards Session-aware RBAC Administration and Enforcement with XACML. In IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), Imperial College London, UK, 20-22 July 2009.

52. Masoom Alam, Mohammad Nauman, Xinwen Zhang, Tamleek Ali, and Patrick C.K. Hung. Behavioral Attestation for Business Processes (BA4BP). In the 7th IEEE International Conference on Web Services (ICWS), Los Angeles, CA, USA, July 6-10, 2009.

53. Xinwen Zhang, Onur Aciicmez, and Jean-Pierre Seifert. Building Efficient Integrity Measurement and Attestation for Mobile Phone Platforms. In the First International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec), 2009.

54. Wenjuan Xu, Xinwen Zhang, and Gail-Joon Ahn. Towards System Integrity Protection with Graph-Based Policy Analysis. In the 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec'09), Montreal, Canada, July 12-15, 2009.

55. Jing Jin, Hongxin Hu, Gail-Joon Ahn, Michael J. Covington, and Xinwen Zhang. Patient-centric Authorization Framework for Sharing Electronic Health Records. In the 14th ACM Symposium on Access Control Models and Technologies (SACMAT), Stresa, Italy, 2009.

56. Mohammad Nauman, Masoom Alam, Xinwen Zhang, and Tamleek Ali. Remote Attestation of Attribute Updates and Information Flows in a Usage Control System. In the 2nd International Conference on the Technical and Socio-economic Aspects of Trusted Computing (TRUST), 2009.

57. Onur Aciiccmez, Jean-Pierre Seifert, and Xinwen Zhang. A Secure DVB Set-top Box via Trusted Computing Technologies. In IEEE Consumer Communications and Networking Conference (CCNC), 2009.

58. Jing Jin, Gail-Joon Ahn, Michael J. Covington, and Xinwen Zhang. Toward an Access Control Model for Sharing Composite Electronic Health Records. In the 4th International Conference on Collaborative Computing (CollaborateCom), 2008.

59. Qi Li, Xinwen Zhang, and Jean-Pierre Seifert. Secure Mobile Payment via Trusted Computing. In the 3rd Asia-Pacific Trusted Infrastructure Technology Conference (APTC), IEEE, 2008.

60. Masoom Alam and Xinwen Zhang. Behavioral Attestation for Web Services. In ACM CCS Workshop on Secure Web Services (SWS), Fairfax, Virginia, USA, 2008.

61. Xinwen Zhang, Jean-Pierre Seifert, and Ravi Sandhu. Trusted Policy Enforcement for Distributed Usage Control. In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), Taichung, Taiwan, 2008

62. Masoom Alam, Xinwen Zhang, and Jean-Pierre Seifert. Model-based Behavioral Attestation. In the 13th ACM symposium on access control models and technologies (SACMAT), Estes Park, Colorado, USA, 2008.

63. Basel Katt, Xinwen Zhang, Ruth Breu, Michael Hafner, and Jean-Pierre Seifert. Beyond UCON Core Models with General Obligation Model and Continuity-Enhanced Policy Enforcement Engine. In the 13th ACM symposium on access control models and technologies (SACMAT), Estes Park, Colorado, USA, 2008.

64. Gail-J Ahn, Xinwen Zhang, and Wenjuan Xu. Systematic Policy Analysis for High-assurance Services in SELinux. In the 9th IEEE Workshop on Policies for Distributed Systems and Networks (POLICY), Palisades, NY, USA, 2008.

65. Qi Li, Mingwei Xu, and Xinwen Zhang. Towards a Group-based RBAC Model and Decentralized User-Role Administration. In the 2nd IEEE International Workshop on Cooperative Distributed Systems (CDS'08, in conjunction with ICDCS 2008), Beijing, China.

66. Qi Li and Xinwen Zhang. Access Control in Group Communication Systems. In IEEE Symposium on Computers and Communications (ISCC'08), July 6 - 9, 2008, Marrakech, Morocco.

67. Xinwen Zhang, Masoom Alam, Jean-Pierre Seifert, and Qi Li. Usage Control Platformization via Trustworthy SELinux. In ACM Symposium on Information, Computer, and Communication Security (ASIACCS), Tokyo, Japan, 2008.

68. Onur Aciiccmez, Afshin Latifi, Jean-Pierre Seifert, and Xinwen Zhang. A Trusted Mobile Phone Prototype. In IEEE Consumer Communications and Networking Conference (CCNC), 2008.

69. Xinwen Zhang, Dongyu Liu, Songqing Chen, and Ravi Sandhu. Towards Digital Rights Protection in BitTorrent-like Systems. In the 15th SPIE/ACM Multimedia Computing and Networking (MMCN), 2008.

70. Xinwen Zhang, Qi Li, Jean-Pierre Seifert, and Mingwei Xu. Flexible Authorization with Decentralized RBAC Model for Grid Computing. In the 10th IEEE High Assurance Systems Engineering Symposium (HASE), 2007.

71. Berthold Agreiter, Masoom Alam, Ruth Breu, Michael Hafner, Alex Pretschner, Jean-Pierre Seifert, and Xinwen Zhang. A Technical Architecture for Enforcing Usage Control Requirements in Service-Oriented Architectures. In ACM CCS Workshop on Secure Web Services (SWS), 2007.

72. Xinwen Zhang, Jean-Pierre Seifert, and Onur Aciicmez. Architecturing Trusted Mobile Platforms via Secure Kernel. In ACM CCS Workshop on Scalable Trusted Computing (STC), 2007.

73. Masoom Alam, Xinwen Zhang, and Jean-Pierre Seifert. Trusted SECTET: A Model-Driven Framework for Trusted Computing based Systems. In the 11th IEEE Enterprise Distributed Object Computing Conference (EDOC), 2007.

74. Berthold Agreiter, Masoom Alam, Michael Hafner, Jean-Pierre Seifert, and Xinwen Zhang. Model Driven Configuration of Secure Operating Systems for Mobile Applications in Healthcare. In ACM Workshop on Model-Based Trustworthy Health Information Systems, 2007. (in conjunction with ACM MODELS'07)

75. Min Xu, Xuxian Jiang, Ravi Sandhu, and Xinwen Zhang. Towards a VMM-based Usage Control Framework for OS Kernel Integrity Protection. In Proc. of the 12th ACM symposium on access control models and technologies (SACMAT), Sophia, France, June 20-22, 2007.

76. Baoxian Zhao, Ravi Sandhu, and Xinwen Zhang. Towards A Times-Based Usage Control Model. In the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec), Redondo Beach, CA, USA, July 8-11, 2007.

77. Xinwen Zhang, Jean-Pierre Seifert , and Masoom Alam. Extending SELinux Policy Model and Enforcement towards Trusted Computing Paradigm on Mobile Platform. In the third Annual Security Enhanced Linux Symposium, 2007.

78. Xinwen Zhang, Songqing Chen, Michael J. Covington, and Ravi Sandhu. SecureBus: Towards Transparent Application-level Trusted Computing with Mandatory Access Control. In the Proceedings of ACM Symposium on Information, Computer, and Communication Security (ASIACCS), Singapore, 2007.

79. Songqing Chen, Xinyuan Wang, Lei Liu, Xinwen Zhang, and Zhao Zhang. WormTerminator: An Effective Containment of Unknown and Polymorphic Fast Spreading Worms. In the Proceedings of ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), San Jose, California, USA, December 3-5, 2006.

80. Zhixiong Zhang, Xinwen Zhang, and Ravi Sandhu. ROBAC: Scalable Role and Organization Based Access Control Models. In the Proceedings of Workshop on Trusted Collaboration (TrustCol), Atlanta, Georgia, USA, November 17, 2006.

81. Qi Li, Xinwen Zhang, Sihan Qing, and Mingwei Xu. Supporting Ad-hoc Collaboration with Group-based RBAC Model. In the Proceedings of the 2nd International Conference on Collaborative Computing (CollaborateCom), Atlanta, Georgia, USA, November 17-20, 2006.

82. Xinwen Zhang, Francesco Parisi-Presicce, and Ravi Sandhu. Towards Remote Policy Enforcement for Runtime Protection of Mobile Code Using Trusted Computing. In International Workshop on Security (IWSEC), 2006.

83. Xinwen Zhang, Masayuki Nakae, Michael J. Covington, and Ravi Sandhu. A Usage-based Authorization Framework for Collaborative Computing Systems. In the Proceedings of ACM Symposium on Access Control Models and Technologies (SACMAT), 2006.

84. Xinwen Zhang, Ravi Sandhu, and Francesco Parisi-Presicce. Safety Analysis of Usage Control Authorization Models. In the Proceedings of ACM Symposium on Information, Computer, and Communication Security (ASIACCS), 2006.
85. Ravi Sandhu and Kumar Ranganathan, and Xinwen Zhang. Secure Information Sharing Enabled by Trusted Computing and PEI Models. In the Proceedings of ACM Symposium on Information, Computer, and Communication Security (ASIACCS), 2006.
86. Masayuki Nakae, Xinwen Zhang, and Ravi Sandhu. A General Design Towards Secure Ad-Hoc Collaboration. In the Proceedings of ACM Symposium on Information, Computer, and Communication Security (ASIACCS), 2006.
87. Ravi Sandhu and Xinwen Zhang. Peer-to-Peer Access Control Architecture Using Trusted Computing Technology. In the 10th ACM Symposium on Access Control Models and Technologies (SACMAT), 2005.
88. Xinwen Zhang, Yingjiu Li, and Divya Nalla. An Attribute-Based Access Matrix Model. In the 20th ACM Symposium on Applied Computing (SAC), Track on Computer Security, 2005.
89. Jaehong Park, Xinwen Zhang, and Ravi Sandhu. Attribute Mutabiligy in Usage Control. In Annual IFIP WG 11.3 Working Conference on Data and Applications Security, 2004.
90. Xinwen Zhang, Jaehong Park, Francesco Parisi-Presicce, and Ravi Sandhu. A Logical Specification for Usage Control. In the 9th ACM Symposium on Access Control Models and Technologies (SACMAT), 2004.
91. Yingjiu Li and Xinwen Zhang. A Security-Enhanced One-Time Payment Scheme for Credit Card. In the 14th International Workshop on Research Issues on Data Engineering (RIDE), 2004.
92. Xinwen Zhang, Jaehong Park, and Ravi Sandhu. Schema based XML Security: RBAC Approach. In the 17th IFIP 11.3 Working Conference on Data and Application Security, 2003.
93. Xinwen Zhang, Sejong Oh, and Ravi Sandhu. PBDM: A Flexible Delegation Model in RBAC. In the 8th ACM Symposium on Access Control Models and Technologies (SACMAT), 2003.

Poster & Demo

1. Trisha Biswas, Asit Chakraborti, Ravishankar Ravindran, Xinwen Zhang, and Guoqiang Wang. Contextualized Information-Centric Home Network. Demo In ACM SIGCOMM 2013.
2. Abedelaziz Mohaisen, Xinwen Zhang, Max Schuchard, Haiyong Xie, and Yongdae Kim. POSTER: Protecting Access Privacy of Cached Contents in Information Centric Networks. In In ACM Conference on Computer and Communication Security (CCS), 2012.
3. Xinwen Zhang et al. Name-based service publishing and discovery in content-centric network (Demo). Emerging Networks Consortium (ENC) at PARC, Spring Summit, 2012.
4. Xiaoxin Wu, Lei Xu, and Xinwen Zhang. A Certificateless Proxy Re-Encryption Scheme for Cloud-based Data Sharing (Poster). In ACM Conference on Computer and Communication Security (CCS), 2011.
5. Xinwen Zhang et al. Secure Mobile Virtual Group (Demo). CCNx Community Meeting (CCNxCon), 2011.
6. Xinwen Zhang et al. Name-based trust and security for information-centric network (Demo). CCNx Community Meeting (CCNxCon), 2011.
7. Wenjuan Xu, Gail-joon ahn, Hongxin Hu, Xinwen Zhang, and Jean-Pierre Seifert. Building Dynamic Remote Attestation Framework (Poster). In ACM Conference on Computer and Communications Security (CCS), 2009.

8. Simon Gibbs, Anugeetha Kunjithapatham, Sangoh Jeong, and Xinwen Zhang. Enabling Elastic Mobile Devices via Cloud Computing (Demo). In IEEE Consumer Communications and Networking Conference (CCNC), 2010.

Technical Report

1. Qingji Zheng and Xinwen Zhang. Multiparty Cloud Computation. arXiv:1206.371: 2012
2. Sokol Kosta, Andrius Aucinas, Pan Hui, Richard Mortier, and Xinwen Zhang. Unleashing the Power of Mobile Cloud Computing using ThinkAir. CoRR abs/1105.3232: 2011

IETF Draft

1. Xinwen Zhang, Ravishankar Ravindran, Haiyong Xie, and Guoqiang Wang. PID: A Generic Naming Schema for Information-centric Network.

Issued Patents

`https://patents.google.com/?inventor=xinwen+zhang&status=GRANT&language=ENGLISH&type=PATENT&num=100`

1. Onur Aciicmez, Jean-Pierre Seifert, Xinwen Zhang, and Afshin Latifi. Representation and verification of data for safe computing environments and systems. US Patent Number: 8788841.
2. Xinwen Zhang, Onur Aciicmez, Jean-Pierre Seifert, and Qingwei Ma. Securing stored content for trusted hosts and safe computing environments. US Patent Number: 8782801.
3. Xinwen Zhang, Onur Aciicmez, Simon J. Gibbs, Anugeetha Kunjithapatham, Sangoh Jeong, and Doreen Cheng. Execution allocation cost assessment for computing systems and environments including elastic computing systems and environments. US Patent Number: 8775630.
4. Xinwen Zhang, Huijun Xiong, and Guoqiang Wang. Method for flexible data protection with dynamically authorized data receivers in a content network or in cloud storage and content delivery services. US Patent Number: 8769705.
5. Zhengyi Le, Xinwen Zhang, John Waclawsky, and Jiwei Wei. Method and apparatus to authenticate a user to a mobile device using mnemonic based digital signatures. US Patent Number: 8769669.
6. Xinwen Zhang, Jean-Pierre Seifert, Wookhee Min, and Onur Aciicmez. Trusted multi-stakeholder environment. US Patent Number: 8752130.
7. Guo Qiang Wang, Ravishankar Ravindran, and Xinwen Zhang. Generalized dual-mode data forwarding plane for information-centric network. US Patent Number: 8694675.
8. Xinwen Zhang and Guangyu Shi. Method and apparatus to use identity information for digital signing and encrypting content integrity and authenticity in content oriented networks. US Patent number: 8645702.
9. Xinwen Zhang, Jean-Pierre Seifert, Onur Aciicmez, and Afshin Latifi. Active access monitoring for safer computing environments and systems. US Patent Number: 8631468.
10. Xinwen Zhang, Liang Xie, Jean-Pierre Seifert, Onur Aciicmez, and Afshin Latifi. Safety and management of computing environments that may support unsafe components. US Patent Number: 8621551.
11. Joshua Schiffman, Xinwen Zhang, Simon J. Gibbs, Anugeetha Kunjithapatham, and Sangoh Jeong. Securely using service providers in elastic computing systems and environments. US Patent number: 8601534.
12. Liang Xie, Xinwen Zhang, Jean-Pierre Seifert, Onur Aciicmez, and Afshin Latifi. Detecting unauthorized use of computing devices based on behavioral patterns. US Patent Number: 8595834.

13. Onur Aciicmez and Xinwen Zhang. Safe command execution and error recovery for storage devices. US Patent Number: 8578179.

14. Sangoh Jeong, Simon Gibbs, Xinwen Zhang, and Anugeetha Kunjithapatham. Execution allocation cost assessment for computing systems and environments including elastic computing systems and environments. US Patent Number: 8560465.

15. Xinwen Zhang, Jean-Pierre Seifert, Onur Aciicmez, and Afshin Latifi. Safe and efficient access control mechanisms for computing environments. US Patent Number: 8510805.

16. Xinwen Zhang, Onur Aciicmez, Simon J. Gibbs, Anugeetha Kunjithapatham, Sangoh Jeong, Doreen Cheng. Execution allocation cost assessment for computing systems and environments. US Patent Number: 8239538.

17. Xinwen Zhang, Jean-Pierre Seifert. Method and system for enforcing trusted computing policies in a hypervisor security module architecture. US Patent number: 8220029.

18. Onur Aciicmez, Xinwen Zhang, Jean-Pierre Seifert. Secure multicast content delivery. US Patent number: 8218772.

19. Xinwen Zhang, Jean-Pierre Seifert, Onur Aciicmez. Authentication, identity, and service management for computing and communication systems. US Patent number: 8201232.

20. Xinwen Zhang, Jean-Pierre Seifert, Onur Aciicmez, Qingwei Ma. Securing CPU affinity in multiprocessor architectures. US Patent number: 8136153.

21. Onur Aciicmez, Xinwen Zhang, Jean-Pierre Seifert. Security-enhanced storage devices using media location factor in encryption of hidden and non-hidden partitions. US Patent Number: 8112634.

22. Xinwen Zhang, Wenjuan Xu, Onur Aciicmez, Jean-Pierre Seifert. Secure inter-process communication for safer computing environments and systems. US Patent Number: 8108519.

23. Onur Aciicmez, Jean-Pierre Seifert, Qingwei Ma, Xinwen Zhang. Method and system for securing instruction caches using substantially random instruction mapping scheme. US US Patent number: 8055848.

24. Xinwen Zhang, Jean-Pierre Seifert, Masoom Alam. Method and system for extending SELinux policy models and their enforcement. US Patent number: 8051459.

25. Onur Aciicmez, Jean-Pierre Seifert, Qingwei Ma, Xinwen Zhang. Method and system for securing instruction caches using cache line locking. US Patent number: 8019946.

26. Onur Aciicmez, Jean-Pierre Seifert, Xinwen Zhang. Changing the order of public key cryptographic computations. US Patent number: 7974409.

27. Onur Aciicmez, Jean-Pierre Seifert, Xinwen Zhang. Altering the size of windows in public key cryptographic computations. US Patent number: 7936871.

28. Onur Aciicmez, Jean-Pierre Seifert, Qingwei Ma, Xinwen Zhang. Enhancing the security of public key cryptosystem implementations. US Patent number: 7903814.

29. Onur Aciicmez, Jean-Pierre Seifert, Xinwen Zhang, Afshin Latifi. Integrating hashing and decompression of compressed data for safe computing. US Patent Number: 7847710.