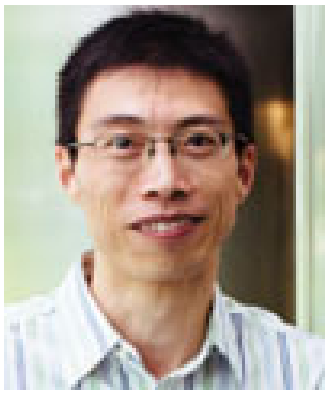
DING Xuhua

School of Computing and Information Systems
Singapore Management University (SMU)
80 Stamford Road
Singapore 178902

Email: xhding@smu.edu.sg
Office Phone: (+65) 68280683



Education

PhD, University of Southern California, United States of America, 2003

Master of Science, Shanghai Jiao Tong University, China, 1999

Bachelor of Science, Shanghai Jiao Tong University, China, 1995

Academic Appointments

Professor of Computer Science, School of Computing and Information Systems, SMU, Jul 2024 - Present

Associate Professor of Computer Science, School of Computing and Information Systems, SMU, Apr 2021 - Jun 2024

Associate Professor of Information Systems, School of Computing and Information Systems, SMU, Jan 2012 - Mar 2021

Assistant Professor of Information Systems, School of Computing and Information Systems, SMU, Jan 2004 - Dec 2011

Lecturer of Information Systems, School of Computing and Information Systems, SMU, Oct 2003 - Dec 2003

Academic Administrative Positions

Co-Director, Centre on Security, Mobile Applications and Cryptography (SMC), Centre on Security, Mobile Applications and Cryptography, SMU, Jan 2026 - Present

Director, Centre on Security, Mobile Applications and Cryptography (SMC), Centre on Security, Mobile Applications and Cryptography, SMU, Jan 2024 - Dec 2025

Coordinator, BSc (CS) Cybersecurity Track, School of Computing and Information Systems, SMU, Jul 2018 - Jun 2023

Member (School of Information Systems), Institutional Review Board, SMU Institutional Review Board, SMU, Jan 2013 - Dec 2016

RESEARCH

Research Interests

Network and system security
Applied cryptography
Trustworthy systems for data protection

Publications

Journal Articles [Refereed]

Enhancing the security of One-Tap Authentication services via dynamic application identification, by LIU, Di; LI, Dawei; GUO, Yuxiao; GUO, Ying; HU, Ruinan; LIU, Jianwei; BIAN, Song; DING, Xuhua; LIU, Yizhong; GUAN, Zhenyu. (2025). *IEEE Transactions on Information Forensics and Security, 20* 10231-10245. https://doi.org/10.1109/TIFS.2025.3607232 (Published)

Concretely mapped symbolic memory locations for memory error detection, by TU, Haoxin; JIANG, Lingxiao; HONG, Jiaqi; DING, Xuhua; JIANG, He. (2024). *IEEE Transactions on Software Engineering, 50* (7), 1747-1767. https://doi.org/10.1109/TSE.2024.3395412 (Published)

Hardware-assisted live kernel function updating on Intel platforms, by ZHOU, Lei; ZHANG, Fengwei; LEACH, Kevin; DING, Xuhua; NING, Zhenyu; WANG, Guojun; XIAO, Jidong. (2024). *IEEE Transactions on Dependable and Secure Computing, 21* (4), 2085-2098. https://doi.org/10.1109/TDSC.2023.3300101 (Published)

T-counter: Trustworthy and efficient CPU resource measurement using SGX in the cloud, by DONG, Chuntao; SHEN, Qingni; DING, Xuhua; YU, Daoqing; LUO, Wu; WU, Pengfei; WU, Zhonghai. (2023). *IEEE Transactions on Dependable and Secure Computing, 20* (1), 867-885. https://doi.org/10.1109/TDSC.2022.3145814 (Published)

A Coprocessor-Based Introspection Framework Via Intel Management Engine, by ZHOU, Lei; ZHANG, Fengwei; XIAO, Jidong; LEACH, Kevin; WEIMER, Westley; DING, Xuhua; WANG, Guojun. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (4), 1920-1932. (Published)

Initializing trust in smart devices via presence attestation, by DING, Xuhua; TSUDIK, Gene. (2018). *Computer Communications, 131* 35-38. https://doi.org/10.1016/j.comcom.2018.07.004 (Published)

FIMCE: A Fully Isolated Micro-Computing Environment for Multicore Systems, by ZHAO, Siqi; DING, Xuhua. (2018). *ACM Transactions on Information and System Security, 21* (3), 1-30. https://doi.org/10.1145/3195181 (Published)

Secure server-aided top-k monitoring, by WANG, Yujue; PANG, Hwee Hwa; YANG, Yanjiang; DING, Xuhua. (2017). *Information Sciences: Informatics and Computer Science Intelligent Systems Applications, 420* 345-363. https://doi.org/10.1016/j.ins.2017.08.068 (Published)

Adaptable key-policy attribute-based encryption with time interval, by MA, Siqi; LAI, Junzuo; DENG, Robert H.; DING, Xuhua. (2017). *Soft Computing, 21* (20), 6191-6200. https://doi.org/10.1007/s00500-016-2177-z (Published)

Privacy-Preserving Ad-Hoc Equi-Join on Outsourced Data, by PANG, Hwee Hwa; DING, Xuhua. (2014). *ACM Transactions on Database Systems, 39* (3), 1-40. https://doi.org/10.1145/2629501 (Published)

Technique for authenticating H.264/SVC and its performance evaluation over wireless mobile networks, by ZHAO, Yifan; LO, Swee Won; DENG, Robert H.; DING, Xuhua. (2014). *Journal of Computer and System Sciences, 80* (3), 520-532. https://doi.org/10.1016/j.jcss.2013.06.008 (Published)

A Hybrid Scheme for Authenticating Scalable Video Codestreams, by WEI, Zhuo; WU, Yongdong; DENG, Robert H.; DING, Xuhua. (2014). *IEEE Transactions on Information Forensics and Security, 9* (4), 543-553. https://doi.org/10.1109/TIFS.2014.2301916 (Published)

Efficient authentication and access control of scalable multimedia streams over packet-lossy networks, by DENG, Robert H.; DING, Xuhua; LO, Swee Won. (2014). *Security and Communication Networks, 7* (3), 611-625. https://doi.org/10.1002/sec.762 (Published)

Efficient block-based transparent encryption for H.264/SVC bitstreams, by DENG, Robert H.; DING, Xuhua; WU, Yongdong; WEI, Zhuo. (2014). *Multimedia Systems, 20* (2), 165-178.

http://dx.doi.org/10.1007/s00530-013-0326-0 (Published)

DriverGuard: Virtualization-Based Fine-Grained Protection on I/O Flows, by CHENG, Yueqiang; DING, Xuhua; DENG, Robert H.. (2013). *ACM Transactions on Information and System Security, 16* (2), 6-30. http://dx.doi.org/10.1145/2505123 (Published)

A scalable and format-compliant encryption scheme for H.264/SVC bitstreams, by Wei, Zhuo; Wu, Yongdong; DING, Xuhua; DENG, Robert H.. (2012). *Signal Processing: Image Communication, 27* (9), 1011-1024. http://dx.doi.org/10.1016/j.image.2012.06.005 (Published)

Scalable content authentication in H.264/SVC videos using perceptual hashing based on Dempster-Shafer theory, by YE, Dengpan; ZHUO, Wei; DING, Xuhua; DENG, Robert H.. (2012). *International Journal of Computational Intelligence Systems, 5* (5), 953-963. (Published)

Database Access Pattern Protection Without Full-Shuffles, by DING, Xuhua; YANG, Yanjiang; DENG, Robert H.. (2011). *IEEE Transactions on Information Forensics and Security, 6* (1), 189-201. https://doi.org/10.1109/TIFS.2010.2101062 (Published)

A new hardware-assisted PIR with O(n) shuffle cost, by DING, Xuhua; YANG, Yanjiang; DENG, Robert H.; WANG, Shuhong. (2010). *International Journal of Information Security, 9* (4), 237-252. https://doi.org/10.1007/s10207-010-0105-2 (Published)

Efficient processing of exact top-k queries over disk-resident sorted lists, by PANG, Hwee Hwa; DING, Xuhua; ZHENG, Baihua. (2010). *VLDB Journal, 19* (3), 437-456. https://doi.org/10.1007/s00778-009-0174-x (Published)

Tuning On-Air Signatures for Balancing Performance and Confidentiality, by ZHENG, Baihua; LEE, Wang-Chien; LIU, Peng; LEE, Dik Lun; DING, Xuhua. (2009). *IEEE Transactions on Knowledge and Data Engineering, 21* (12), 1783-1797. http://dx.doi.org/10.1109/TKDE.2009.43 (Published)

Leak-free mediated group signatures, by DING, Xuhua; Tsudik, Gene; Xu, Shouhuai. (2009). *Journal of Computer Security, 17* (4), 489-514. http://dx.doi.org/10.3233/JCS-2009-0342 (Published)

Multiuser private queries over encrypted databases, by YANG, Yanjiang; Bao, Feng; DING, Xuhua; DENG, Robert H.. (2009). *International Journal of Applied Cryptography, 1* (4), 309-319. http://dx.doi.org/10.1504/IJACT.2009.028029 (Published)

Equipping smart devices with public key signatures, by DING, Xuhua; Mozzacchi, D.; Tsudik, Gene. (2007). *ACM Transactions on Internet Technology, 7* (1), http://doi.org/10.1145/1189740.1189743 (Published)

Fine-grained control of security capabilities, by BONEH, D.; DING, Xuhua; TSUDIK, Gene. (2004). *ACM Transactions on Internet Technology, 4* (1), 60-82. http://doi.org/10.1145/967030.967033 (Published)

Journal Articles [Non-Refereed]

Genomic Security (Lest We Forget), by BRADLEY, Tatiana; DING, Xuhua; TSUDIK, Gene. (2017). *IEEE Security and Privacy, 15* (5), 38-46. https://doi.org/10.1109/MSP.2017.3681055 (Published)

Book Chapters

Remote platform attestation: The testimony for trust management, by DING, Xuhua; Gu, LIANG; DENG, Robert H.; Xie, Bing; MEI, Hong. (2010). *Trust modelling and management in digital environments: From social concept to system development* (pp. 1-19) Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-61520-682-7.ch001 (Published)

Conference Proceedings

A system framework to symbolically explore Intel TDX module execution, by PITIGALAARACHCHILLAGE, Pansilu; DING, Xuhua. (2025.0). *CCS '25: Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security, Taipei, Taiwan October 13-17,* (pp. 3885-3899) New York : ACM. https://doi.org/10.1145/3719027.3765212 (Published)

PRISM: To fortify widget based userapp data exchanges using Android virtualization framework, by NG, YingTat; CHEN, Zhe; QIU, Haiqing; DING, Xuhua. (2025.0). *ASIA CCS '25: Proceedings of the 20th ACM Asia*

Conference on Computer and Communications Security, Hanoi, Vietnam, August 25-29, (pp. 1567-1581) New York : ACM. https://doi.org/10.1145/3708821.3736205 (Published)

Oblivious digital tokens, by LISKIJ, Mihael; DING, Xuhua; TSUDIK, Gene; BASIN, David A.. (2025.0). *SEC '25: Proceedings of the 34th USENIX Conference on Security Symposium, Seattle, USA, August 13-15,* (pp. 7897-7915) New York : ACM. https://doi.org/10.5555/3766078.3766483 (Published)

TETD: Trusted execution in trust domains, by WANG, Zhanbo; ZHAN, Jiaxin; DING, Xuhua; ZHANG, Fengwei; HU, Ning. (2025.0). *SEC '25: Proceedings of the 34th USENIX Conference on Security Symposium, Seattle, USA, August 13-15,* (pp. 1187-1206) New York : ACM. https://doi.org/10.5555/3766078.3766140 (Published)

SCRUTINIZER: Towards secure forensics on compromised TrustZone, by ZHANG, Yiming; ZHANG, Fengwei; LUO, Xiapu; HOU, Rui; DING, Xuhua; LIANG, Zhenkai; YAN, Shoumeng; WE, Tao; HE, Zhengyu. (2025.0). *Proceedings of the 32nd Annual Network and Distributed System Security Symposium (NDSS2025), San Diego, California, 2025 February 24-28,* (pp. 1-16) US: https://doi.org/10.14722/ndss.2025.230147 (Published)

ESem: To harden process synchronization for servers, by WANG, Zhanbo; ZHAN, Jiaxin; DING, Xuhua; ZHANG, Fengwei; HU, Ning. (2024.0). *ASIA CCS '24: Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, Singapore, July 1-5,* (pp. 1554-1567) New York: ACM. https://doi.org/10.1145/3634737.3657025 (Published)

KRover: A symbolic execution engine for dynamic kernel analysis, by PITIGALAARACHCHILLAGE, Pansilu; DING, Xuhua; QIU, Haiqing; TU, Haoxin; HONG, Jiaqi; JIANG, Lingxiao. (2023.0). *CCS '23: Proceedings of the 30th ACM SIGSAC Conference on Computer and Communications Security, Copenhagen, November 26-30,* (pp. 2009-2023) New York: ACM. https://doi.org/10.1145/3576915.3623198 (Published)

DScope: To reliably and securely acquire live data from Kernel-Compromised ARM devices, by CHEN, Zhe; QIU, Haiqing; DING, Xuhua. (2023.0). *Proceedings of the 28th European Symposium on Research in Computer Security, Netherlands, 2023 September 25-29,* Cham: Springer. (Published)

How to resuscitate a sick VM in the cloud, by DING, Xuhua . (2023.0). *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks: Supplemental Volume (DSN-S): Porto, June 27-30: Proceedings,* (pp. 89-93) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/DSN-S58398.2023.00030 (Published)

FastKLEE: faster symbolic execution via reducing redundant bound checking of type-safe pointers, by TU, Haoxin; JIANG, Lingxiao; DING, Xuhua; JIANG, He. (2022.0). *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Singapore, 2022 November 14 - 18,* Singapore: Association for Computing Machinery. https://doi.org/10.1145/3540250.3558919 (Published)

SMILE: Secure memory introspection for live enclave, by ZHOU, Lei; DING, Xuhua; ZHANG Fengwei. (2022.0). *Proceedings of IEEE Symposium on Security and Privacy* , USA: IEEE. http://doi.org/10.1109/SP46214.2022.9833714 (Published)

ScriptChecker: To tame third-party script execution with task capabilities, by LUO, Wu; DING, Xuhua; WU, Pengfei; ZHANG, Xiaolei; SHEN, Qingni; WU, Zhonghai. (2022.0). *Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, California, 2022 February 27- March 3,* (pp. 1-17) San Diego, California: Internet Society . (Accepted)

Catch you with cache: Out-of-VM introspection to trace malicious executions, by SU, Chao; DING, Xuhua; ZENG, Qinghai. (2021.0). *Proceedings of the 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Taipei, Taiwan, 2021 June 21-24,* (pp. 326-337) Taipei, Taiwan: IEEE. (Published)

A novel dynamic analysis infrastructure to instrument untrusted execution flow across user-kernel spaces, by HONG, Jiaqi; DING, Xuhua. (2020.0). *Proceedings of 42nd IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2021 May 23-27,* (pp. 402-418) US: IEEE. (Published)

On the root of trust identification problem, by NUNES, Ivan De Oliveira; DING, Xuhua; TSUDIK, Gene. (2021.0). *Proceedings of the 20th ACM/IEEE on Information Processing in Sensor Networks, Nashville, USA, 2021 May 18-21,* (pp. 315-327) Nashville, USA: ACM. (Published)

To detect stack buffer overflow with polymorphic canaries, by WANG, Zhilong; DING, Xuhua; PANG,

Chengbin; GUO, Jian; ZHU, Jun; MAO, Bing. (2018.0). *48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks DSN 2018: Luxembourg City, 25-28 June: Proceedings,* (pp. 243-254) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/DSN.2018.00035 (Published)

Presence attestation: The missing link in dynamic trust bootstrapping, by ZHANG, Zhangkai; DING, Xuhua; TSUDIK, Gene; CUI, Jinhua; LI, Zhoujun. (2017.0). *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, October 30-November 3,* (pp. 89-102) New York: ACM. https://doi.org/10.1145/3133956.3134094 (Published)

Seeing through the same lens: Introspecting guest address space at native speed, by ZHAO, Siqi; DING, Xuhua; XU, Wen; GU, Dawu. (2017.0). *Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, 2017 August 16-18,* (pp. 799-813) Berkeley, CA: USENIX Association. (Published)

On the effectiveness of virtualization based memory isolation on multicore platforms, by ZHAO, Siqi; DING, Xuhua. (2017.0). *2nd IEEE European Symposium on Security and Privacy EuroS&P 2017: Proceedings: Paris, 26-28 April,* (pp. 546-560) Piscataway, NJ: IEEE. https://doi.org/10.1109/EuroSP.2017.25 (Published)

H-Binder: A hardened binder framework on Android systems, by SHEN, Dong; ZHANG, Zhangkai; DING, Xuhua; LI, Zhoujun; DENG, Robert H.. (2017.0). *Security and privacy in communication networks: 12th International Conference, SecureComm 2016, Guangzhou, China, October 10-12, Proceedings,* (pp. 24-43) Cham: Springer. https://doi.org/10.1007/978-3-319-59608-2_2 (Published)

Attribute-based encryption with granular revocation, by CUI, Hui; DENG, Robert H.; DING, Xuhua; LI, Yingjiu. (2016.0). *Security and Privacy in Communication Networks: 12th International Conference, SecureComm 2016, Guangzhou, China, October 10-12: Proceedings,* (pp. 165-181) Cham: Springer. https://doi.org/10.1007/978-3-319-59608-2_9 (Published)

SuperCall: A Secure Interface For Isolated Execution Environment to Dynamically Use External Services, by CHENG, Yueqiang; LI, Qing; YU, Miao; DING Xuhua; SHEN, Qingni. (2016.0). *Proceedings of the 11th EAI International Conference on Security and Privacy in Communication Networks.,* (pp. 193-211) Dallas, United States: Springer International Publishing. http://link.springer.com/chapter/10.1007%2F978-3-319-28865-9_11 (Published)

Hardware-Assisted Fine-Grained Code-Reuse Attack Detection, by YUAN, Pinghai; ZENG, Qingkai; DING, Xuhua. (2015.0). *Research in Attacks, Intrusions, and Defenses: 18th International Symposium, RAID 2015, Kyoto, Japan, November 2-4, 2015: Proceedings,* (pp. 66-85) Cham: Springer Verlag. http://dx.doi.org/10.1007/978-3-319-26362-5_4 (Published)

On security of content-based video stream authentication, by LO, Swee-Won; WEI, Zhou; DENG, Robert H.; DING, Xuhua. (2015.0). *Computer Security – ESORICS 2015: 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, Proceedings,* (pp. 366-383) Cham: Springer. http://dx.doi.org/10.1007/978-3-319-24174-6_19 (Published)

Efficient Virtualization-based Application Protection against Untrusted Operating System, by CHENG, Yueqiang; DING, Xuhua; DENG, Robert H.. (2015.0). *AsiaCCS'15: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security: April 14-17, 2015, Singapore,* (pp. 345-356) New York: ACM. http://dx.doi.org/10.1145/2714576.2714618 (Published)

ROPecker: A generic and practical approach for defending against ROP attack, by CHENG, Yueqiang; ZHOU, Zongwei; MIAO, Yu; DING, Xuhua; DENG, Robert H.. (2014.0). *NDSS Symposium 2014: Proceedings of the 21st Network and Distributed System Security Symposium, San Diego, February 23-26,* (pp. 1-14) Reston, VA: Internet Society. https://doi.org/10.14722/ndss.2014.23156 (Published)

Achieving revocable fine-grained cryptographic access control over cloud data, by YANG, Yanjiang; DING, Xuhua; LU, Haibing; Wan, Zhiguo; Zhou, Jianying. (2013.0). *Information Security: 16th International Conference, ISC 2013, Dallas, Texas, November 13-15: Proceedings,* (pp. 293-308) Cham: Springer. https://doi.org/10.1007/978-3-319-27659-5_21 (Published)

Self-blindable credential: Towards anonymous entity authentication upon resource-constrained devices, by YANG, Yanjiang; DING, Xuhua; LU, Haibing; WENG, Jian; ZHOU, Jianying. (2013.0). *Information Security: 16th International Conference, ISC 2013, Dallas, Texas, November 13-15: Proceedings,* (pp. 238-247) Cham: Springer. https://doi.org/10.1007/978-3-319-27659-5_17 (Published)

Technique for authenticating H.264/SVC streams in surveillance applications, by ZHUO, Wei; DENG, Robert H.; SHEN, Jialie; WU, Yongdong; DING, Xuhua; LO, Swee Won. (2013.0). *Electronic Proceedings of the 2013*

IEEE International Conference on Multimedia and Expo Workshops (ICMEW 2013): 15-19 July, 2013, San Jose, California, (pp. 1-14) Los Alamitos, CA: IEEE Computer Society. http://doi.ieeecomputersociety.org/10.1109/ICMEW.2013.6618259 (Published)

Accountable Trapdoor Sanitizable Signatures, by LAI, Junzuo; DING, Xuhua; Wu, Yongdong. (2013.0). *Information Security Practice and Experience: 9th International Conference, ISPEC 2013, Lanzhou, China, May 12-14, 2013: Proceedings,* (pp. 117-131) Berlin Heidelberg: Springer Verlag. http://dx.doi.org/10.1007/978-3-642-38033-4_9 (Published)

Verifiable and private top-k monitoring, by DING, Xuhua; PANG, Hwee Hwa. (2013.0). *ASIA CCS '13: Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, Hangzhou, China, May 8-10,* (pp. 553-558) New York: ACM. https://doi.org/10.1145/2484313.2484388 (Published)

Simple identity-based encryption with mediated RSA, by DING, Xuhua; TSUDIK, Gene. (2013.0). *Proceedings of The Cryptographers' Track at the RSA Conference 2013, San Francisco, CA, February 25 - March 1,* (pp. 193-210) Berline: Springer. https://doi.org/10.1007/3-540-36563-X_13 (Published)

Guardian: Hypervisor as Security Foothold for Personal Computers, by CHENG, Yueqiang; DING, Xuhua. (2013.0). *Trust and Trustworthy Computing: 6th International Conference, TRUST 2013, London, UK, June 17-19, 2013. Proceedings,* (pp. 19-36) Berlin Heidelberg: Springer Verlag. http://dx.doi.org/10.1007/978-3-642-38908-5_2 (Published)

An improved authentication scheme for H.264/SVC and its performance evaluation over non-stationary wireless mobile networks, by ZHAO, Yifan; LO, Swee-Won; DENG, Robert H.; DING, Xuhua. (2012.0). *Network and System Security: 6th International Conference, NSS 2012, Wuyishan, Fujian, China, November 21-23, Proceedings,* (pp. 192-206) Cham: Springer. https://doi.org/10.1007/978-3-642-34601-9_15 (Published)

A Generic Approach for Providing Revocation Support in Secret Handshake, by YANG, Yanjiang; LU, Haibing; WENG, Jian; DING, Xuhua; ZHOU, Jianying. (2012.0). *Proceedings of the 14th International Conference on Information and Communications Security ICICS'12,* (pp. 276-284) Berlin: Springer Verlag. http://dx.doi.org/10.1007/978-3-642-34129-8_24 (Published)

No tradeoff between confidentiality and performance: An analysis on H.264/SVC partial encryption, by WEI, Zhuo; DING, Xuhua; DENG, Robert H.; WU, Yongdong. (2012.0). *Communications and multimedia security: 13th IFIP TC 6/TC 11 International Conference, CMS 2012, Canterbury, September 3-5: Proceedings,* (pp. 72-86) Cham: Springer. https://doi.org/10.1007/978-3-642-32805-3_6 (Published)

Coercion Resistance in Authentication Responsibility Shifting, by GUPTA, Payas; DING, Xuhua; GAO, Debin. (2012.0). *ASIACCS '12: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security,* (pp. 97-98) New York, NY: ACM. http://dx.doi.org/10.1145/2414456.2414512 (Published)

Virtualization based password protection against malware in untrusted operating systems, by CHENG, Yueqiang; DING, Xuhua. (2012.0). *Trust and Trustworthy Computing: 5th International Conference, TRUST 2012, Vienna, Austria, June 13-15: Proceedings,* (pp. 201-218) Berlin: Springer. https://doi.org/10.1007/978-3-642-30921-2_12 (Published)

A Generic Construction of Accountable Decryption and Its Applications, by Zhou, Xuhua; DING, Xuhua; CHEN, Kefei. (2012.0). *Proceedings of the 17th Australasian Conference on Information Security and Privacy (ACISP 2012),* (pp. 322-335) Berlin: Springer Verlag. http://dx.doi.org/10.1007/978-3-642-31448-3_24 (Published)

DriverGuard: A fine-grained protection on I/O flow, by CHENG, Yueqiang; DING, Xuhua; DENG, Robert H.. (2011.0). *Computer Security – ESORICS 2011: 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12-14,* (pp. 227-244) Berlin: Springer. https://doi.org/10.1007/978-3-642-23822-2_13 (Published)

Hierarchical identity-based chameleon hash and its applications, by BAO, Feng; DENG, Robert H.; DING, Xuhua; LAI, Junzuo; ZHAO, Yunlei. (2011.0). *Applied Cryptography and Network Security: 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10: Proceedings,* (pp. 201-219) Berlin: Springer. https://doi.org/10.1007/978-3-642-21554-4_12 (Published)

Lightweight Delegated Subset Test with Privacy Protection, by Zhou, Xuhua; DING, Xuhua; CHEN, Kefei. (2011.0). *Information Security Practice and Experience: 7th International Conference, ISPEC 2011,*

Guangzhou, China, May 30 - June 1: Proceedings, (pp. 138-151) Guangzhou, China: Springer Verlag. http://doi.org/10.1007/978-3-642-21031-0_11 (Published)

Embellishing text search queries to protect user privacy, by PANG, Hwee Hwa; DING, Xuhua; XIAO, Xiaokui. (2010.0). *Proceedings of the VLDB Endowment: 36th International Conference on Very Large Data Bases: Singapore, 13-17 September 2010,* (pp. 598-607) New York: ACM. https://doi.org/10.14778/1920841.1920918 (Published)

A hybrid method to detect deflation fraud in cost-per-action online advertising, by DING, Xuhua. (2010.0). *Applied cryptography and network security: 8th International Conference, ACNS 2010, Beijing, China, June 22-25: Proceedings,* (pp. 545-562) Berlin: Springer. https://doi.org/10.1007/978-3-642-13708-2_32 (Published)

On Trustworthiness of CPU Usage Metering and Accounting, by LIU, Mei; DING, Xuhua. (2010.0). *IEEE 30th International Conference on Distributed Computing Systems Workshops: Proceedings: ICDCSW 2010: 21-25 June 2010, Genova, Italy,* (pp. 82-91) Genova, Italy: IEEE. http://dx.doi.org/10.1109/ICDCSW.2010.40 (Published)

Remote attestation on function execution, by GU, Liang; CHENG, Yueqiang; DING, Xuhua; DENG, Robert H.; GUO; Yao; SHAO, Weizhong. (2010.0). *Trusted Systems: First International Conference, INTRUST 2009, Beijing, China, December 17-19: Revised Selected Papers,* (pp. 60-72) Berlin: Springer. https://doi.org/10.1007/978-3-642-14597-1_4 (Published)

Conditional proxy re-encryption secure against chosen-ciphertext attacks, by WENG, Jian; DENG, Robert H.; DING, Xuhua; CHU, Cheng-Kang; LAI, Junzuo. (2009.0). *ASIACCS '09: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, March 10-12,* (pp. 322-332) New York: ACM. https://doi.org/10.1145/1533057.1533100 (Published)

Privacy-Preserving Querying in Sensor Networks, by Cristofaro, Emiliano; DING, Xuhua; Tsudik, Gene. (2009.0). *ICCCN 2009: Proceedings of 18th International Conference on Computer Communications and Networks, 2-6 August 2009, San Francisco,* (pp. 1-6) San Francisco, CA: IEEE. http://dx.doi.org/10.1109/ICCCN.2009.5235352 (Published)

Model-driven remote attestation: Attesting remote system from behavioral aspect, by GU, Liang; DING, Xuhua; DENG, Robert H.; ZOU Yanzhen; XIE, Bing; SHAO, Weizhong; MEI, Hong. (2008.0). *2008 ICYCS 9th International Conference for Young Computer Scientists: November 18-21, Zhang Jia Jie, Hunan, China: Proceedings,* (pp. 2347-2353) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/ICYCS.2008.349 (Published)

Remote attestation on program execution, by GU, Liang; DING, Xuhua; DENG, Robert H.; XIE, Bing; MEI, Hong. (2008.0). *Proceedings of the 3rd ACM Workshop on Scalable Trusted Computing, Alexandria, Virginia, October 31,* (pp. 11-20) New York: ACM. https://doi.org/10.1145/1456455.1456458 (Published)

An efficient PIR construction using trusted hardware, by YANG, Yanjiang; DING, Xuhua; DENG, Robert H.; BAO, Feng. (2008.0). *Information Security: 11th International Conference, ISC 2008, Taipei, Taiwan, September 15-18: Proceedings,* (pp. 64-79) Berlin: Springer. https://doi.org/10.1007/978-3-540-85886-7_5 (Published)

A dynamic trust management scheme to mitigate malware proliferation in P2P networks, by DING, Xuhua; YU, Wei; PAN, Ying. (2008.0). *IEEE International Conference on Communications, ICC '08, 19-23 May, Beijing,* (pp. 1605-1609) Piscataway, NJ: IEEE. http://doi.org/10.1109/ICC.2008.310 (Published)

Private query on encrypted data in multi-user setting, by BAO, Feng; DENG, Robert H.; DING, Xuhua; YANG, Yanjiang. (2008.0). *Information Security Practice and Experience: 4th International Conference, ISPEC 2008, Sydney, Australia, April 21-23: Proceedings,* (pp. 71-85) Berlin: Springer. https://doi.org/10.1007/978-3-540-79104-1_6 (Published)

Anomaly based Webphishing page detection, by Pan, Y.; DING, Xuhua. (2006.0). *ACSAC '06: 22nd Annual Computer Security Applications Conference, 11-15 December 2006, Miami Beach: Proceedings,* (pp. 381-392) Miami, FL: IEEE. http://dx.doi.org/10.1109/ACSAC.2006.13 (Published)

Protecting RFID Communications in Supply Chains, by LI, Yingjiu; DING, Xuhua. (2006.0). *Proceedings of the ACM Symposium on Information, Computer, and Communications Security: ASIACCS'07, Singapore, March 20-22, 2007,* (pp. 234-241) Singapore: ACM. http://dx.doi.org/10.1145/1229285.1229318 (Published)

Private Information Retrieval using trusted hardware, by WANG, Shuhong; DING, Xuhua; DENG, Robert H.; BAO, Feng. (2006.0). *Computer Security - ESORICS 2006: 11th European Symposium on Research in Computer Security, Hamburg, Germany, September 18-20: Proceedings,* (pp. 49-64) Berlin: Springer. https://doi.org/10.1007/11863908_4 (Published)

Secure Real-Time User Preference Collection for Broadcast Scheduling, by DING, Xuhua; WANG, Shuhong; ZHENG, Baihua. (2006.0). *2nd International Conference on Security and Privacy in Communication Networks (SecureComm'06),* (pp. 1-10) Baltimore, MD: IEEE. http://dx.doi.org/10.1109/SECCOMW.2006.359540 (Published)

Multiplex Encryption a Practical Approach to Encrypting Multi-Recipient Emails, by DING, Xuhua; Wei, Wei; CHEN, Kefei. (2005.0). *Information and Communications Security: 7th International Conference, ICICS 2005, Beijing, China, December 10-13: Proceedings,* (pp. 269-279) Beijing, China: Springer Verlag. http://dx.doi.org/10.1007/11602897_23 (Published)

Leak-Free Group Signatures with Immediate Revocation, by DING, Xuhua; Tsudik, Gene; Xu, Shouhuai. (2004.0). *Proceedings of the 24th International Conference on Distributed Computing Systems, 24-26 March, 2004, Hachioji, Tokyo,* (pp. 608-615) Hachioji, Tokyo, Japan: IEEE. http://dx.doi.org/10.1109/ICDCS.2004.1281628 (Published)

Experimenting with server-aided signatures, by DING, Xuhua; Mozzacchi, D.; Tsudik, Gene. (2002.0). *Proceedings on Network and Distributed System Security Symposium, San Diego, California, 2002 February 6-8,* San Diego, CA: Internet Society. (Published)

A method for fast revocation of public key certificates and security capabilities, by BONEH, Dan; DING, Xuhua; Tsudik, Gene; WONG, Chi Ming. (2001.0). *Proceedings of the 10th conference on USENIX Security Symposium, Washington, D.C., 2001 August 13-17,* Washington DC: ACM. (Published)

Research Grants

Singapore Management University

Development of Secured Components & Systems in Emerging Technologies through Hardware & Software Evaluation, National Cybersecurity R&D (NCR) Programme, Cyber Security Agency of Singapore (CSA) , PI (Project Level): DING Xuhua, Debin GAO, Robert H DENG, David LO , Co-PI (Project Level): Guansong PANG, JIANG Lingxiao, DUAN Yue, YANG Guomin, PANG Hwee Hwa, 2023, S$11,365,070

National Satellite of Excellence in Mobile Systems Security and Cloud Security, National Cybersecurity R&D (NCR) Programme, National Research Foundation (NRF) , PI (Project Level): Robert H DENG , Co-PI (Project Level): Debin GAO, PANG Hwee Hwa, DING Xuhua, LI Yingjiu, 2019, S$7,498,320

A Novel Hybrid Kernel Symbolic Execution Framework For Malware Analysis, NSoE TSS Grant Call, National Satellite of Excellence - Trustworthy Software Systems , PI (Project Level): DING Xuhua , Co-PI (Project Level): JIANG Lingxiao, 2019, S$715,000

A system framework for reliable and dependable incident response on mobile devices, NSoE MSS-CS Research Programme, National Satellite of Excellence - Mobile Systems Security and Cloud Security , PI (Project Level): DING Xuhua , Co-PI (Project Level): Debin GAO, 2019, S$1,201,607

AutoPrivacyModel: Automated Feature Modelling for Identifying Illegitimate Uses of Privacy-Sensitive Data in Mobile Applications, NSoE MSS-CS Research Programme, National Satellite of Excellence - Mobile Systems Security and Cloud Security , PI (Project Level): JIANG Lingxiao , Co-PI (Project Level): David LO, SHAR Lwin Khin, DING Xuhua, Debin GAO, 2019, S$700,403

Advanced defense techniques for mobile systems and future networks, Huawei Technologies co. Ltd , PI (Project Level): Robert H DENG , Co-PI (Project Level): Debin GAO, DING Xuhua, LI Yingjiu, 2015

Secure Mobile Centre - Technologies and Solutions for Securing Mobile Computing, National Cybersecurity R&D (NCR) Programme, National Research Foundation (NRF) , PI (Programme Level): Robert H DENG , PI (Project Level): DING Xuhua, Debin GAO, JIANG Lingxiao, LI Yingjiu, David LO, PANG Hwee Hwa, 2014, S$6,415,200

Mobile Platform Security Based on Virtualization, Huawei Technologies co. Ltd , PI (Project Level): DING Xuhua, 2013, S$143,780

The Protection of I/O Flows Between Peripheral Devices and Applications, Ministry of Defence (MINDEF) , PI (Project Level): DING Xuhua, 2011, S$145,782

Techniques and Systems for Securing Scalable Multimedia Content Dissemination, Public Sector Research Funding (PSF), Agency for Science, Technology and Research (A*STAR) , PI (Project Level): Robert H DENG , Co-PI (Project Level): DING Xuhua, 2010, S$605,376

A Study on System Call Security and Extensible Secure Execution Environment, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): DING Xuhua, 2014, S$20,289.67

Trapdoor Circuit and Its Application on Multiuser Computation, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): DING Xuhua, 2013, S$19,651

A Study on Software Root of Trust Using Virtualization Techniques, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): DING Xuhua, 2012, S$18,751.11

SESUM: A Secure Email System Using a Mediator, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): DING Xuhua, 2004, S$40,000

TEACHING

Courses Taught

Singapore Management University

Undergraduate Programmes :

- Computer Science Project Experience
- Foundations of Cybersecurity
- Network Security

Postgraduate Professional Programmes :

- Capstone Project - Cybersecurity

Postgraduate Research Programmes :

- Empirical Research Project 1
- Empirical Research Project 2
- Empirical Research Project 3

THESES AND DISSERTATIONS

Theses and Dissertations Supervised

Singapore Management University

Supervisor, "Secure Enforcement Of Isolation Policy On Multicore Platforms With Virtualization Techniques", Dissertation by ZHAO SIQI, PhD in Information Systems, Singapore Management University, 2018

Theses and Dissertations Assessed

Singapore Management University

Committee Member, "Techniques for Identifying Mobile Platform Vulnerabilities and Detecting Policy-violating Applications", Dissertation by SU MON KYWE, PhD in Information Systems, Singapore Management University, 2017

Committee Member, "Towards Secure Online Distribution of Multimedia Codestream", Dissertation by LO SWEE WON, PhD in Information Systems, Singapore Management University, 2016

Committee Member, "Online Social Network Based Information Disclosure Analysis", Dissertation by LI YAN, PhD in Information Systems, Singapore Management University, 2014

Committee Member, "Security and Privacy in RFID-Enabled Supply Chains", Dissertation by CAI SHAOYING, PhD in Information Systems, Singapore Management University, 2014

Committee Member, "Virtualization-Based System Hardening Against Untrusted Kernels", Dissertation by CHENG YUEQIANG, PhD in Information Systems, Singapore Management University, 2014

Committee Member, "A Study of the Imitation, Collection and Usability Issues of Keystroke Biometrics", Dissertation by TEY CHEE MENG, PhD in Information Systems, Singapore Management University, 2013

Co Supervisor, "Exploiting Human Factors in User Authentication", Dissertation by GUPTA PAYAS, PhD in Information Systems, Singapore Management University, 2013