

Research Statement

Robert Deng

School of Computing & Information Systems, Singapore Management University

Tel : (65) 6828-0920; Email: robertdeng@smu.edu.sg

1 December 2024

Background

The same quality of openness of the cyberspace that enabled various social and business opportunities also provided opportunities for malicious parties to create havocs. My overall research objective has been developing core technologies and systems to build trust and protect privacy in the cyberspace. Specifically, my research efforts focus on 1) identifying security requirements of existing and emerging systems and applications, 2) designing efficient security algorithms and protocols to meet these security requirements, and 3) conducting rigorous analysis to expose serious vulnerabilities in existing systems and devising efficient techniques to fix the vulnerabilities.

Research Areas

A. Security protocols

A security protocol is a sequence of logical message exchanges between multiple parties that performs a security function in the presence of powerful adversaries. Security protocols are designed for certain application and system contexts and under precisely defined threat models; they serve as the foundation of secure system designs. My effort in this area includes the following.

- *Fair exchange.* A fair exchange protocol allows two parties who potentially do not trust each other to exchange digital valuables “simultaneously” over the Internet. Such protocols find many applications such as online electronic contract signing, fair purchasing and certified document delivery. Existing protocols either require many rounds of interactions between the two parties and without guarantee of true fairness or require an on-line trusted third party (TTP) to mediate the exchange which is both a security and performance bottleneck. I and co-authors proposed the first fair exchange protocol with off-line TTP that achieves true fairness [S&P’98]. In our design, the TTP does not take part in the exchange unless one party tries to cheat the other party. A software system and a patent [US patent 7,171,559] of the fair exchange protocol were licensed by Singapore’s Kent Ridge Digital Labs to Computer Associates International, USA, in 1998.
- *RFID privacy.* The problem of unauthorized tracking of RFID tag bearers had been recognized as an imperative privacy concern in the deployments of RFID systems. As a result, several formal RFID privacy models were proposed independently in the literature. However, it was not clear how these models are related (e. g., which model is stronger) and what are required to implement these models. I and co-authors systematically studied these models in a unified framework and established in theory their relationships and the necessary conditions to implement them [CCS’09, TISS’01]. We further proposed a new and practical RFID privacy model [JCS’11] based on a zero-knowledge formulation and showed that the new model is strictly stronger than the existing models, which answered an open question in the literature.
- *TLS deep packet inspection.* Transport Layer Security Inspection (TLSI) enables enterprises to decrypt, inspect and then re-encrypt users’ traffic before it is routed to the destination. This breaks the end-to-end security guarantee of the TLS specification and prompted the US National Security Agency to issue an alert on TLSI citing potential security issues including insider threats. We proposed Pine [Best Paper ESORICS’20], a new protocol for privacy-preserving inspection of encrypted traffic that preserves the end-to-end security guarantee of TLS and at the same time significantly improves the computation time and communication overhead. For a typical connection from a client to a server, Pine is 27% faster and saves 92.3% communication cost compared with the state-of-the art in the literature.
- *Security and privacy in IoT networks.* Existing service discovery protocols in wireless networks, such as Wi-Fi, AirDrop, and BLE, often leak sensitive information and allow attackers to track users’ movements. We proposed a new service discovery protocol [NDSS’24] which allows a service provider and a client to respectively specify a fine-grained access policy that the other party must satisfy before a service is discovery and connection is established, and hence providing privacy of both service providers and clients.

We also proposed a novel protocol that enables a service provider to quickly and efficiently identify and authenticate from hundreds to thousands IoT sensors simultaneously and establish secure connections with them [CCS'24].

B. New attacks and prevention

Cybersecurity is a constant battle between defenders and attackers. To defend a system, one needs to understand the vulnerabilities of the systems and how they can be exploited by hackers. Hence, discovering vulnerabilities and new attacks is a vital aspect of cybersecurity, and most of the critical vulnerabilities and state-of-the-art attack methodologies were discovered by university researchers.

- *Fault based attack on public key cryptosystems.* I and co-authors were the first to publish fault-based attacks to public key cryptosystems (PKCs) on tamper-resistant devices [Cipher'96, SP'97]. The attack extracts private cryptographic keys from tamper-resistant hardware devices such as smart cards. This result received tremendous attention from the security research community, smart card industry, and standard bodies. Fault-based attacks, together with timing attacks and differential-power analysis, formed a new research area: side channel attack to security hardware, which has become one of the most challenging problems in security today.
- *Attacks to user authentication systems.* Password and PIN have been the dominate user authentication technique since the advent of computers. However, password and PIN leakage has been the main source of attacks to information systems. Whether it was feasible to design leakage-resilient password systems (LRPSes) remained an open problem despite several decades of intensive research. We proposed for the first time two generic attacks to LRPSes and created a quantitative analysis framework on usability costs of LRPSes using results in cognitive computational psychology, and showed that it's impossible to design a LRPS which is both secure and usable without the assistance of a trusted device [Distinguished Paper NDSS'12]. We proposed GLACIATE [ESORICS'19], a fully automated tool combining machine learning and program analysis, to detect implementation flaws in password authentication code in Android apps. We collected 16,387 apps from Google Play for evaluation. GLACIATE successfully identified 4,105 of these with faulty password authentication implementations.
- *Generic attacks on iOS.* Any third-party apps developed for iOS devices are required to go through Apple's app vetting process and then appear on the official iTunes App Store only upon approval. When an app is downloaded from the store and installed on an iOS device, it is given a limited set of privileges, which are enforced by iOS app sandbox. We proposed for the first time a generic technique that enables third-party apps to launch attacks on non-jailbroken iOS devices and constructed multiple proof-of-concept attacks, such as cracking device PIN, sending SMS messages and taking screen snapshots without user's awareness [ACNS'13]. Our apps embedded with the malicious codes passed Apple's vetting process, appeared in iTunes App Store, and worked as intended on non-jailbroken devices. We notified Apple our findings in October 2012, which then rectified the problems before its global launch of iOS 7 and acknowledged our effort in September 2013.

C. Data security and privacy

Outsourcing data to the cloud brings many benefits to users; however, data breaches have taken center stage in recent years. According to *IBM Cost of a Data Breach Report 2024*, the global average cost of a data breach was US\$4.88m in 2024. My approach to address cloud data breaches is using end-to-end encryption (EE2E) such that data is protected during transit and storage, and at the same time data can still be shared, searched, and processed, all in encrypted form.

- *Access control of encrypted data.* Data encryption using the traditional symmetric and public key cryptosystems is not amenable to scalable access control because they are one-to-one encryption systems. Attribute-based encryption (ABE), as a one-to-many public key encryption system, is a promising solution for realizing fine-grained access control of encrypted data in the cloud. However, the basic ABE system lacks many essential features for practical deployment. My research contributed towards making ABE practically deployable. We designed a hierarchical attribute-set-based encryption system to support access control when the number of users is large [TIFS'12], proposed verifiable outsourced decryption for ABE [TIFS'13] which allows a public server to help ABE decryption while without learning anything about

plaintext data, and proposed novel user revocation methods for ABE to support dynamic user private key management [ESORICS'16, S&P'24].

- *Secure search over encrypted data.* Searchable Encryption (SE) enables private queries on encrypted data. “Efficiently deployable, efficiently searchable encryption” (EDESE) is one of the most SE schemes that have been deployed. We proposed LEAP [CCS'21], a leakage-abuse attack on EDESE that can accurately recover the underlying keywords of query tokens based on partially known documents. This is the first attack on EDESE that achieves keyword recovery and document recovery without error based on partially known documents.
- *Secure computations.* Fully homomorphic encryption (FHE), regarded as the holy grail of cryptography, enables an untrusted server to perform computations over encrypted data while without learning the input and the output of the computation. A severe limitation of FHE, however, is that the computation server needs to periodically perform the very costly “bootstrapping” operation after only a small number of computations, which greatly limits the general applicability of FHE in practice. I and co-authors introduced a novel twin-server framework for Secure Outsourced Computation over Integers (SOCI) [TIFS'22, '24]. This framework eliminates the need for “bootstrapping”, enables an unlimited number of computations over ciphertexts, and significantly improves performance in secure computing tasks such as person re-identification [Best Paper DSC'2022].

Future Directions

The traditional PKC (public key cryptography), which is ubiquitously deployed in almost all devices and IT infrastructures to provide authentication, confidentiality, and integrity protection for users and businesses, can be broken easily using Shor's algorithm on cryptographically relevant quantum computers (CRQCs). It is generally believed that CRQCs will be available in the next decade and NIST (National Institute of Standards and Technology) encourages public and private sectors to start PQC (post-quantum cryptography) migration, i. e., transitioning from the traditional PKC to the new PQC as soon as possible. Singapore's MAS published in February 2024 “Advisory on Addressing the Cybersecurity Risks Associated with Quantum” to all Singapore financial institutions. New PQC algorithms, applications, and migration will be the main focus of my research in the near future.

References

- [S&P'95] R. H. Deng, S. K. Bhonsle, W. Wang, and A. A. Lazar, "Integrating security in CORBA based object architectures," *Proceedings of the 1995 IEEE Symposium on Security and Privacy*, pp. 50-61, May 1995, Oakland, CA.
- [Cipher'96] F. Bao, R. Deng, Y. Han, A. Jeng, D. Narasimhalu, T. Nagir, “New attacks to public key cryptosystems on tamperproof devices”, https://www.ieee-security.org/Cipher/Newsbriefs/1996/961029_sgtamper.html
- [SP'97] F. Bao, R. H. Deng, Y. Han, A. Jeng, D. Narasimhalu, and T. Ngair, "Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults", In B. Christianson, B. Crispo, M. Lomas, and M. Roe Editors, *Security Protocols, LNCS 1361*, pp. 115-124, 1997.
- [S&P'98] F. Bao, R. H. Deng, and W. Mao, "Efficient and practical fair exchange protocols", *1998 IEEE Symposium on Security and Privacy*, pp. 77-85, May 1998, Oakland, CA, USA.
- [CCS'02] R. H. Deng, J. Zhou and F. Bao, “Defending against redirect attacks in mobile IP”, *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 59-67, November 2002, Washington DC.
- [CCS'09] C. Ma, Y. Li, R. H. Deng and T. Li, “RFID privacy: relation between two notions, minimal condition, and efficient construction”, *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS 2009)*, pp. 54-65, 9-13 November 2009, Chicago, USA.
- [JCS'11] R. H. Deng, Y. Li, M. Yung and Y. Zhao, “A zero-knowledge based framework for RFID privacy”, *Journal of Computer Security*, Vol. 19, No. 6, 2011.
- [NDSS'12] Q. Yan, J. Han, Y. Li and R. H. Deng, “On limitations of designing leakage-resilient password systems: attacks, principles and usability”, *Proceedings of the 19th Network and Distributed System Security Symposium*, February 2012, San Diego, California, USA. Distinguished Paper Award

- [TIFS'12] Z. Wan, J. Liu and R. Deng, "HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing", *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 2, pp.743-754, April 2012.
- [ACNS'13] J. Han, S. Kywe, Q. Yan, F. Bao, R. Deng, D. Gao, Y. Li and J. Zhou, "Launching generic attacks on iOS with approved third-party applications", *Proceedings of the 11th International Conference on Applied Cryptography and Network Security*, LNCS Vol. 7954, Springer, pp. 272-289, June 2013, Banff, Canada.
- [TIFS'13] J. Lai, R. Deng, C. Guan and J. Weng, "Attributed-based encryption with verifiable outsourced decryption", *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 8, pp. 1343-1354, August 2013.
- [CCS'15] Y. Li, Y. Li, Q. Yan, H. Kong and R. H. Deng, "Seeing your face is not enough: an inertial sensor-based liveness detection for face authentication", *Proceedings of the 22nd ACM Conference on Computer and Communications Security*, pp. 1558-1569, Denver, Colorado, USA, 12-16 October 2015.
- [ESORICS'16] H. Cui, R. Deng, Y. Li, B. Qin, "Server-aided revocable attribute-based encryption", *Proceedings of the 21st European Symposium on Research in Computer Security*, LNCS 9879, pp. 570-587, Heraklion, Greece, 26-30 September 2016.
- [ESORICS'19] S. Ma, E. Bertino, S. Nepal, D. Li, R. Deng, and S. Jha, "Finding flaws from password authentication code in Android apps", *Proceedings of the 24th European Symposium on Research in Computer Security*, pp. 619-637, Luxembourg, 23-27 Sept 2019.
- [ESORICS'20] J. Ning, X. Huang, G. Poh, S. Xu, J. Loh, J. Weng, R. H. Deng, "Pine: enabling privacy-preserving deep packet inspection on TLS with rule-hiding and fast connection establishment", *Proceedings of the 25th European Symposium on Research in Computer Security*, Guildford, UK, 14-18 Sept 2020. Best Paper
- [CCS'21] J. Ning, X. Huang, G. Poh, J. Yuan, Y. Li, J. Weng, R. Deng, "LEAP: leakage-abuse attack on efficiently deployable, efficiently searchable encryption with partially known dataset", *Proceedings of the ACM Conference on Computer and Communications Security*, Seoul, South Korea, Nov. 14-19, 2021
- [TIFS'22] B. Zhao, J. Yuan, X. Liu, Y. Wu, H. Pang, R. Deng, "SOCl: A Toolkit for Secure Outsourced Computation on Integers", *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp. 3637-3648, 2022.
- [DSC'22] B. Zhao, Y. Li, X. Liu, H. Pang, R. Deng, "FREED: An efficient privacy-preserving solution for person re-identification", *Proceedings of the IEEE Conference on Dependable and Secure Computing (IEEE DSC 2022)*, pp. 1-8, 22-24 June 2022, Edinburgh, UK (Best Paper Award).
- [TIFS'24] Y. Zhao, W. Deng, X. Li, X.g Liu, Q. Pei, R. Deng, "SOCl+: An enhanced toolkit for secure outsourced computation on integers", *IEEE Transactions on Information Forensics and Security*, Vol.19, pp. 5607-5619, 2024.
- [NDSS'24] Y. Yang, R. Deng, G. Yang, Y. Li, H. Pang, M. Huang, R. Shi, J. Weng, "PriSrv: privacy-enhanced and highly usable service discovery in wireless communications", *Proceedings of the Network and Distributed System Security Symposium (NDSS 2024)*, 26 Feb – 1 Mar 2024, San Diego, USA.
- [S&P'24] X. Li, G. Yang, T. Xiang, B. Zhao, H. Pang, R. Deng, "Make revocation cheaper: hardware-based revocable attribute-based encryption", *Proceedings of IEEE Symposium on Security and Privacy (S&P 2024)*, pp. 3109-3127, 20-22 May 2024, San Francisco, USA.
- [CCS'24] Z. Ren, X. Li, Y. Miao, M. Zhu, S. Yuan, R. Deng, "PIC-BI: practical and intelligent combinatorial batch identification for UAV assisted IoT networks", *Proceedings of the ACM Computer and Communications Security*, 14-18 October, Salt Lake City, USA.