Research Statement

Robert Deng
School of Computing and Information Systems, Singapore Management University
Tel: (65) 6828-0920; Email: robertdeng@smu.edu.sg
19 December 2023

Background and Evolution of My Research

The same quality of openness of the cyberspace that enables various social and business opportunities also provides 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.

From the very early days of my research, I observed that there had been a huge gap between the theoretical cryptographic research community and the system and application-oriented research community -- numerous cryptographic algorithms were published but very few of them were being used mainly because these algorithms were designed for academic novelty and theoretical provable security but with little or no consideration in efficiency, usability and scalability. Hence, the main focal point of my research has been bridging the gap between the cryptographic research and the system and application security research by 1) identifying security requirements of existing and emerging systems and applications, and 2) designing efficient algorithms and protocols to meet these requirements.

Research Areas

A. Security protocol

A security protocol is a sequence of logical message exchanges between multiple parities 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 protocols*. 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 email 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 TPP does not take part in the exchange unless one party tries to cheat the other party. The protocol achieves true fairness in the sense that no loss is incurred to a party no matter how improperly the other party performs.
- *RFID privacy models and protocols*. 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. We established in theory the relationship between the two most well-known RFID privacy models, the unpredictability-privacy (unp-privacy) model and the indistinguishability-privacy (ind-privacy) model, and we proved the minimal condition on RFID tags to achieve unp-privacy [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 ind-privacy model, which answered an open question in the literature.
- *TLS deep packet inspection protocols*. 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 implementation and recently prompted the US National Security Agency to issue an alert on TLSI citing potential security issues including insider threats. PrivDPI in CCS'19 proposed a privacy-preserving approach that inspects encrypted traffic directly to address the security issues but it incurs significant processing overhead. We proposed Pine [ESORICS'20], a new protocol for privacy-preserving inspection of encrypted traffic that 1) simplifies the preprocessing step of PrivDPI thus significantly reduces the computation time and communication overhead; 2) supports inspection rule hiding; and 3) enables dynamic rule addition without the need to re-execute the protocol from scratch. For a typical connection from a client to a server, Pine is 27% faster and saves 92.3% communication cost compared with PrivDPI.

- *Privacy-enhanced service discovery protocols.* Service discovery is essential in wireless communications. However, existing service discovery protocols provide no or very limited privacy protection for service providers and clients, and they often leak sensitive information (e.g., service type, client's identity and mobility pattern) or only enable unilateral authorization control, which leads to various network-based (e.g., spoofing, man-in-the-middle, identification and tracking) attacks. We proposed PriSrv [NDSS'24], a private service discovery protocol which allows a service provider and a client to respectively specify a fine-grained authorization policy that the other party must satisfy before a connection is established. PriSrv consists of a private service broadcast phase and an anonymous mutual authentication phase with bilateral control, where the private information of both parties is hidden beyond the fact that a mutual match to the respective authorization policy occurred.

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 system and how they can be exploited by hackers. Hence, discovering vulnerabilities and new attacks is a vital aspect of cybersecurity research.

- *Attacks to authentication systems*. Password leakage has been the main source of attacks to information systems. Whether it is 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 in order to systematically assess their security strength, 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 [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. Instead of creating detection templates/rules manually, GLACIATE automatically and accurately learns the common authentication flaws from a relatively small training dataset, and then identifies whether the authentication flaws exist in other apps. We collected 16,387 apps from Google Play for evaluation. GLACIATE successfully identified 4,105 of these with faulty password authentication implementations.

  While PIN-based user authentication systems such as ATM have long been considered secure, we proposed a novel attack, named UltraPIN [AsiaCCS'21], which can be launched from commodity smartphones. As a target user enters a PIN on a PIN-based user authentication system, an attacker can use UltraPIN to infer the PIN from a short distance (50cm to 150cm) without a line of sight. Rigorous experiments show that UltraPIN is highly effective in PIN inference and its performance is robust to changes in keypad layout, keypad size, keypad angle, smartphone position, and smartphone to keypad distance.

- *Generic attacks on iOS.* Any third-party apps developed for iOS devices are required to go through Apple's app vetting process and 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.

We were also the first to establish a baseline for security comparison between Andriod and iOS platforms. We analyzed more than 2,600 apps that run on both platforms and examined the difference in the usage of their security sensitive APIs (SS-APIs). This work was featured as a promotional article in NDSS'13.

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 2020*, the global average cost of a data breach was $3.86m in 2020. 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. We designed a hierarchical attribute-set-based encryption system to support access control when the number of users is very 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 a server-aided revocable ABE [ESORICS'16] and a hardware-aided revocable ABE [S&P'24] to support dynamic user private key management.

- *Privacy-preserving keyword search over encrypted data*. Searchable Encryption (SE) enables private queries on encrypted data. Most existing SE schemes focus on constructing "efficiently deployable, efficiently searchable encryption" (EDESE). We proposed LEAP [CCS'21], a leakage-abuse attack on EDESE schemes that can accurately recover the underlying keywords of query tokens based on partially known documents. This is the first attack on EDESE schemes that achieves keyword recovery and document recovery without error based on partially known documents.

- *Secure computation*. Encryption provides strong protection to data privacy. However, encrypted data must be still amendable to computation in addition to sharing and search. Fully homomorphic encryption (FHE) allows a user to privately outsource computation to an untrusted server which performs computation but never gains access to the input, the intermediate result, and the final output. A major limitation of FHE, however, is that the server cannot follow data dependent flows in its computation since all the intermediate results are encrypted, and the server cannot take actions based on the output of the computation since the final result is also encrypted. Recently, we proposed a twin-server architecture for secure computation [TDSC'18b, TIFS'22] which overcomes the limitation of FHE and we applied the architecture for privacy-preserving person re-identification [DSC'22].

Future Directions

- *Privacy protection in machine learning* (ML). As Google, Microsoft, Amazon and the like provide customers with access to APIs to easily embed ML tasks into their applications, organizations can use ML-as-a-service (MLaaS) engines to outsource complex computations tasks to the cloud. This approach naturally raises serious privacy issues. I am excited with the opportunities of applying secure computation to achieve privacy-preserving MLaaS and in particular in preventing

leakage of user data during model training and predictions, and in protecting the secret or proprietary model parameters.

- *Privacy protection in Internet of Things* (IoT). IoT provides numerous services for users and devices. The sheer scale and pervasiveness of IoT brings with it a large attack surface which can have a huge implication on individual's privacy. For example, by monitoring the service types a user requests over time, one can deduce his/her movement patterns and lifestyle. A key question is how to preserve users' privacy while without adversely affect users' service experience given that IoT devices are limited in resources.

Selection Publications

[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.

[CCS'97] R. H. Deng, Y. Han, A. B. Jeng, and T.-H. Ngair, "A new on-line cash check scheme", *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pp. 111-116, Zurich, Switzerland, April 1997.

[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.

[MM'03] C. Peng, R. H. Deng, Y. Wu and W. Shao, "A flexible and scalable authentication scheme for JPEG2000 image codestreams", *Proceedings of the 11th ACM International Conference on Multimedia*, pp. 433-441, 4-6 Nov 2003, Berkeley, USA.

[S&P'06] Y. Li, H. Liu and R. H. Deng, "Practical inference control for data cubes", *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 115-120, May 2006, Oakland, CA, USA.

[TMM'07] Y. Wu, D. Ma and R. H. Deng, "Flexible access control to JPEG2000 image code-streams", *IEEE Transactions on Multimedia*, Vol. 9, No. 6, pp. 1314-1324, October 2007.

[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.

[TDSC'10] Y. Yang, Y. Li, R. H. Deng and F. Bao, "Shifting Inference Control to User Side: Architecture and Protocol", *IEEE Transactions on Dependable and Secure Computing*, Vol. 7, No. 2, pp. 189-202, April-June 2010.

[TISS'11] Y. Li, R. H. Deng, J. Lai, and C. Ma, "On two RFID privacy notions and their relations", *ACM Transactions on Information and Systems Security*, Vol. 14, No. 4, 2011.

[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.

[NDSS'13] J. Han, Q. Yan, D. Gao, J. Zhou and R. H. Deng, "Comparing mobile privacy protection through cross-platform applications", *Proceedings of the 20th Annual Network & Distributed System Security Symposium,* February 2013, San Diego, USA.

[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'15] S. Lo, Z. Wei, R. H. Deng and X. Ding, "On security of content-based video stream authentication", *Proceedings of the 20th Europrean Symposium on Research in Computer Security*, pp. 366-383, Vienna, Austria, 21-25 September 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.

[TBD'16] Z. Yan, W. Ding, X. Yu, H. Zhu, R. Deng, "Deduplication on encrypted big data in cloud", *IEEE Transactions on Big Data*, Vol. 2, No. 2, pp. 138-150, July, 2016. 2017 Best Journal Paper

[TDSC'18] Z. Wan and R. H. Deng, "VPSearch: achieving verifiability for privacy-preserving multi-keyword search over encrypted cloud data", *IEEE Transactions on Dependable and Secure Computing,* Vol. 15, No. 6, pp. 1083-1095, Nov/Dec, 2018.

[TDSC'18a] H Cui, Z. Wan, R. H. Deng, G. Wang, and Y. Li, "Efficient and expressive keyword search over encrypted data in the cloud", *IEEE Transactions on Secure and Dependable Secure Computing*, Vol. 15, No. 3, pp. 409-422, May/June 2018.

[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.

[NDSS'19] D. Wu, D. Gao, R. Chang, E. He, E. Cheng, and R. H. Deng, "Understanding open ports in Android applications: discovery, diagnosis, and security assessment", *Proceedings of the 26th Annual Network & Distributed System Security Symposium* (NDSS 2019), 24-27 February 2019, San Diego, USA.

[TDSC'20] Y. Yang, X. Liu, R. H. Deng and Y. Li, "Lightweight sharable and traceable secure mobile health system", *IEEE Transactions on Dependable and Secure Computing,* Vol. 17, No. 1, pp. 78-91, Jan/Feb 2020.

[TDSC'20a] X. Liu, R. H. Deng, K. Choo, Y. Yang, H. Pang, "Privacy-preserving outsourced calculation toolkit in the cloud," *IEEE Trans. Dependable Secure Computing*, 17, No. 5, pp. 898-911, Sept/Oct 2020.

[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

[AsiaCCS'21] X.Liu, Y. Li, and R. Deng, "UltraPIN: inferring PIN entries via Ultrasound", *Proceedings of the 21st ACM Asia Conference on Computer and Communications Security*, pp. 944-957, Hong Kong, 7-11 June 2021.

[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

[NDSS'21] J. Xu, Y. Li, and R. Deng, "Differential training: a generic framework to reduce label noises for Android malware detection", *Proceedings of the 2021 Network and Distributed System Security Symposium* (NDSS 2021), 21-24 February 2021, Online.

[TDSC'21] Y. Zhang, R. Deng, E. Bertino, D. Zheng, "Robust and universal seamless handover authentication in 5G HetNets", *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 2, pp. 858-874, Mar – Apr 2021.

[TIFS'22] B. Zhao, J. Yuan, X. Liu, Y. Wu, H. Pang, R. Deng, "SOCI: 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).

[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 2024 Network and Distributed System Security Symposium* (NDSS 2024), 26 February - 1 March 2024, San Diego, CA, USA.

[S&P'24] X. Li, G. Yang, T. Xiang, S. Xu, B. Zhao, H. Pang, R. H. Deng," Make revocation cheaper: hardware-Based revocable attribute-based encryption", *Proceedings of the IEEE Symposium on Security and Privacy* (S&P'24), 20-23 May 2024, San Francisco, CA, USA.