Research Statement

Robert H. Deng
School of Information Systems, Singapore Management University
Tel: (65) 6828-0920; Email: robertdeng@smu.edu.sg
January 2015

Background

Cyberspace is critical to any business and paramount to the survival of any organization in today's globalized digital economy. However, the same technology that enables digital economy also provides opportunities for hackers, malicious individuals and even terrorist organizations to create havocs. Despite efforts in recent years to add security components to computing systems, networks and software, the act of hostile parities can propagate far and wide, with damaging efforts on a national or international scale. Most indicators and studies of the frequency, impact, scope and cost of security incidents point to continuously increasing levels and varieties of attacks.

My research focuses on cybersecurity techniques and solutions that create impact in real world systems and applications.

Mobile Computing Security

With the rapid growth of the mobile market, security of mobile platforms is receiving increasing attention from both research community as well as the public. We made the first attempt to establish a baseline for security comparison between the two most popular mobile platforms by studying applications that run on both Android and iOS and examined the difference in the usage of their security sensitive APIs (SS-APIs) [1]. This article was featured at the home page of NDSS2013's promotional website.

Any third-party applications developed for iOS devices are required to go through Apple's application vetting process and appear on the official iTunes App Store upon approval. When an application is downloaded from the store and installed on an iOS device, it is given a limited set of privileges, which are enforced by iOS application sandbox. Although details of the vetting process and the sandbox are kept as black box by Apple, it was generally believed that these iOS security mechanisms are effective in defending against malwares. We proposed a generic attack vector that enables third-party applications to launch attacks on non-jailbroken iOS devices. Following this generic attack mechanism, we are able to construct multiple proof-of-concept attacks, such as cracking device PIN and taking snapshots without user's awareness. Our applications embedded with the attack codes passed Apple's vetting process and worked as intended on non-

jailbroken devices. Our proof-of-concept attacks shown that Apple'svetting process and iOS sandbox have weaknesses which can be exploited by third-party applications. We further provided mitigation strategies for both vetting and sandbox mechanisms, in order to defend against the proposed attack vector [2].

RFID Security and Privacy

Radio Frequency Identification (RFID) has been widely envisioned as an inevitable replacement of barcodes and other consumer labelling techniques for automatic object identification. However, since RF signals are invisible and penetrating, RFID systems provide a perfect working environment for attackers. The problem of unauthorized tracking of RFID system users and RFID tag bearers has been recognized as one of the most imperative privacy concerns in the deployments of RFID systems.

Existing research efforts mainly offer ad hoc notions of security. As a result, most of the RFID privacy protocols proposed in the literature have been broken. This calls for formal models and formal analysis methodology to be adopted in the design of RFID privacy protocols. Recently, there have been several attempts in establishing formal RFID privacy models in the literature. These models fall into two categories: one based on the notion of indistinguishability of two RFID tags, denoted as ind-privacy, and the other based on the unpredictability of the output of a RFID protocol, denoted as unp-privacy. We formally established the relationship between ind-privacy and unp-privacy and proved the minimal condition for RFID tags to support such models [3, 4]. We also proposed a new privacy model, called ZK-privacy model, which is more general than the existing models [5, 6].

RFID technology has been used to improve efficiency and visibility of supply chains. Unauthorized tracking in such systems may take place at the physical-level or the system-level. Prior research has mostly focused on the prevention of clandestine scanning at the physical level, where an adversary uses an unauthorized reader collecting RF waves to track the movement of RFID tags. However, the threat of unauthorized tracking at the system level, where an adversary tracks movement of RFID tagged assets by eavesdropping network messages or compromising date center servers, has not been well recognized in the literature. Compared to the former, the latter could be even more harmful as the adversary is able to obtain tracking information on a global scale and without physical presence. Our initial effort on protecting RFID information at the network level is reported in [7].

Multimedia Distribution Security

Modern multimedia processing standards, such as JPEG2000 for image coding and H.264/SVC for video coding are designed with scalability in mind and possess the so called “compress once, decompress many times” properties.

Such scalable multimedia coding techniques automatically adapt to network bandwidth as well as capabilities of end user devices. Authentication and access control of multimedia content are indispensable in certain applications, such as government, finance, health care and law. Our authentication scheme [8] and access control scheme [9] for JPEG2000 code streams are fully compatible with the core part of the JPEG2000 and have been incorporated into the international standard document ISO/IEC JPSEC 1544-8 in April 2007.

We investigated solutions for multimedia content protection in the server-proxy-user architecture, which is increasingly becoming accepted as a promising paradigm for multimedia content delivery. In this architecture, one or more intelligent intermediary proxies reside along the path from a multimedia server that disseminates content to end users. Each proxy serves a distinct group of users and is entrusted by the server to perform certain transcoding operations upon the content according to the end users' specific capabilities, configurations, or preferences. We systematically study techniques for safeguarding end-to-end multimedia content authenticity [10] and confidentiality throughout the entire lifecycle of content delivery in the the server-proxy-user architecture.

Our current research focuses on protectiong H.264/SVC video streams over packet-lossy networks. We proposed and implemented a very efficient and robust authentication schemes for H.264/SVC [16]. Partial encryption is often used as a tradeoff between security and performance to protect scalable video streams. We showed experimentally and theoretically that partial encryption leaks significant content information from the enhancement layers in all three scalability dimensions and concluded that all layers must be encrypted to protect confidential video streams [11]. We proposed a novel block based technique for authenticating SVC streams, which is robust against transcoding operations by network proxies [17].

Cloud Computing Security and Privacy

Cloud computing enables end users with limited resources to outsource data storage and processing services to the cloud, where massive storage and computational capacities are available. In cloud computing, users have to give up their data to the cloud service provider for storage and business operations, while the cloud service provider is usually a commercial enterprise which cannot be totally trusted. Hence, data security and privacy have been major concerns in cloud computing. A promising solution is encryption, i.e., data owners encrypt their data and upload ciphertext to the cloud. In order for such encrypted data to be useful, however, encryption must not hinder access and processing on the data.

Access control is a classic security topic which dates back to 1960s or early 1970s, and various access control models have been proposed since then. Unfortunately, these schemes are only applicable to systems in which data

owners and the service providers are within the same trusted domain (e. g. when data is stored in cleartext at trusted service providers). Since data owners and service providers are usually not in the same trusted domain in cloud computing, a new framework and techniques are needed to achieve flexible access control of encrypted data stored at untrusted cloud service providers. We designed HASBE (hierarchical attribute-based solution for flexible and scalable access control in the cloud) [12] which assumes that servers are not trusted to keep data confidential and not trusted to enforce access control correctly. HASBE not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of attribute-set-based encryption.

Ciphertext Policy Attribute-Based Encryption (CP-ABE) is one of the core technologies for realizing flexible and scalable access control of encrypted data in the cloud. In a traditional CP-ABE scheme, an access structure, referred to as ciphertext policy, is sent along with a ciphertext explicitly, and anyone who obtains a ciphertext can know the access structure associated with the ciphertext. In certain applications, access structures contain sensitive information and must be protected from everyone except the users whose private key attributes satisfy the access structures. We proposed a new model for CP-ABE with partially hidden access structures [18]. In our model, each attribute consists of two parts: an attribute name and its value; if the private key attributes of a user do not satisfy the access structure associated with a ciphertext, the specific attribute values of the access structure are hidden, while other information about the access structure is public. We also presented an efficient construction of CP-ABE with partially hidden access structures and demonstrated how it can be used to design privacy-preserving access control systems for encrypted data in untrusted servers [13].

One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. ABE system with outsourced decryption largely eliminates the decryption overhead for users. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE ciphertext satisfied by that user's attributes or access policy into a simple ciphertext, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed ciphertext. We proposed a verifiable ABE system with outsourced decryption. The system not only ensures that an adversary (including a malicious cloud) will not be able to learn anything about the encrypted message, but also guarantees the correctness of the transformation done by the cloud [15].

In addition to allow access control of encrypted data in the cloud, a more challenging problem is allowing process of encrypted data by the cloud, such that the cloud performs certain computations on the data but without knowing the

data values. We proposed verifiable homomorphic encryption which enables verifiable computation of linear functions on outsourced encrypted data [15].

References

1. Jin Han, Qiang Yan, Debin Gao, Jianying Zhou and Robert H. Deng, "Comparing mobile privacy protection through cross-platform applications", *Proceedings of the 20th Annual Network & Distributed System Security Symposium* (NDSS 2013), 24-27 February 2013, San Diego, USA.
2. Jin Han, Su Mon Kywe, Qiang Yan, Feng Bao, Robert H. Deng, Debin Gao, Yingjiu Li and Jianying Zhou, "Launching generic attacks on iOS with approved third-party applications", Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS2013), LNCS Vol. 7954, Springer, pp. 272-289, June 2013, Banff, Canada.
3. Changshe Ma, Yingjiu Li, Robert H, Deng and Tieyan 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), November 2009, Chicago, USA.
4. Yingjiu Li, Robert H. Deng, Junzuo Lai, and Changshe Ma, "On two RFID privacy notions and their relations", ACM *Transactions on Information and Systems Security*, Vol. 14, No. 4, 2011.
5. Robert H. Deng, Yingjiu Li, Moti Yung and Yunlei Zhao, "A new framework for RFID privacy", *Proceedings of the 15th European Symposium on Research in Computer Security* (ESORICS 2010), LNCS 6345, Springer, pp. 1-18, 20-22 September 2010, Athens, Greece.
6. Robert H. Deng, Yingjiu Li, Moti Yung and Yunlei Zhao, "A zero-knowledge based framework for RFID privacy", *Journal of Computer Security*, Vol. 19, No. 6, 2011.
7. Jie Shi, Darren Sim, Yingjiu Li and Robert H. Deng, "SecDS: a secure EPC discovery services system in EPCglobal network", *Proceedings of the 2nd ACM Conference on Data and Application Security and Privacy* (CODASPY 2012), San Antonio, TX, USA, February 2012.
8. R. H. Deng, D. Ma, W. Shao and Y. Wu, "Scalable trusted online dissemination of JPEG2000 images", *ACM Multimedia Systems Journal*, Vol. 11, November 2005.
9. Y. Wu, D. Ma and R. H. Deng, "Flexible access control to JPEG2000 image code-streams", *IEEE Transactions on Multimedia*, Vol. 9, No. 6, October 2007.
10. R. H. Deng and Y. Yang, "A study of data authentication in proxy-enabled multimedia delivery systems: model, schemes and application", *ACM Transactions on Multimedia Computing*, *Communications and Applications*, Vol. 5, No. 4, October 2009.
11. Zhuo Wei, Xuhua Ding, Robert H. Deng, and Yongdong Wu, "No tradeoff between confidentiality and performance: an analysis on H.264/SVC partial encryption", *Proceedings of the 13th Joint IFIP TC6 and TC11 Conference*

on Communications and Multimedia Security (CMS 2012), LNCS 7394, Best Paper Award, Canterbury, UK.

12. Zhiguo Wan, Jun'e Liu and Robert H. 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, 2012.
13. Junzuo Lai, Robert H. Deng and Yingjiu Li, "Expressive CP-ABE with partially hidden access structures", *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2012)*, May 2012, Seoul, Korea.
14. Junzuo Lai, Robert H. Deng, Chaowen Guan and Jian Weng, "Attributed-based encryption with verifiable outsourced decryption", *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 8, pp. 1343-1354, August 2013.
15. Junzuo Lai, Robert H. Deng, Hweehwa Pang and Jian Weng, "Verifiable computation on outsourced encrypted data", Proceedings of the 19th European Symposium on Research in Computer Security, LNCS 8712, Springer, pp. 273-291, 7-11 September, 2014, Wroclaw, Poland.
16. Zhuo Wei, Yongdong Wu, Robert H. Deng and Xuhua Ding, "A hybrid scheme for authenticating scalable video codestreams", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 4, pp. 543-553, April 2014.
17. Robert H. Deng, Xuhua Ding, Yongdong Wu and Zhuo Wei, "Efficient block-based transparent encryption for H.264/SVC bitstreams", Multimedia Systems, Vol. 20, No. 2, pp. 165-178, February 2014.