Research Assessment Exercise 2020
Impact Case Study

University: The Hong Kong Polytechnic University
Unit of Assessment (UoA): 13 Computer studies/science (incl. information technology)

Title of case study: Security and Privacy for the FinTech Infrastructure

(1) Summary of the impact

Our research into the FinTech infrastructure, e.g., cryptographic techniques for blockchain, mobile system security, decentralized identity and privacy, attracted research income of over 16 million HKD in 2018. The resulting technologies have been used to secure digital assets in various cryptocurrency platforms. It also forms the core of a food and drug counterfeit detection and regulatory system adopted by several companies. Now, the research of FinTech infrastructure is being deployed at an identity management system that provides various notary and attestation services to different businesses including academic qualification and insurance companies in HK and Mainland China.

(2) Underpinning research

Responding to FinTech's need to secure computing and ensure data privacy of users, this research proposed methodologies in mobile system security and privacy, blockchain infrastructure and security, and privacy enhancing technology. The findings of this research resulted on the registration of a US patent in network security in 2018.

Mobile Security and Privacy: Latest mobile malware uses advanced approaches, such as packer, emulator detection, etc., to evade the detection and impede the analysis. To address these challenging issues, Dr. Daniel Luo and his team designed the first in-VM unpacker named DexHunter to unpack Android apps and release it to the public. Besides circumventing the emulator detection, we developed Malton, the first on-device non-invasive analysis platform for the new Android runtime (i.e., the ART runtime) [1].

Although more and more developers prepare privacy policies for their apps, little is known whether these privacy policies are trustworthy or not. Therefore, we conducted the first systematic study on privacy policy by proposing a novel approach and developing a new system named PPChecker to automatically identify problematic privacy policy, generating a benefit for users. Moreover, we developed the first system AutoPPG to automatically construct correct and readable descriptions to facilitate the generation of privacy policy for apps.

Blockchain Infrastructure: We focus on investigating smart contracts and Ethereum, the largest blockchain that support smart contracts. In 2018, Dr. Daniel Luo and his team conducted the first systematic investigation on Ethereum via graph analysis, obtaining many new observations and insights regarding the interactions among users and smart contracts [3]. We are also the first to reveal that many smart contracts contain gas-inefficient bytecodes, which waste money and may cause out-of-gas errors, can be replaced with gas-efficient bytecodes to save money. We have developed a system named GasReducer to automatically correct gas-inefficient bytecodes in smart contracts. We also performed the first investigation on the gas costs setting in Ethereum, finding that they are not properly configured and can be exploited to launch attacks. Moreover, we propose and develop TokenScope, the first system to automatically detect the inconsistent behaviors of cryptocurrency tokens in Ethereum [5].

Blockchain Security: Conceptualized in 2008, blockchain is the core technology supporting the first

widely used cryptocurrency Bitcoin. Since there is no coordination in the blockchain environment, a specific class of cryptographic techniques, namely, cryptography for ad hoc group, is needed to provide security and privacy for blockchain system. Dr. Allen Au and his team developed the ring signature technique, a layer of encryption, to provide data privacy, while anonymous signatures are needed to ensure transaction privacy [2]. In 2019, Dr. Bin Xiao and his team analyzed the mining attacks in the blockchain systems that enable attackers to gain an unfair share of the mining reward by deviating from the honest mining strategy in the Bitcoin system. They proposed two new strategies: power adjusting and bribery racing, and introduce two novel mining attacks that can increase the reward of attackers [4]: Power Adjusting Withholding (PAW) and Bribery Selfish Mining (BSM).

Recently, we started exploring threats not just from ordinary attackers, but also emerging threats caused by quantum computers. Specifically, our goal is to develop privacy-preserving cryptographic techniques [6] that can be operated on today's computers yet secured against attacks from quantum computers. Research in this area is extremely valuable and any new advances would easily result in a great impact.

Privacy-Enhancing Technologies: By combining techniques to withstand attacks from quantum computers and anonymous digital signatures without a central authority, we proposed the first anonymous post-quantum cryptocash. Other exciting results from our team in this area include secure and fair protocol that allow the exchange of virtual assets between different blockchain systems (cross chain transactions), accountable anonymous cryptocash and privacy-preserving cryptocash which hides not just sender identity, but also receiver identity and transaction amount.

Patent for Internet Security: Dr. Luo and his team have focused on detecting and defending against various Denial-of-Service attacks. Besides academia papers published in top venues, we recently got one US patent on detecting link-flooding attacks: "Network Attack Detection Method", **US Patent** (US 9876807B2), granted on January 23, 2018.

(3) References to the research

[1] L. Xue, Y. Zhou, T. Chen, X. Luo, and G. Gu, Malton: Towards On-Device Non-Invasive Mobile Malware Analysis for ART, Proc. of 26th USENIX Security Symposium (USENIX SEC), Vancouver, Canada, August 16-18, 2017.
[2] S. Sun, M.H. Au, J.K. Liu, T.H. Yuen. RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero. ESORICS 2017
[3] T. Chen, Y. Zhu, Z. Li, J. Chen, X. Li, X. Luo, X. Lin, and X. Zhang, "Understanding Ethereum via Graph Analysis", IEEE International Conference on Computer Communications (INFOCOM), 2018. Best Paper Award
[4] S. Gao, Z. Li, Z. Peng, and B. Xiao, "Power Adjusting and Bribery Racing: Novel Mining Attacks in the Bitcoin System", Proc. of the 26th ACM Conference on Computer and Communications Security (ACM CCS) (to appear), London, UK, November 11-15, 2019.
[5] T. Chen, Y. Zhang, Z. Li, X. Luo, T. Wang, R. Cao, X. Xiao, and X. Zhang, "TokenScope: Automatically Detecting Inconsistent Behaviors of Cryptocurrency Tokens in Ethereum", Proc. of the 26th ACM Conference on Computer and Communications Security (ACM CCS) (to appear), London, UK, November 11-15, 2019.
[6] R. Yang, M. H. Au, Z. Zhang, Q. Xu, Z. Yu and W. Whyte. Efficient Lattice-Based Zero-Knowledge Arguments with Standard Soundness: Construction and Applications. Proc. of the 38th Annual International Cryptology Conference (CRYPTO 2019) (to appear), 2019

(4) Details of the impact

The impact of our research can be demonstrated in many elements, from best paper award [4],

collaboration with industry and media reports [1]. At a high level, our techniques address the two out of three fundamental challenges faced by typical blockchain applications, namely, efficiency, security and privacy, and therefore enable the development of blockchain-based FinTech applications in different domains.

Impact on mobile and Internet security and privacy

Latest mobile malware adopted sophisticated techniques to evade the existing detection systems and hinder the inspection by security analysts. To address this challenging issue, we have proposed novel solutions to detect and analyze mobile malware targeting on Android system and the vulnerabilities in mobile apps. Moreover, we developed practical systems to facilitate security researchers and professionals to scrutinize mobile malware and legitimate apps and two systems have been released to the public in 2014 and 2015. These initiatives have benefited security researchers.

Impact on Blockchain and Cryptocurrency

The team led by Dr. Allen Au at PolyU, together with their Australian partners, is widely acknowledged to be one of the leading team in protecting user privacy in popular cryptocurrencies. Their work has been discussed or incorporated in CryptoNote, Monero and ZCash with a total market cap of 40 Billion USD [2]. The impact was signified in the grand opening of the Joint Lab on Cryptocurrency and Blockchain Technology, funded by Collinstar Capital, a founding member of the HCash foundation and the leading FinTech Company in Australia [1]. HCash is going to adapt technologies developed by this joint lab, and as of the time of writing, the market cap of HCash is 0.28 Billion USD.

Concretely, our work on "New Empirical Traceability Analysis of CryptoNote-Style Blockchains" has been acknowledged by the recent Monero technical report (MRL-0007), and we are working with Monero to help improving their user privacy. Our work on "RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero" has been widely reported in the public. According to KryptoMoney, the publication of this improvement on cryptocurrency has caused Monero's value to increase by 60% [7]. Our Previous work has been adopted by the Hyperledger Fabric project for privacy-friendly membership management [8]. Hyperledger fabric is a blockchain infrastructure supported by big industry players like IBM, Intel and SAP, and is regarded by many to be the most popular blockchain technology for enterprise applications. Our work on cryptocurrency has been granted a CN patent [6].

Impact on Supply Chain Management

Blockchain technologies allow tracking of goods along a supply chain in an efficient and transparent manner. However, security and privacy remains a major hindrance for its adoption. Our team is one of the first to recognize blockchain's potential in supply chain management. In February 2017, Dr. Au started discussions with UBI Blockchain Internet Ltd. (OTC QB: UBIA) to apply blockchain technologies to fight against fake food/drug. The project is supported by the Innovation and Technology Commission. We developed a prototype system and evaluate its feasibility on 5 products from a mainland drug company 广西厚德大健康产业股份有限公司 [3]. Our prototype has been further commercialized by UBI [9].

Impact on Decentralized Identity Management System

Identity management has always been an important component of any ICT systems. Our privacy-friendly technologies [5] are specifically helpful in securing the personal data of the users, should such a system is to be built. Since 2017, Dr. Au's team has implemented the core algorithm of an identity management system for Valigo Ltd., a local company, generating a benefit on insurance companies and their claimants to simplify claim process. The story has been reported in [10].

(5) Sources to corroborate the impact

[1] Media reports on the establishment of the joint lab of Monash University – Poly U – Collinstar Capital on blockchain and cryptocurrency. [list of over 100 media reports]
https://www.crowdfundinsider.com/2018/03/131152-hong-kongs-polyu-teams-up-with-australias-monash-university-collinstar-capital-for-blockchain-research/
https://medium.com/@CollinstarCapital/collinstar-monash-hk-polytechnic-joint-research-laboratory-opening-ceremony-coming-soon-b96a32ddc515
https://www.comp.polyu.edu.hk/en-us/news/detail/458
[2] Media reports on our paper "RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero".
Monero price increased by 60% (https://coinspectator.com/news/37389/monero-price-surges-top-gainer-in-cryptocurrency-market).
Discussions of our scheme in online forums (e.g. reddit.com).
Developer meeting notes (https://monerobase.com).
Note that as of 21 May 2018, the market cap of Monero is 3.7 billion USD.
[3] Report on our collaboration with UBI Blockchain Internet to develop a blockchain-based system on food and drug safety.
https://www.marketwatch.com/story/ubi-blockchain-internet-announces-hong-kong-government-financing-of-companys-blockchain-based-food-and-drug-safety-technology-development-project-with-hong-kong-polytechnic-university-2018-01-10
http://au.sys-con.com/node/4219058
http://news.sina.com.tw/article/20180111/25363864.html
[4] 2018 Best Paper Award, "Understanding Ethereum via Graph Analysis", IEEE International Conference on Computer Communications (**INFOCOM**) (https://infocom2018.ieee-infocom.org/awards).
[5] Our paper "BLAC: Revoking Repeatedly Misbehaving Anonymous Users without Relying on TTPs" has been cited by 2 US patents
[6] Our CN patent, "一種離線電子貨幣支付的安全運行方法", was granted on 24 Feb 2018 (no. 201510225247.8, https://patents.google.com/patent/CN104850984A/nl)
[7] https://kryptomoney.com/cryptocurrency-news-monero-price-surges/
[8] https://hyperledger-fabric.readthedocs.io/en/release-1.2/idemix.html
[9] https://kknews.cc/zh-mo/tech/6b6m6mp.html
[10] The Hong Kong Polytechnic University 2017/18 Annual Reports on KT Recurrent Funding, p2 https://www.ugc.edu.hk/doc/eng/ugc/activity/kt/PolyU17.pdf