Research Assessment Exercise 2020
Impact Case Study

University: The Chinese University of Hong Kong

Unit of Assessment (UoA): 13 CSIT - Computer Studies/Science (incl. information Technology)

Title of case study: Protecting Billions of Stake-holders from Critical Security Vulnerabilities in Single-Sign-On (SSO) and Mobile Payment Systems via Scalable Security Testing and Code Analysis

(1) Summary of the impact (indicative maximum 100 words)

Single-Sign-On and Mobile Payment systems are prominent realizations of the Multi-Party Distributed Authentication/Authorization framework. CUHK researchers have developed new techniques and automated software to enable Scalable Security Testing and Code Analysis of these systems. The research directly led to the discovery of multiple never-seen-before, high-impact security vulnerabilities/attacks. Through timely sharing of our findings/remedies with the vendors, we successfully eliminated critical security/privacy risks for billions of stake-holders — end-users, online/brick-and-mortar stores, 3rd-party service providers and leading platforms including Provider1, Provider2, Provider3, Provider4 and Provider5. Our work has also become a reference for a major-priority action-item in the upcoming OASIS Open Data standards.

(2) Underpinning research (indicative maximum 500 words)

Recently, many online-service providers like Provider1, Provider2 and Provider4 have evolved to their respective all-in-one platforms, offering services ranging from online social networking, entertainment, real-time communications, e-commerce to mobile payment. Each platform strives to establish its own ecosystem to encompass millions of outside merchants/developers to provide 3rd-party mobile applications, web-based services and brick-and-mortar Point-of-Sales for billions of end-users. The Multi-Party Distributed Authentication/Authorization (MPDAA) framework has been widely adopted as the foundation to enable secure, user-friendly and “sticky” experience for each platform. Prominent examples of MPDAA services include OAuth2.0-based Single-Sign-On (SSO), aka Social-Login, and their Mobile-Payment-Service-enabling derivatives. Under the OAuth2.0-SSO framework, three parties are involved, namely,

(i) the Identity Service Provider (IdP) e.g. Facebook ;
(ii) the Relying Party (RP) – a 3rd-party web-based service/mobile application provider, e.g. Expedia.com ;
(iii) the End-user who can conveniently use his/her established IdP account to conduct business with the RP without creating a new RP account.

For the case of Mobile Payment services, (i), (ii), (iii) correspond to the Cashier (e.g. Provider5’s service), the 3rd-party Merchant (e.g. Expedia.com), and the Paying Customer, respectively.

Unfortunately, the rapid adoption of SSO and Mobile Payment services has also resulted in the proliferation of insecure SSO-related implementations and the corresponding vulnerabilities. The root causes of the problem include:

1) Inherent technical challenges/intricacies of realizing *foolproof security* for multiple, distributed heterogeneous parties ;
2) Numerous home-brewed, platform-specific extensions/modifications of SSO standards by different platforms ;

3) The large number of 3rd-party developers who lack the technical resources and/or business incentives to implement applications/services which are compatible yet secure across different platforms ;
4) The business concern of alienating 3rd-party merchants/developers if a platform's security-vetting process for 3rd-party apps/services is too conservative.

To tackle these problems, Profs. Wing Cheong Lau, Kehuan Zhang and their students, have developed, over the past 5+ years, a series of new techniques and publicly-available software tools to enable large-scale systematic security testing[1,4,5] and code analysis[2,3,4,6] for discovering critical vulnerabilities on SSO/Mobile Payment systems. Specifically, we have released OAuthTester[1] and MoSSOT[5], two adaptive model-based security testing tools and successfully applied them to automate large-scale blackbox testing/discovery of SSO/Mobile-Payment-related vulnerabilities in real-world web-based services[1] and mobile applications[2,5] respectively. We have also developed S3KVetter[4] to analyze the API design and logical correctness of the implementation code of popular SSO/Mobile Payment Software Development Kits (SDKs). This is achieved through key extensions of dynamic symbolic execution techniques to handle multi-party distributed systems with locked-step interactions. Our security analysis of SSO/Mobile Payment software also detected widespread, inadvertent leakage of critical secret-keys from apps and mobile-payment merchants[5]. We have also discovered and neutralized a threat on the QR-code generation/scanning process at mobile payment Point-of-Sales which allows hijacking of the security-critical token of a top-tier cashier service[3]. In [6], we discovered the BadBluetooth vulnerability/attack when an affected Android-based Bluetooth peripheral was involved in the end-to-end authentication/authorization process during some mobile/pervasive-computing use-cases. To empower cybersecurity practitioners to tackle ongoing SSO/Mobile Payment security challenges, we have open-sourced our suite of security testing/analysis tools (https://github.com/cuhk-mobitec).

(3) References to the research (indicative maximum of 6 references)

*** = CUHK students supervised by Profs. Wing Cheong Lau and/or Kehuan Zhang**

[1] Ronghai Yang*, Guanchen Li*, Wing Cheong Lau, Kehuan Zhang and Pili Hu*, "Model-based Security Testing: An Empirical Study on OAuth 2.0 Implementations," ACM AsiaCCS, Xi'an, China, May 2016. [Acceptance Rate: 73/350 = 20.8%]

[2] Ronghai Yang*, Wing Cheong Lau and Tianyu Liu*, "Signing into One Billion Mobile App Accounts Effortlessly with OAuth2.0, " Black Hat Europe, London, Nov. 2016. (An extended version of this work titled "Breaking and Fixing Mobile App Authentication with OAuth2.0-based Protocols," by Ronghai Yang*, Wing Cheong Lau and Shangcheng Shi*, appeared in the 15th International Conference on Applied Cryptography and Network Security (ACNS), Osaka, Japan, Aug. 2017 [Acceptance Rate: 34/149 = 22.8%])

[3] Xiaolong Bai, Zhe Zhou*, XiaoFeng Wang, Zhou Li, Xianghang Mi, Nan Zhang, Tongxin Li, Shi-Min Hu and Kehuan Zhang, "Picking up My Tab: Understanding and Mitigating Synchronized Token Lifting and Spending in Mobile Payment," The 26th USENIX Security Symposium, Vancouver, Canada, August 2017. [Acceptance Rate: 85/572 = 14.9% ; The 2 lead authors of this paper are ordered alphabetically.] (This work was also presented as a Black Hat briefing under the title: "All your Payment Tokens are Mine: Vulnerabilities of Mobile Payment Systems," by Zhe Zhou* in Black Hat Asia, Singapore, Mar 2018.)

[4] Ronghai Yang*, Wing Cheong Lau, Jiongyi Chen*, Kehuan Zhang, "Vetting Single-Sign-On SDK Implementations via Symbolic Reasoning," The 27th USENIX Security Symposium, Baltimore, Maryland, U.S.A., Aug 2018. [Acceptance Rate: 100/520 = 19.2%].

[5] Shangcheng Shi*, Xianbo Wang*, Wing Cheong Lau, "MoSSOT: An Automated Blackbox Tester for Single Sign-On Vulnerabilities in Mobile Applications," ACM AsiaCCS, Auckland, New Zealand, July 2019. [Acceptance Rate: 58/528 = 11.0%]

[6] Fenghao Xu*, Wenrui Diao*, Zhou Li, Jiongyi Chen*, Kehuan Zhang, "BadBluetooth: Breaking Android Security Mechanisms via Malicious Bluetooth Peripherals," The 26th

Annual Network and Distributed System Security Symposium (NDSS), San Diego, California, USA, Feb 2019. [Acceptance Rate: 89/570 = 15.6%]

(4) Details of the impact (indicative maximum 750 words)

A 2015 Gigya/OnePoll survey found 88% consumers already had experience with Single-Sign-On and 65% respondents often or always used SSO when dealing with 3rd-party web-services/mobile applications. Motivated by SSO's rapid adoption, we built OAuthTester in 2014 to examine the SSO-implementations of 500 popular websites and the API design of 12 top-tier IdPs and found widespread vulnerabilities[1]. We broadened our study in 2016[2,5] to cover 600 top-ranked mobile apps which supported SSO services of several major IdPs. Using MoSSOT[5] together with our static/dynamic code analysis techniques[2], we discovered critical vulnerabilities in 133 of those apps. Particularly, our new Profile-Attack[2] alone exposed 75 popular apps (with total downloads exceeding 2.4 billion) to remote app-account hijacking through which attackers can steal sensitive information including victim's travel itineraries, private messaging archives, financial records, photos and viewing/shopping history. Five days after our responsible-disclosure to the affected IdPs[c,d], Provider3 notified *all* of its 3rd-party application developers about this critical vulnerability together with fixes[c]. Our subsequent re-testing found most of the affected apps had promptly fixed the vulnerability as advised. A *partial* list of the successfully-fixed apps had a total download count exceeding 2.2 billion, which included a top-5 travel-planning app, a video-streaming app with 280 million registered users, and a dating/private-messaging app with 156 million+ downloads. Following our advice, Provider3 updated its Single-Sign-On programming guide *within one day* of our report to explicate the possible misuses which caused the Profile-Attack[c]. Provider3 subsequently granted us the maximum allowable award from its bug-bounty program and placed us on its 2016 Top-10 Whitehat list[c]. Provider2 also modified the SSO documentation for its 3rd-party app developers and inducted us to its Bughunter Hall of Fame[d]. Our work[2] also serves as a reference for a major-priority action-item in the OASIS Open Data Protocol (OData) standards to add specific guidance on implementing OAuth/OpenID for mobile devices[e].

We continued to develop S3KVetter[4] in 2017 to test ten popular SSO/Mobile Payment Software Development Kits (SDKs) which were downloaded 10 million+ times by 3rd-party app developers. We found 7 classes of critical vulnerabilities and informed the affected platform-providers/vendors who subsequently fixed their SDKs. For this work, we received the 2018 Facebook/USENIX Internet Defense Prize (3rd place). Quoting the Award Committee[a]:

> *"This work takes a critical look at the implementation of single sign-on code. Single sign-on provides a partial solution to the internet's over-reliance on passwords. This code is widely used, and ensuring its safety has direct implications for user safety online."*

We also leveraged the App-Secret-Leak-Detection function of MoSSOT[5] to discover inadvertent yet critical leakage of 10,000+ valid merchant payment secret-keys from 170,000 Android APKs and 20,000 public GitHub repositories. Using these leaked secret-keys, attackers can access mobile-payment-transaction details and authorize illicit payment transfer/refund to arbitrary users. Some of the affected merchants/apps included the official online-tax-payment app/service of a province with a population over 80 million, the medical-bill-payment app/service for a major hospital, and an online-social-networking app with 8.6 million paying customers. In Aug 2019, we informed the cashiers involved and received prompt confirmations and acknowledgements[b,f]. The affected merchants were immediately notified for corrective actions.

Our discovery of the new class of "Synchronized Token Lifting and Spending" attack in [3] affected popular Point-of-Sale mobile payment systems including a QR-code-based service by

Provider5. Six days after receiving our report, Provider5 announced[g] the termination and replacement of the vulnerable service.

By exploiting design flaws in the Bluetooth profile management scheme under Android, our BadBluetooth work in [6] enabled a new attack to circumvent end-to-end authentication/authorization by breaking the Android security mechanism with malicious Bluetooth peripherals. Upon our responsible-disclosure, the Android Security team rated the problem as "High Severity" and has been developing fixes for billion+ vulnerable mobile devices[h].

The technical-depth and quality of the aforementioned research have been demonstrated via publications/presentations in premier academic and industrial conferences including USENIX Security Symposium, NDSS, AsiaCCS, ACNS and Black Hat. Our work also received broad media coverage, e.g. by Forbes, International Business Times, Phoenix TV[i], raising public awareness on the security/privacy pitfalls of the related applications/services. Above all, our discoveries have directly resulted in the elimination of security vulnerabilities with far-reaching, critical impact. To quote Company1[b]:

> *"Had these vulnerabilities and security issues not been discovered and fixed, they would have affected the overall integrity of the authentication and authorization process of many large-scale online social platforms like ours, which collectively, are serving billions of monthly active users. ... CUHK security team have made the online ecosystem a safer place for billions of netizens world-wide."*

(5) Sources to corroborate the impact (indicative maximum of 10 references)

[a] "Facebook Awards $200,000 to 2018 Internet Defense Prize Winners", retrieved on 9-9-2019 from https://research.fb.com/facebook-awards-200000-to-2018-internet-defense-prize-winners/
[b] Support letter from the Senior Director of a major cyber-security department of Company1.

To corroborate the widespread and immediate actions taken by the industry and media coverage:

[c] Response, acknowledgement and action from Provider3 for the SSO Profile-Attack discoveries.
[d] Response, acknowledgement and action from Provider2 for the SSO Profile-Attack discoveries.
[e] OASIS Open Data Protocol (OData) Standards Issue Tracking Page, retrieved on 9-9-2019 from: https://issues.oasis-open.org/browse/ODATA-1011
[f] Response, acknowledgement and action from Provider4 on the Merchant/App Mobile Payment Key leakage discoveries.
[g] Response, acknowledgement and action for the "Synchronized Token Lifting and Spending" vulnerability on the QR-code-based service from Provider5.
[h] Response, acknowledgement and action from the vendor for the BadBluetooth vulnerability on Android devices.
[i] Sample coverages of our research by international, mainland and local media.