Abstract

Wallet may be described as container application used for configuring, accessing and analysing data from underlying payment application(s). There are two dominant types of digital wallet applications, proximity wallet and remote wallet. In the payment industry, one often hears about authentication approach for proximity or remote wallets or the underlying payment applications separately, but there is no such approach, as per our knowledge, for combined wallet, the holder application. While Secure Element (SE) controlled by the mobile network operator (i.e., SIM card) may ensure strong authentication, it introduces strong dependencies among business partners in payments and hence is not getting fraction. Embedded SE in the form of trusted execution environment [3, 4, 5] or trusted computing [24] may address this issue in future. But such devices tend to be a bit expensive and are not abundant in the market. Meanwhile, for many years, context based authentication involving device fingerprinting and other contextual information for conditional multi-factor authentication, would prevail and would remain as the most dominant and strong authentication mechanism for mobile devices from various vendors in different capability and price ranges. EMVCo payment token standard published in 2014 tries to address security of wallet based payment in a general way. The authors believe that it is quite likely that EMVCo payment token implementations would evolve in course of time in such a way that token service providers would start insisting on device fingerprinting as strong means of
authentication before issuing one-time-use payment token. This paper talks about challenges of existing authentication mechanisms used in payment and wallet applications, and their evolution.

References

- Joshua Rubin, ZVELCO, 8th February, 2012, company blog: https://zvelo.com/blog/entry/google-wallet-security-pin-exposure-vulnerability
- GlobalPlatform Device Technology Secure Element Access Control, Version 1.0 Public Release, May 2012
- GlobalPlatform Device Technology, TEE System Architecture, Version 1.0, Public Release, December 2011, Document Reference: GPD_SPE_009
- TEE from FIME and Trustonic. FIME, advanced secure-chip testing provider, and Trustonic – formed by ARM, Gemalto and Giesecke & Devrient (G&D) as per communication released on 11 February, 2013. http://www.trustonic.com/news/release/trustonic-is-first-to-qualify-a-globalplatform-compliant-tee/en
- Using Trusted Execution Environments in Two-factor Authentication: comparing approaches, Roland van Rijswijk-Deij and Erik Poll, Radboud University Nijmegen, The Netherlands
- White paper: An Overview of Samsung KNOX, April, 2013, Enterprise Mobility Solutions, Samsung Electronics Co., Ltd
- Secure Authentication for Mobile Internet Services, Critical Considerations, December, 2011, v1, SIM Alliance
- ARM Security Technology, Building a Secure System using TrustZone Technology, ARM, April, 2009
- IBM X-Force 2012 Trend and Risk Report, March 2013
- Trustwave 2013 Global Security Report
- Vasudevan, E. Owusu, Z. Zhou, J. Newsome, and J. M. McCune. Trustworthy Execution on Mobile Devices: What security properties can my mobile platform give me? In Trust and Trustworthy Computing, vol. 7344 of LNCS, pp 159–178. Springer, 2012.
- Amal Saha, Sugata Sanyal, Analysis of Applicability of ISO 9564 PIN based Authentication to Closed-Loop Mobile Payment Systems, International Journal of Advanced Networking Applications, Volume 6, Issue 2, 2014
- EMVCo Payment Tokenisation Specification and HCE and its focus on authentication - http://www.emvco.com/specifications.aspx?id=263
- Apple Pay Contactless Secure Payment and Tokenisation - https://www.apple.com/iphone-6/apple-pay/
- Fraud Protection for Native Mobile Applications, ThreatMetrix TrustDefender Mobile, http://www.threatmetrix.com/wp-content/uploads/2014/11/TrustDefender-Mobile-Technical-Brief.pdf
- Host Card Emulation (HCE) Whitepaper by Smartcard Alliance - http://www.smartcardalliance.org/wp-content/uploads/HCE-101-WP-FINAL-081114-clean.pdf
- Future of Secure Mobile Payments by Amal Saha, CISO Platform Annual Summit, 2013 -http://www.slideshare.net/cisoplatform7/future-of-secure-mobile-payments-amal-saha,
Survey of Strong Authentication Approaches for Mobile Proximity and Remote Wallet Applications - Challenges and Evolution

- Google Host Card Emulation — https://developer.android.com/guide/topics/connectivity/nfc/hce.html
- Device Fingerprinting in mobile payment use case - IBM Trusteer http://www.trusteer.com/products/trusteer-pinpoint-criminal-detection
- Ayu Tiwari, Sudipta Sanyal, Ajith Abraham, S. J. Knapskog and Sugata Sanyal, (2011). A multi-factor security protocol for wireless payment-secure web authentication using mobile devices. ArXiv preprint arXiv: 1111.3010.
- Hristo Bojinov et al. "Mobile Device Identification via Sensor Fingerprinting." &quot;arXiv preprint arXiv: 1408.1416 (2014).
- Michael Rausch, Nathan Good, and Chris Jay Hoofnagle. "Searching for Indicators of Device Fingerprinting in the JavaScript Code of Popular Websites." &quot;Proceedings, Midwest Instruction and Computing Symposium, 2014.
- M Rausch, A Bakke, S Patt, B Wegner and D Scott. Demonstrating a Simple Device Fingerprinting System, Proceedings, Midwest Instruction and Computing Symposium, 2014.
- Trusted Computing Group (TCG), http://www.trustedcomputinggroup.org and http://www.trusted-computinggroup.org/solutions/mobile_security
- Secure Element and smart card form factors as per GlobalPlatform, http://globalplatform.org/me-diaguideSE.asp
- Google Wallet - https://www.google.com/wallet/, http://en.wikipedia.org/wiki/Google_Wallet
- EMV Contactless Specification - http://www.emvco.com/specifications.aspx?id=21
- Trusted Service Manager (TSM), http://www.gsma.com/digitalcommerce/wp-content/uploads/2013/12/GSMA-TSM-White-Paper-FINAL-DEC-2013.pdf
- Intel Trusted Execution Environment - http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/malware-reduction-general-technology.html
- Animesh Kr Trivedi, Rishi Kapoor, Rajan Arora, Sudip Sanyal and Sugata Sanyal, RISM - Reputation Based Intrusion Detection System for Mobile Ad hoc Networks, Third International Conference on Computers and Devices for Communications, CODEC-06, pp. 234-237. Institute of Radio Physics and Electronics, University of Calcutta, December 18-20, 2006, Kolkata, India
- A K Trivedi, R Arora, R Kapoor, S Sanyal, S Sanyal. A Semi-distributed Reputation Based Intrusion Detection System for Mobile Adhoc Networks, arXiv preprint arXiv: 1006.1956

Index Terms

Computer Science
Security
Keywords

Proximity Wallet  Remote Wallet  Multi-factor Authentication  Trusted Computing
Trusted Execution Environment

Device Fingerprinting

Context Based Authentication.