R210 Essay: Banking Security

Chongyang Shi (*cs940*)

February 7, 2018

1 Summaries of research

Several years into the rollout of EMV card payments, the landmark research by Murdoch et al. [1] demonstrated authentication flaws in the design and implementations of EMV via a man-in-the-middle attack. Based on detailed analysis of the EMV protocol, the attack took advantage of inappropriate compartmentalisation of cardholder verification information between the card issuer and the payment terminal, which cannot be mitigated through existing and planned security enhancements in EMV, such as dynamic or combined data authentication. The authors also highlighted the negative impacts of the incentive for liability shift towards customers, as well as complications from the secrecy of the protocol design process. Offering a potential explanation for some existing fraud liability disputes, the authors suggested protocol improvements and a strategic rethink in future protocol design processes.

After vulnerabilities of EMV came to light through Murdoch et al. [1], Bond et al. [2] discovered a new class of *pre-play* attacks against EMV ATMs. Motivated by a customer's fraud dispute which cannot be explained through known attacks, the authors investigated the feasibility of exploiting flawed unpredictable number implementations to allow monitored transactions to be replayed at a predetermined future time. After collecting field data through a specially-designed card and studying used ATMs, they were able to both confirm the attack's feasibility and expand the attack to exploit a protocol flaw that cannot be fixed by patching vulnerable implementations. Responses and concerns from the industry were also addressed. It appears that the authors wished to achieve more than inspecting the hardware when purchasing used ATMs, but may have encountered difficulties in reverse-engineering to recover more software-level details.

Murdoch and Anderson [3] summarised vulnerabilities observed in the EMV protocol and its implementations, including those used in the aforementioned attacks, and proposed five principles of protocol design to preserve robust evidence, in light of imbalances in handling current EMV fraud disputes. These principles ensure the availability of evidence and the rigorousness of processes and procedures involved. Alternative payment systems to EMV and possible improvements to EMV were analysed based on these principles. The authors concluded with discussions on open questions in EMV security research. Many of the proposed EMV improvements will incur greater cost to the card issuers due to large scale card reissuance and additional keeping of logs required. Without a liability shift back towards the banks, they may not be sufficiently incentivised to do so.

2 Key themes of research

2.1 Fraud prevention measures tend to move rather than eliminate frauds

Murdoch et al. [1, p. 433] noted that the likely explanation for the overall rising level of fraud since EMV's introduction is that EMV merely moved fraud rather than eliminating it. This was seconded by Bond et al. [2, Sec. II] with the observation that crooks had adapted to performing frauds involving card-not-present payments and magnetic-strip clones instead. The misaligned incentive in the liability shift was in play, and the secretive process of designing EMV protocol failed to create robust security. The lack of merchant authentication in the EMV clearing process also opened up another attack surface to criminals no longer able to impersonate the cardholder, as observed by Murdoch and Anderson [3, p. 3].

2.2 Poor documentation and closed designs damage security

In addition to having been designed behind closed doors, another fallacy of the EMV protocol is the complex and poorly-structured documentations produced, as noted by Murdoch et al. [1, p. 439] when analysing the vulnerability. The same difficulties were noted by Bond et al. [2, Sec. VI], which had likely prevented the discovery of a flaw during a prior formal review of the protocol. This issue is not limited to the EMV protocol, as it was observed by Murdoch and Anderson [3, p. 4] in documentations of a wide range of security protocols.

2.3 Retaining evidence in a payment dispute can be mutually beneficial

While it is often in the financial interest of the bank to keep transaction evidence private in a dispute [1, Sec. VII] [2, VIII. A.], all authors have suggested that it may be mutually beneficial for the bank to retain and disclose transaction evidence during disputes. Because not retaining the evidence can result in the bank not being able to prove the correct PIN was used in a transaction [1, p. 441], or to prove the unpredictable number was properly generated in the event of a pre-play fraud dispute. A significant proportion of Murdoch and Anderson's work [3, Sec. 3] were dedicated to emphasising the value of reliable evidence.

3 Ideas in current context

While the man-in-the-middle attack performed on EMV cards by Murdoch et al. [1, p. 442] did not rely on magnetic-strip fallback information on the cards, it is arguably still a downgrade attack masquerading to the EMV card that a cardholder signature verification has taken place, which is less secure than PIN-based authentication. If the EMV card would only permit PIN-verified transactions, it would not have returned an ARQC at all under this attack, as no PIN was sent to the card. Downgrade attacks taking advantage of compatibilities with less secure protocols have been widely deployed both before and after this work, including negotiation attacks against EAP [4], and POODLE [5] and DROWN [6] attacks against TLS with SSLv2/v3 fallbacks.

In analysing deeper flaws within the EMV protocol, Bond et al. [2, Sec. VI] noted that malware-infected ATMs could be used to facilitate pre-play attacks. As observed by authors, aging hardware and operating systems are often present on ATMs. A significant proportion of ATMs in the market at the time ran Windows XP Embedded, the support of which was phased out in 2016, despite an extension beyond the demise of its consumer variant [7]. Slow replacement of unpatched ATMs raised severe security concerns. Additionally, the authors' concern of deliberately weakened RNG was echoed by the eventually revealed NSA Dual_EC_DRBG backdoor [8].

Based on their principles for payment mechanisms, Murdoch and Anderson predicted that "Bitcoin may be more fragile than most of its users realise" [3, p. 11]. Due to aspects of exchange mechanisms being concentrated on individual commercial organisations, the lack of procedures and governance were considered a factor behind the collapse of a major exchange (Mt.Gox [9]) happened close to the publication of research. During the recent fiat exchange price surge of Bitcoin, the corresponding surge of transaction fees to impractical levels also demonstrated the fragileness of the cryptocurrency [10].

4 Literature review

Following the work of Murdoch et al. [1], Barisani et al. [11] demonstrated another variant of EMV downgrade attack. Through a combination of skimming and CVM downgrading modification, it was effective against newer CDA cards which permit offline authentications. A generic interface for demonstrating and protecting EMV cards from these attacks was built by Choudary [12]. More recently, Degabriele et al. [13] published a theoretical attack against RSA-based EMV cards by inspecting error information during decryptions, which can be effective against countermeasures suggested by Murdoch et al.

With the introduction of contactless payments, Roland and Langer [14] developed a pre-play attack against contactless payment systems with inspiration from Bond et al. [2], with lesser demands on practical precision but also limited maximum damage. Chothia et al. [12] developed a protocol to protect contactless transactions against relay attacks, but it is ineffective if the same unpredictable number flaw as observed by Bond et al. exist in terminal devices involved. Emms et al. [15] developed another attack against contactless cards, the platform of which can be used for more efficient data collection in the attack by Bond et al.

Observations of EMV vulnerabilities by Murdoch and Anderson [3] were cited by Miller [16] in support of a new ecosystem doing away with chip-based payment authentications. Principles of payment mechanisms proposed by Murdoch and Anderson were also considered in the work by Lou et al. [17] to develop an EMV-compatible protocol for more secure and trackable offline transactions.

(1241 words according to texcount.)

References

[1] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond, "Chip and pin is broken," in *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 2010, pp. 433–446.

[2] M. Bond, O. Choudary, S. J. Murdoch, S. Skorobogatov, and R. Anderson, "Chip and skim: cloning emv cards with the pre-play attack," in *Security and Privacy (SP), 2014 IEEE Symposium on*. IEEE, 2014, pp. 49–64.

[3] S. J. Murdoch and R. Anderson, "Security protocols and evidence: Where many payment systems fail," in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 21–32.

[4] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (eap)," Tech. Rep., 2004.

[5] B. Möller, T. Duong, and K. Kotowicz, "This poodle bites: exploiting the ssl 3.0 fallback," *Security Advisory*, 2014.

[6] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J. A. Halderman, V. Dukhovni *et al.*, "Drown: Breaking tls using sslv2." in *USENIX Security Symposium*, 2016, pp. 689–706.

[7] J. Leyden, "Is atm security threatened by windows xp support cutoff?" 2015 December. [Online]. Available: https://www.theregister.co.uk/2015/12/08/xp_embedded_atm_security_cutoff_panic/

[8] S. Checkoway, R. Niederhagen, A. Everspaugh, M. Green, T. Lange, T. Ristenpart, D. J. Bernstein, J. Maskiewicz, H. Shacham, M. Fredrikson *et al.*, "On the practical exploitability of dual ec in tls implementations." in *USENIX security symposium*, 2014, pp. 319–335.

[9] T. Hals, "Mt. gox files u.s. bankruptcy, opponents call it a ruse," March 2014. [Online]. Available: https://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy/mt-gox-files-u-s-bankruptcy-opponents-call-it-a-ruse-idUSBREA290WU20140310

[10] L. Bershidsky, "Bitcoin's high transaction fees show its limits," November 2017. [Online]. Available: https://www.bloomberg.com/view/articles/2017-11-14/bitcoin-s-high-transaction-fees-show-its-limits

[11] A. Barisani, D. Bianco, A. Laurie, and Z. Franken, "Chip & pin is definitely broken," in *Presentation at CanSecWest Applied Security Conference, Vancouver*, 2011.

[12] O. S. Choudary, "The smart card detective: a hand-held emv interceptor," University of Cambridge, Computer Laboratory, Tech. Rep., 2012.

[13] J. P. Degabriele, A. Lehmann, K. G. Paterson, N. P. Smart, and M. Strefler, "On the joint security of encryption and signature in emv," in *Cryptographers' Track at the RSA Conference*. Springer, 2012, pp. 116–135.

[14] M. Roland and J. Langer, "Cloning credit cards: A combined pre-play and downgrade attack on emv contactless." in *WOOT*, 2013.

[15] M. Emms, B. Arief, L. Freitas, J. Hannon, and A. van Moorsel, "Harvesting high value foreign currency transactions from emv contactless credit cards without the pin," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 716–726.

[16] A. Miller, "Defending debit: A historical study of the indirect effects of the durbin amendment on investment in debit card security," in *Workshop on the Economics of Information Security*, 2014, pp. 2–28.

[17] J.-N. Lou, M.-H. Yang, and Y.-C. Ho, "Emv-based mobile payment protocol for offline transaction-with the ability of mutual authentication," *International Journal of Science and Engineering*, vol. 5, no. 1, pp. 61–66, 2015.