R210 Essay: Banking Security

Chongyang Shi (*cs940*)

February 7, 2018

1 Summaries of research

Several years into the roll out of EMV card payments, the landmark research by Murdoch et al. [1] demonstrated authentication flaws in the design and implementations of EMV through 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, and 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 of liability shift towards customers, as well as the secrecy and complexity of the protocol design process. Offering a potential explanation for some existing fraud liability disputes, the authors recommended fixes for the flaws along with strategic rethink in future protocol design processes.

With vulnerabilities of EMV came to light after Murdoch et al. [1], Bond et al. [2] discovered a new class of *pre-play* attacks against EMV ATMs. Motivated by a customer's case without clear explanation through known attacks, the authors investigated the feasibility of exploiting flawed unpredictable number implementations to allow monitored transactions to be replayed at predetermined future times. After collecting field data through a specially-designed card, as well as 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 hardware inspections in purchasing used ATMs, but may have encountered difficulties in reverse-engineering to recover more software 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 to address the 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 a discussion of 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. Without a liability shift back towards the banks, they may not be 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 overall rising levels of fraud since EMV's introduction is the fact that EMV merely moved fraud rather than eliminating it. This was confirmed by Bond et al. [2, Sec. II] in the observation that crooks adapted to perform frauds involving card-not-present payments and magnetic-strip clones instead. The misaligned incentive of liability shift was in play, and the secretive design process of the 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 designing behind closed doors, another fallacy in developing the EMV protocol was the complex and poorly-structured documentations produced, as noted by Murdoch et al. [1, p. 439] in analysing the vulnerability. The same difficulty was 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 problem is not limited to the EMV protocol, as observed by Murdoch and Anderson [3, p. 4] in a wide range of secure protocols.

2.3 Retaining evidence in a payment dispute can be mutually beneficial

While it is often in the financial interest of the banks 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 in 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 case of a pre-play fraud dispute. A significant proportion of Murdoch and Anderson's work [3, Sec. 3] was dedicated to emphasising the value of reliable evidence.

3 Ideas in current context

4 Literature review

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.