More EMV!

Tom Chothia

1

Introduction

- This lecture is more on EMV.
- Advanced attacks against EMV, inc Apple Pay
- A proposed solution to distance bounding for EMV
- Mores more, bigger formal models!

2

2018 IEEE Symposium on Security and Privacy

Distance-Bounding Protocols: Verification without Time and Location

Sjouke Mauw
CSC/SnT
University of Luxembourg
Belval, Luxembourg
sjouke.mauw@uni.lu

Zach Smith
CSC
University of Luxembourg
Belval, Luxembourg
zach.smith@uni.lu

Jorge Toro-Pozo
CSC
University of Luxembourg
Belval, Luxembourg
jorge.toro@uni.lu

Rolando Trujillo-Rasua
SnT
University of Luxembourg
Belval, Luxembourg
rolando.trujillo@uni.lu

***Abstract*—Distance-bounding protocols are cryptographic protocols that securely establish an upper bound on the physical distance between the participants. Existing symbolic verification frameworks for distance-bounding protocols consider timestamps and the location of agents. In this work we introduce a causality-based characterization of secure distance-bounding that discards the notions of time and location. This allows us to verify the correctness of distance-bounding protocols with standard protocol verification tools. That is to say, we provide the first fully automated verification framework for distance-bounding protocols. By using our framework, we confirmed known vulnerabilities in a number of protocols and discovered unreported attacks against two recently published protocols.**

***Keywords*-distance-bounding; security protocols; causality; formal verification; automatic verification**

I. Introduction

Contactless systems are gaining more and more popularity

protocol, if the prover-to-verifier distance is d and the RTT is Δt, then it must hold that $d \leq \frac{1}{2}\Delta t \cdot c$, where c denotes the maximum network transmission speed (for radio-waves, this is the speed of light). This intuition is supported by the physical fact that no message can be transmitted at a speed higher than c.

In the context of distance-bounding protocols, their security has traditionally been verified over the years, by accounting for their resistance to three types of attack: mafia fraud [1], distance fraud [6], and terrorist fraud [6]. Resistance is measured in terms of probability of success of the adversary in a given adversary model [7]–[9]. However, this probabilistic analysis based on attack-resistance does not seem to be a promising verification scheme, as new attacks might be discovered in the future.

A clear and convincing proof of the flaws of the attack-based security analysis is the work by Cremers et al. [10].

3

A different way to model distance bounding security.

- Start(V,Nr)
- Action (P,Nc,Nr)
- End (V,Nc,Nr)
- Claim(P,V,Nc,Nr)

```
lemma DB_Security: "All P V AC chal resp #l .
DB_Check_Sucessful( P, V, chal, resp )@l ==>
  ( ( Ex #i #j #k. DB_Start_Fast_Phase(V,chal)@i
      & DB_Action(P, chal, resp)@j
      & DB_End_Fast_Phase(V, chal, resp)@k & i < j & j < k )"
```

4

First Contact: New vulnerabilities in Contactless Payments

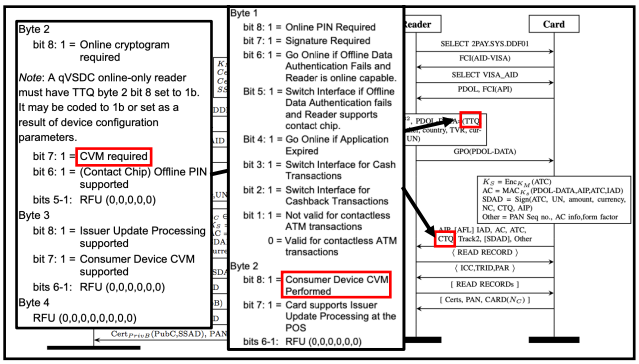
Leigh-Anne Galloway

Tim Yunusov

September 5, 2019

Document Version 1.0

5



6

The EMV Standard: Break, Fix, Verify

David Basin, Ralf Sasse, and Jorge Toro-Pozo
Department of Computer Science
ETH Zurich, Switzerland

***Abstract*—EMV is the international protocol standard for smartcard payment and is used in over 9 billion cards worldwide. Despite the standard's advertised security, various issues have been previously uncovered, deriving from logical flaws that are hard to spot in EMV's lengthy and complex specification, running over 2,000 pages.**

We formalize a comprehensive symbolic model of EMV in Tamarin, a state-of-the-art protocol verifier. Our model is the first that supports a fine-grained analysis of all relevant security guarantees that EMV is intended to offer. We use our model to automatically identify flaws that lead to two critical attacks: one that defrauds the cardholder and a second that defrauds the merchant. First, criminals can use a victim's Visa contactless card to make payments for amounts that require cardholder verification, without knowledge of the card's PIN. We built a proof-of-concept Android application and successfully demonstrated this attack on real-world payment terminals. Second, criminals can trick the terminal into accepting an unauthentic offline transaction, which the issuing bank should later decline, after the criminal

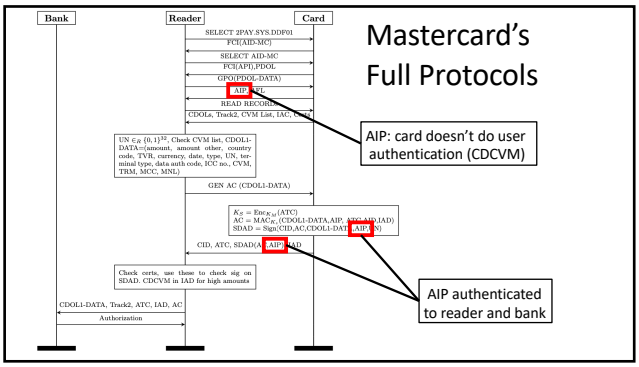
ca. 600,000 Euros [11]. The underlying flaw of Murdoch *et al.*'s attack is that the card's response to the terminal's offline PIN verification request is not authenticated.

Some of the security issues identified result from flawed implementations of the standard. Others stem from logical flaws whose repairs would require changes to the entire EMV infrastructure. Identifying such flaws is far from trivial due to the complexity of EMV's execution flow, which is highly flexible in terms of card authentication modes, cardholder verification methods, and online/offline authorizations. This raises the question of how we can systematically explore all possible executions and improve the standard to avoid another twenty years of attacks.

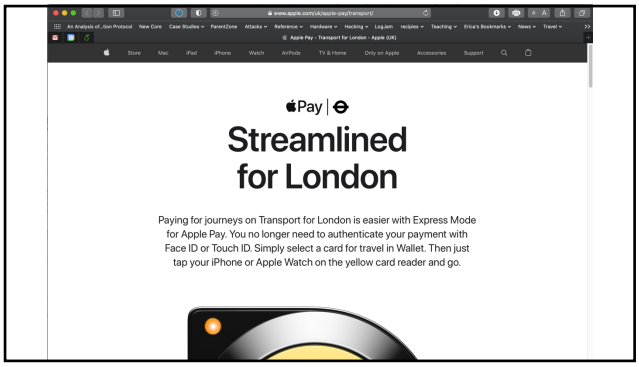
Approach Taken: Break, Fix, Verify

In this paper we focus on weakness of and improvements to

7



8



9

Practical EMV Relay Protection

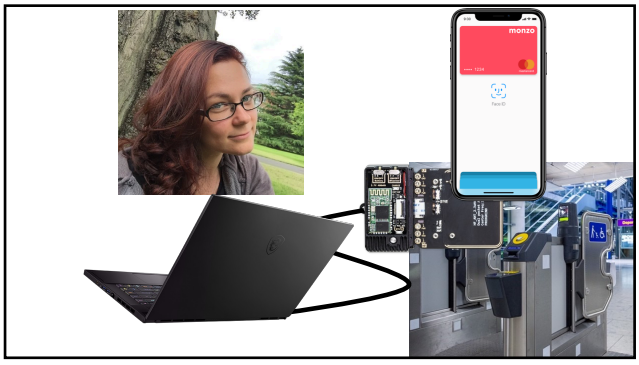
Andreea-Ina Radu*, Tom Chothia*, Christopher J.P. Newton†, Ioana Boureanu† and Liqun Chen†
*University of Birmingham, UK †University of Surrey, UK

***Abstract*—Relay attackers can forward messages between a contactless EMV bank card and a shop reader, making it possible to wirelessly pickpocket money. To protect against this, Apple Pay requires a user's fingerprint or Face ID to authorise payments, while Mastercard and Visa have proposed protocols to stop such relay attacks. We investigate transport payment modes and find that we can build on relaying to bypass the Apple Pay lock screen, and illicitly pay from a locked iPhone to any EMV reader, for any amount, without user authorisation. We show that Visa's proposed relay-countermeasure can be bypassed using rooted smart phones. We analyse Mastercard's relay protection, and show that its timing bounds could be more reliably imposed at the ISO 14443 protocol level, rather than at the EMV protocol level. With these insights, we propose a new relay-resistance protocol (L1RP) for EMV. We use the Tamarin prover to model**

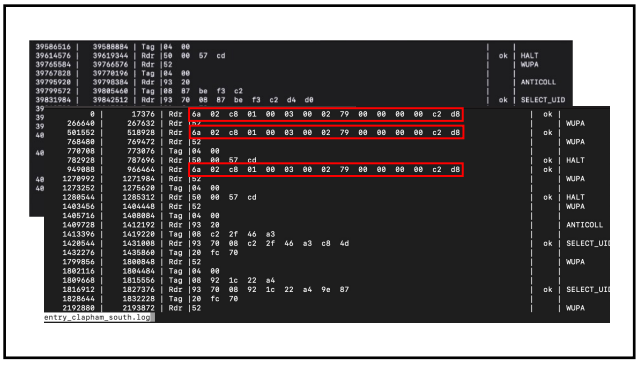
from a *locked* iPhone to any EMV shop reader (with non-transit merchant codes), for any amount; we tested up to £1000. For Mastercard, we found that relays from locked phones were only possible to readers with a transit merchant code. We formally model these protocols and verify the results, using the Tamarin prover; we extend the state-of-the-art EMV models from [2] to support mobile apps in different modes.

We disclosed this attack to both Apple and Visa, and discussed it with their security teams. Apple suggested that the best solution was for Visa to implement additional fraud detection checks, explicitly checking Issuer Application Data (IAD) and the Merchant Category Code (MCC). Meanwhile, Visa observed that the issue only applied to Apple (i.e., not

10



11

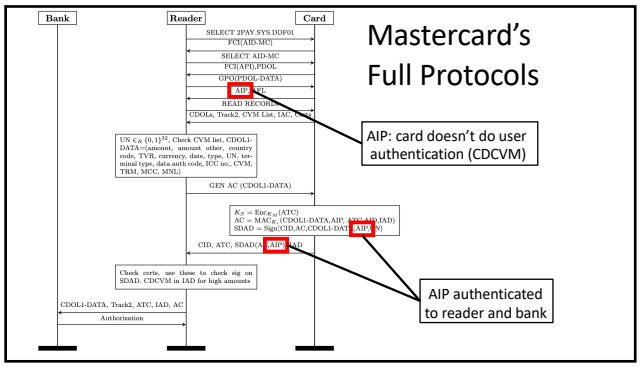


12

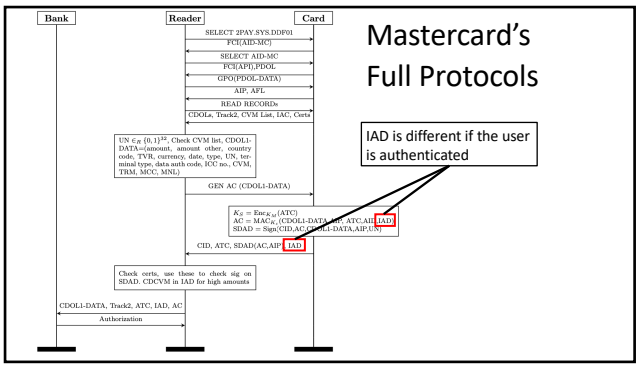
Investigating transport mode

- Apply Pay
  - "Magic Bytes" unlock Apple Pay – but are not enough on their own.
  - Merchant Category Code (MCC) must be a transit operator
  - Reader must be in "online authentication for offline"
- Samsung pay
  - Samsung pay does not use the magic bytes
  - Phone will also start a EMV transaction, even when locked
  - BUT Samsung Pay only allows

13



14



15

Visa-proprietary Specs

Based on VIS 1.6 (for contact transactions) + educated guesses

IAD Format 4? (for mobile payments)

IADs in the wild:

Plastic visa: `07 065C0A03A00000`

Apple Pay (auth): `20 1F4A5732A0000000010030273000000004000000000000000000000000000000`

Parsed IADs:

07 is the total length of the data
06 is the length of issuer discretionary data
5C is derivation key index
0A is the cryptogram version
03 Length of CVR
A00000 is the CVR
A0 - 1010 0000
- second GENERATE AC not requested
- ARQC returned in first GENERATE AC

20 is the total length of the data
1F is the length of issuer discretionary data
4A is the cryptogram version -- left nibble 0100 (4) should indicate IAD format
57 is derivation key index
32A0000000 is the CVR here
32 - CVR byte 1 RFU
A0 - 1010 0000
- second GENERATE AC not requested
- ARQC returned in first GENERATE AC
00 left nibble RFU, right nibble Issuer Discretionary Data Option ID
10030273000000040000000000000000000000000000 is issuer discretionary data

16

Visa-proprietary Specs

Based on VIS 1.6 (for contact transactions) + educated guesses

IAD Format 4? (for mobile payments)

IADs in the wild:

Plastic visa: `07 065C0A03A00000`

Apple Pay (auth): `20 1F4A5732A0000000010030273000000004000000000000000000000000000000`

Apple Pay (transport): `20 1F4A5760A0000000010030273000000004000000000000000000000000000000`

Google Pay (auth): `20 1F4346512000000000000000001061800000000000000000000000000000000`

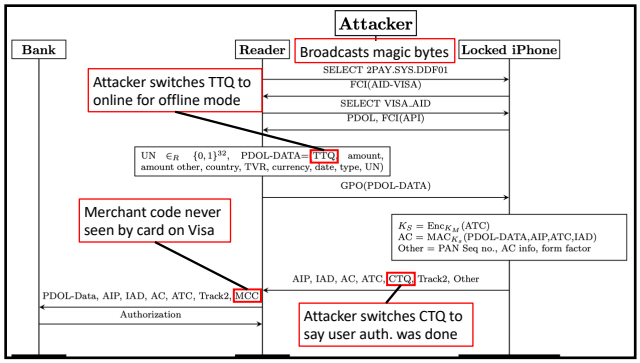
Samsung Pay (transport): `20 1F4363002000000000000000000651500000000000000000000000000000000`

Samsung Pay (auth): `20 1F4346422000000000000000001133600000000000000000000000000000000`

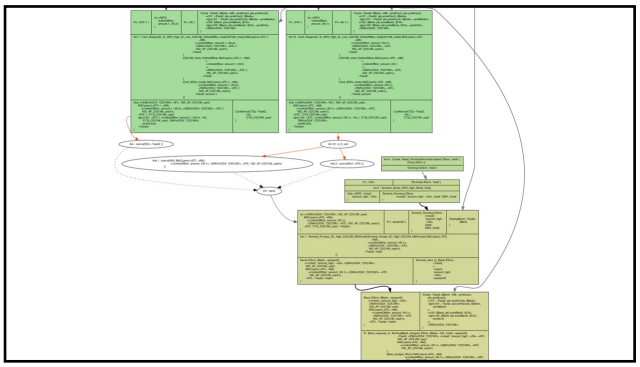
CVR byte 1 RFU

EMV spec – CVR byte 5 marked as RFU (all bits)

17



18



19

Stopping the attack

- Apple can mitigate this by enforcing a payment limit
  - Transit mode should never allow high value transactions
  - A zero limit for transport mode, like Samsung, fixes the problem.
- Visa can also fix it:
  - Visa should check the IAD to stop over the limit attacks
  - Visa could refuse all non-CDCVM iPhone payments to not transit operators.

20

Disclosure to Apple

- Apple: this transactions would never go through.
- Us: They did go through.
- Apple: this transactions would never go through.
- Us: here are the receipts, bank statements and shop account showing the payments where all processed.
- Apple: …. Oh
- Apple: It's all Visa's fault!

21

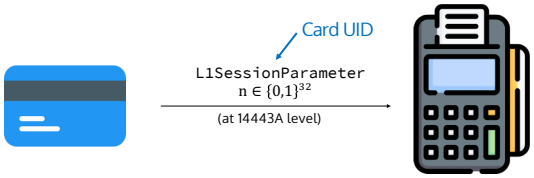
22

Disclosure to Visa

- "impractically close physical proximity to a victim's smart device"
- "the fraudster to be or work with an acquirer-approved collusive merchant to authorize the fraudulent transactions"
- "in the event one were to be processed, the cardholder would not be liable as part of Visa's zero fraud liability policy" ?

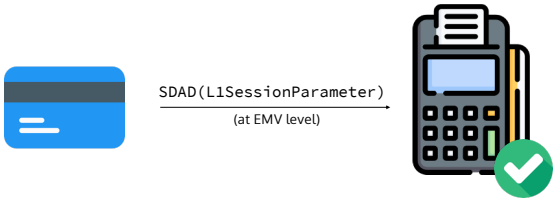
23

Visa's Level 1 Relay Protection



24

Visa's Level 1 Relay Protection



25

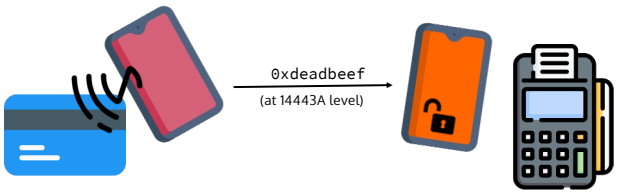
Visa Relay Protection Attack

26

Visa Relay Protection Attack

27

Visa Relay Protection Attack



28

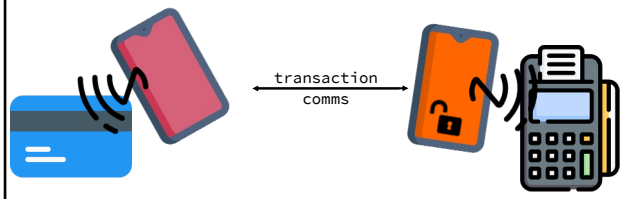
Visa Relay Protection Attack

29

Visa Relay Protection Attack

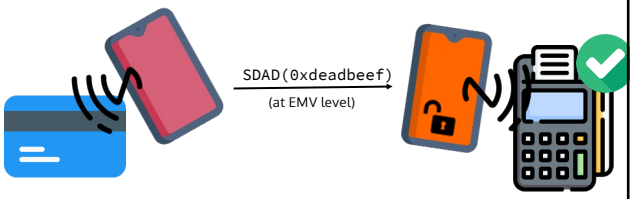
30

Visa Relay Protection Attack



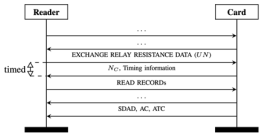
31

Visa Relay Protection Attack



32

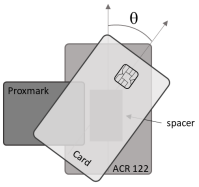
Mastercard Relay Resistant Protocol

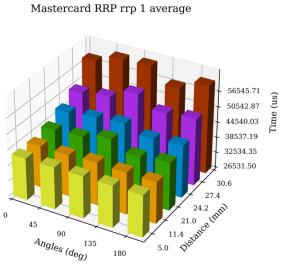


VS

33

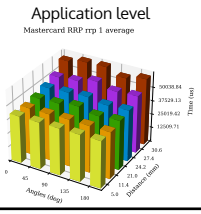
Mastercard Relay Resistant Protocol

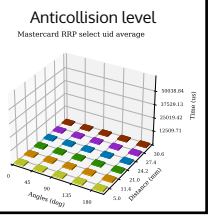




34

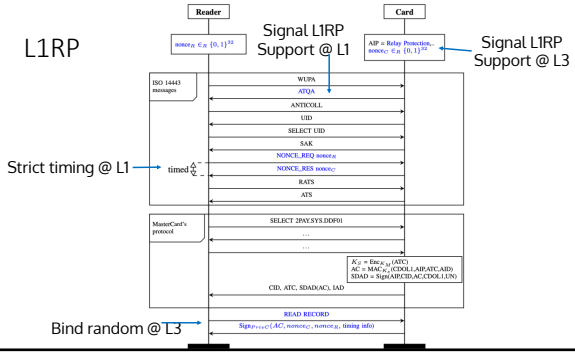
How do we solve all this?





35

L1RP



36

We have formally modelled:

- Verified L1RP
- New models for Visa and Mastercard mobile p
- Verified Apple Pay Visa attack
- Verified Visa Relay Protection attack

Powered by Tamarin

37

ISO standardization

- We are going through the process of getting this added to the level 1 ISO 14443 standard for smart cards.
- The special interest working group have approved it. EMV Co. and NXP supportive.
- Next discussed at the British Standards Institute.
- Then discussed at ISO meeting.
- Then ISO will create a working group to consider the idea …

38

Conclusion

- Feature creep can turn neat, secure systems into a hot mess.
- Formal modelling can cope with the complexities of large, complex systems.
- In this case we found that
  - Apple Pay lock screen can be bypassed for any iPhone with a Visa in transit mode.
  - The contactless limit can also be bypassed allowing unlimited EMV contactless transactions from a locked iPhone.
- Formal modelling works for complex systems.

39

Take away message:

- If you are analysing the security of a system consider building a model of it in ProVerif or Tamarin.
  - Might automatically find a vulnerability
  - The process of building a model really helps you understand the system
- If you are proposing a new secure design, make a model to go in your paper.
  - Helps make the design more precise
  - Increase the confidence of the reviewers
  - Might avoid you submitting a paper with a vulnerability in the design.

40