Breaking Credit Cards with Tamarin

Xenia Hofmeier

based on Slides by Jorge Toro
Institute of Information Security
ETH Zurich

Tamarin Prover Tutorial, Summerschool on real-world crypto and privacy, v.1
June 4, 2024

EMV standard

- EMV (or "Chip & PIN") is the protocol standard for **smartcard payment**
- Founded by **E**uropay, **M**astercard, and **V**isa, other payment networks joined too
- **12+ billion** EMV cards in circulation worldwide
- EMV was advertised to offer the highest **security**

EMV security

Primary goal: protect cardholders

Low-value purchases do not require a PIN

High-value purchases **should** be protected by PIN

Some images from https://pngtree.com/so/

EMV security

Primary goal: protect cardholders

Low-value purchases do not require a PIN

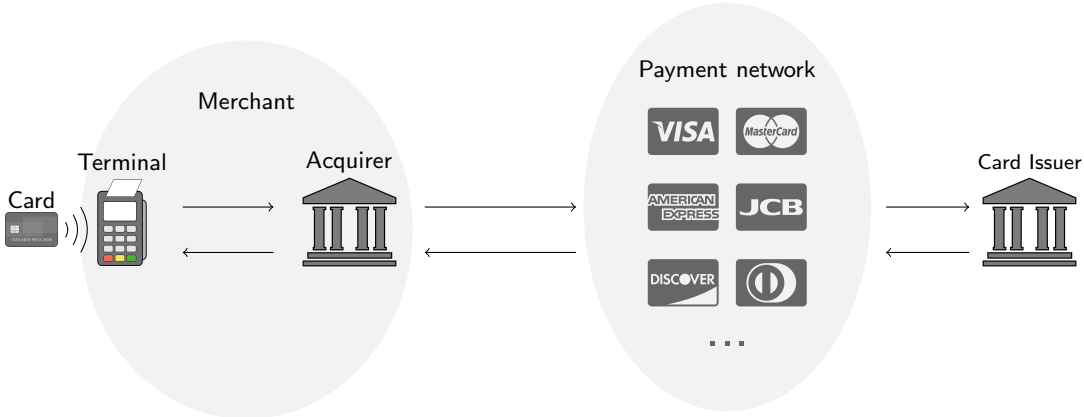
High-value purchases **should** be protected by PIN

We'll show that they are **not**

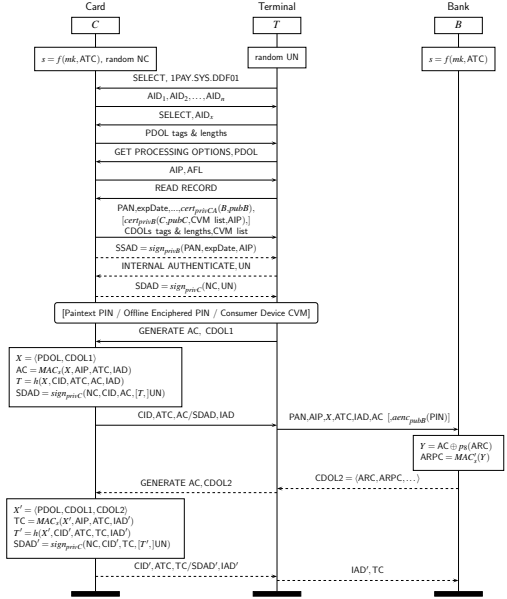
Images from: https://pngtree.com/so/extend-a-finger
https://pngtree.com/so/emoji-icons

Some images from `https://pngtree.com/so/`

Involved parties

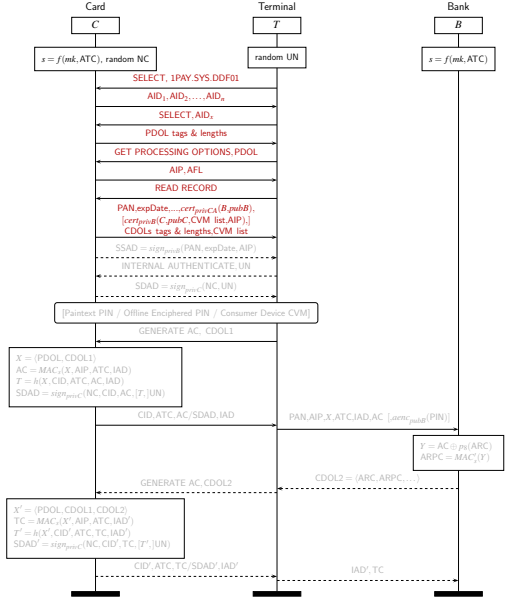


EMV protocol



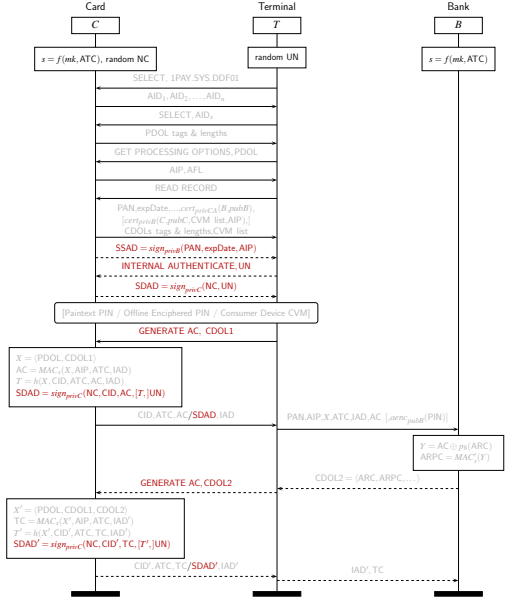
EMV protocol

1. **Initialization**: card and terminal agree on application to use and exchange card and transaction data



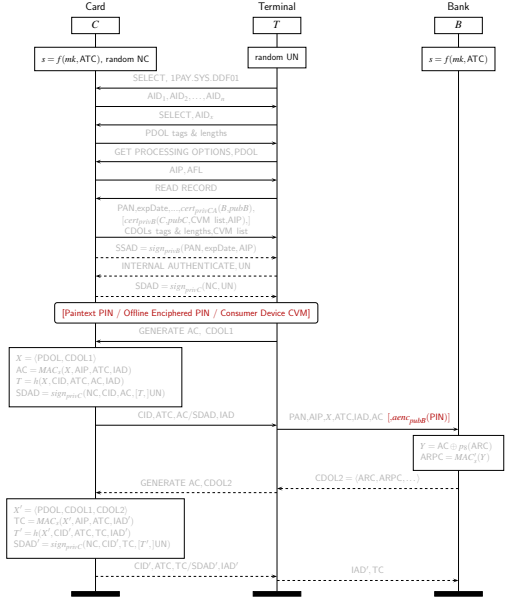
EMV protocol

1. **Initialization**: card and terminal agree on application to use and exchange card and transaction data
2. **Card Authenticates to the Terminal**: terminal performs a PKI-based validation of the card. Multiple methods exist.



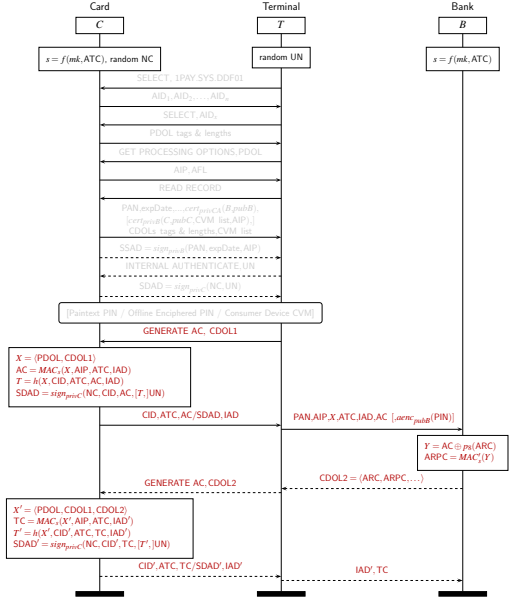
EMV protocol

1. **Initialization**: card and terminal agree on application to use and exchange card and transaction data
2. **Card Authenticates to the Terminal**: terminal performs a PKI-based validation of the card. Multiple methods exist.
3. **Cardholder Verification**: terminal checks that person presenting the card is the legitimate cardholder. Four (digital) methods:
   - Signature
   - No CVM
   - Plaintext PIN
   - Offline Enciphered PIN
   - Online PIN
   - Consumer Device CVM



EMV protocol

1. **Initialization**: card and terminal agree on application to use and exchange card and transaction data
2. **Card Authenticates to the Terminal**: terminal performs a PKI-based validation of the card. Multiple methods exist.
3. **Cardholder Verification**: terminal checks that person presenting the card is the legitimate cardholder. Four (digital) methods:
   - Signature
   - No CVM
   - Plaintext PIN
   - Offline Enciphered PIN
   - Online PIN
   - Consumer Device CVM
4. **Card Authenticates to the Bank**: The card generates an MAC for the card. The card and Bank share a symmetric key.



Break, Fix, Verify

- Developed first comprehensive model of EMV (Used Tamarin to analyze 2,000+ pages of paper specification)
- Found both known and new security issues
- Proposed and machine-checked fixes (disclosed to relevant vendors)

Modelling the configurations

- Different Kernels, configurations in one model:
  - Allow for different configurations in parallel
  - Using branching

Analysing Configurations seperately

- Generate one model for each configuration
- The lemmas analyze only one configuration: Configuration models differ in the action facts for the lemmas
- Results in 24 Models for Contact and 17 for contactless
- Analyze each lemma for each configuration model
- We can identify secure and vulnerable configurations

Security of EMV contactless

Target Model	exec.	bank accepts	auth. to terminal	auth. to bank
Visa_EMV_Low	✓	✓	×(1)	×(1)
Visa_EMV_High	✓	✓	×(1)	×(1)
Visa_DDA_Low	✓	×(2)	×(2)	✓
Visa_DDA_High	✓	✓	✓	✓
Mastercard_SDA_OnlinePIN_Low	✓	×(2)	×(2)	✓
Mastercard_SDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_SDA_NoPIN_Low	✓	×(2)	×(2)	✓
Mastercard_SDA_NoPIN_High	–(3)	–	–	–
Mastercard_DDA_OnlinePIN_Low	✓	×(2)	×(2)	✓
Mastercard_DDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_DDA_NoPIN_Low	✓	×(2)	×(2)	✓
Mastercard_DDA_NoPIN_High	–(3)	–	–	–
Mastercard_CDA_OnlinePIN_Low	✓	✓	✓	✓
Mastercard_CDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_CDA_NoPIN_Low	✓	✓	✓	✓
Mastercard_CDA_NoPIN_High	–(3)	–	–	–

Legend:

✓: property verified ×: property falsified –: not applicable

(1): disagrees with card on CVM (2): disagrees with card on AC

(3): high-value transactions without CVM are not completed contactless

bold: satisfies all 4 properties

Security of EMV contactless

Target Model	exec.	bank accepts	auth. to terminal	auth. to bank
Visa_EMV_Low	✓	✓	×(1)	×(1)
Visa_EMV_High	✓	✓	×(1)	×(1)
Visa_DDA_Low	✓	×(2)	×(2)	✓
Visa_DDA_High	✓	✓	✓	✓
Mastercard_SDA_OnlinePIN_Low	✓	×(2)	×(2)	✓
Mastercard_SDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_SDA_NoPIN_Low	✓	×(2)	×(2)	✓
Mastercard_SDA_NoPIN_High	–(3)	–	–	–
Mastercard_DDA_OnlinePIN_Low	✓	×(2)	×(2)	✓
Mastercard_DDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_DDA_NoPIN_Low	✓	×(2)	×(2)	✓
Mastercard_DDA_NoPIN_High	–(3)	–	–	–
Mastercard_CDA_OnlinePIN_Low	✓	✓	✓	✓
Mastercard_CDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_CDA_NoPIN_Low	✓	✓	✓	✓
Mastercard_CDA_NoPIN_High	–(3)	–	–	–

Legend:
✓: property verified ×: property falsified –: not applicable
(1): disagrees with card on CVM (2): disagrees with card on AC
(3): high-value transactions without CVM are not completed contactless
bold: satisfies all 4 properties

- Common Mastercard transactions are **secure**

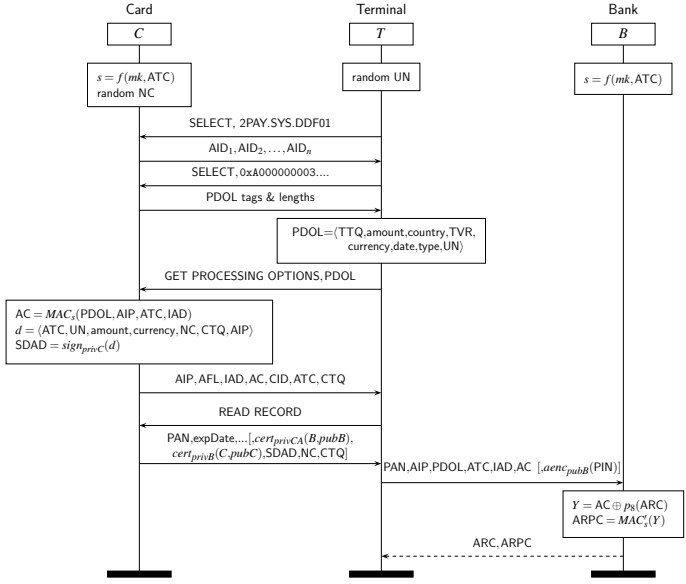
Security of EMV contactless

Target Model	exec.	bank accepts	auth. to terminal	auth. to bank
Visa_EMV_Low	✓	✓	×(1)	×(1)
Visa_EMV_High	✓	✓	×(1)	×(1)
Visa_DDA_Low	✓	×(2)	×(2)	✓
Visa_DDA_High	✓	✓	✓	✓
Mastercard_SDA_OnlinePIN_Low	✓	×(2)	×(2)	✓
Mastercard_SDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_SDA_NoPIN_Low	✓	×(2)	×(2)	✓
Mastercard_SDA_NoPIN_High	–(3)	–	–	–
Mastercard_DDA_OnlinePIN_Low	✓	×(2)	×(2)	✓
Mastercard_DDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_DDA_NoPIN_Low	✓	×(2)	×(2)	✓
Mastercard_DDA_NoPIN_High	–(3)	–	–	–
Mastercard_CDA_OnlinePIN_Low	✓	✓	✓	✓
Mastercard_CDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_CDA_NoPIN_Low	✓	✓	✓	✓
Mastercard_CDA_NoPIN_High	–(3)	–	–	–

Legend:
✓: property verified ×: property falsified –: not applicable
(1): disagrees with card on CVM (2): disagrees with card on AC
(3): high-value transactions without CVM are not completed contactless
bold: satisfies all 4 properties

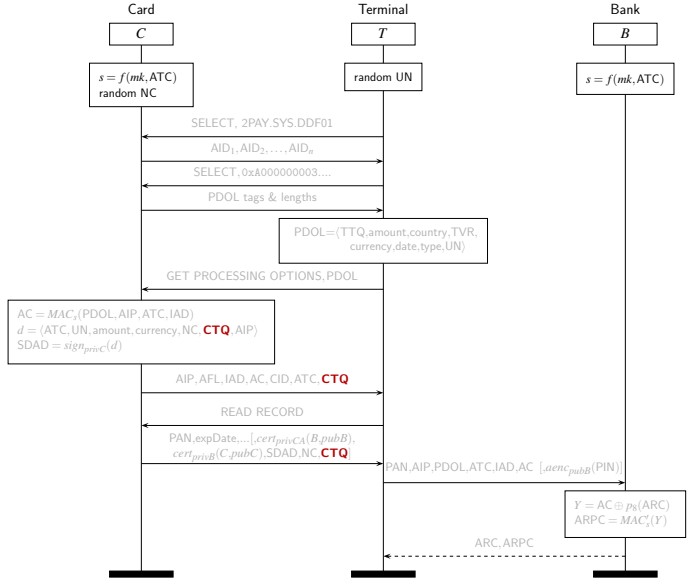
- Common Mastercard transactions are **secure**
- Common Visa transactions are **not secure**

Visa protocol: A look at the problem



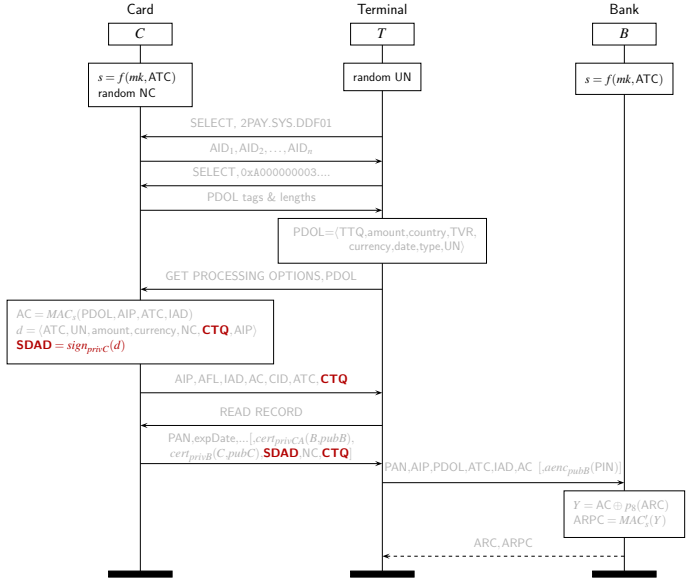
Visa protocol: A look at the problem

- Card's choice for Cardholder Verification Method (**CVM**) is encoded in the Card Transaction Qualifiers (**CTQ**)



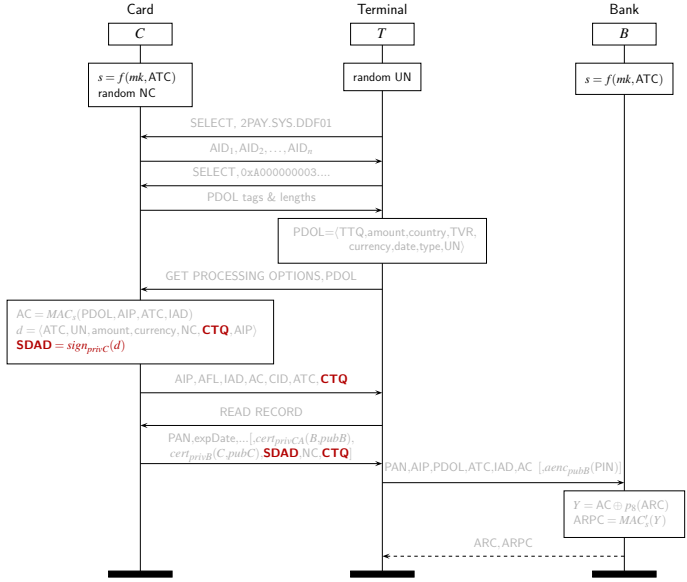
Visa protocol: A look at the problem

- Card's choice for Cardholder Verification Method (**CVM**) is encoded in the Card Transaction Qualifiers (**CTQ**)
- **CTQ** protected only by the Signed Dynamic Authentication Data (**SDAD**)



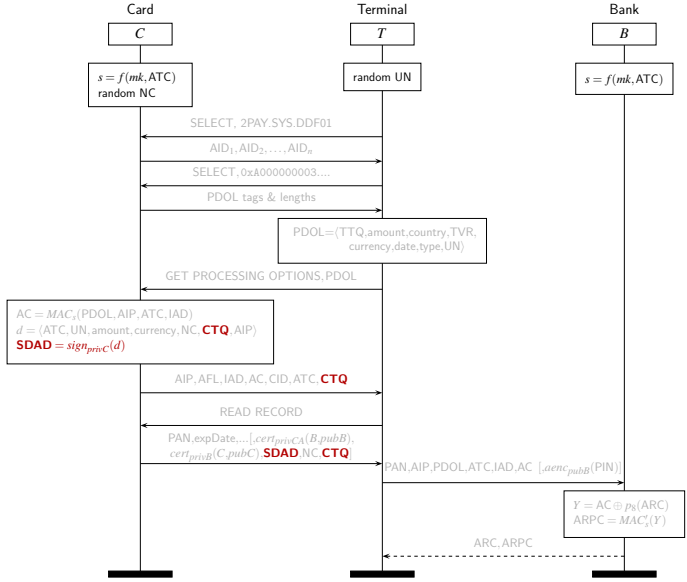
Visa protocol: A look at the problem

- Card's choice for Cardholder Verification Method (**CVM**) is encoded in the Card Transaction Qualifiers (**CTQ**)
- **CTQ** protected only by the Signed Dynamic Authentication Data (**SDAD**)
- Most Visa transactions **don't use** the SDAD



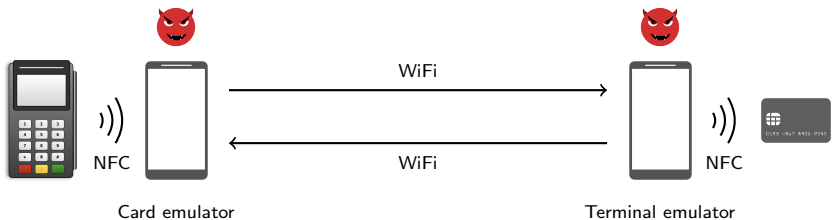
Visa protocol: A look at the problem

- Card's choice for Cardholder Verification Method (**CVM**) is encoded in the Card Transaction Qualifiers (**CTQ**)
- **CTQ** protected only by the Signed Dynamic Authentication Data (**SDAD**)
- Most Visa transactions **don't use** the SDAD
- Thus CTQ and **CVM can be modified**!



Weaponizing: PIN bypass attack

Machine-in-the-middle attack built on top of a **relay attack** architecture:

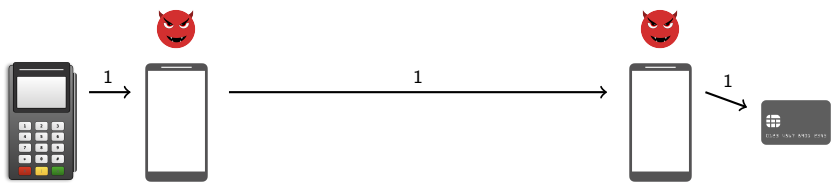


Evil image from `https://pngtree.com/so/`

Weaponizing: PIN bypass attack

Machine-in-the-middle attack built on top of a **relay attack** architecture:

1. Terminal sends command indicating **Cardholder Verification Required**

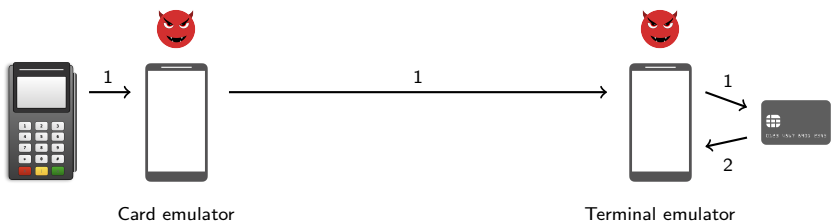


Evil image from `https://pngtree.com/so/`

Weaponizing: PIN bypass attack

Machine-in-the-middle attack built on top of a **relay attack** architecture:

1. Terminal sends command indicating **Cardholder Verification Required**
2. Card responds with CTQ indicating **Online PIN Required**

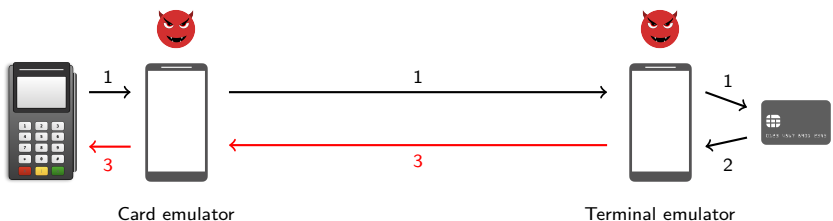


Evil image from https://pngtree.com/so/

Weaponizing: PIN bypass attack

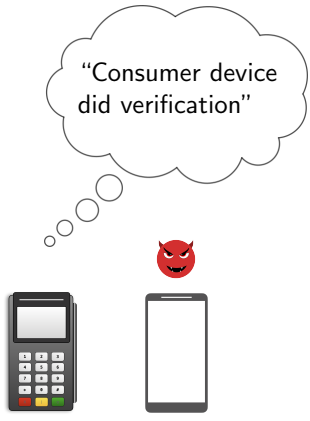
Machine-in-the-middle attack built on top of a **relay attack** architecture:

1. Terminal sends command indicating **Cardholder Verification Required**
2. Card responds with CTQ indicating **Online PIN Required**
3. Attacker modifies CTQ to indicate that
   Online PIN is not Required and **Consumer Device CVM was Performed**



Evil image from https://pngtree.com/so/

Weaponizing: PIN bypass attack



Card emulator

Terminal emulator

Evil image from https://pngtree.com/so/

What about Mastercard?

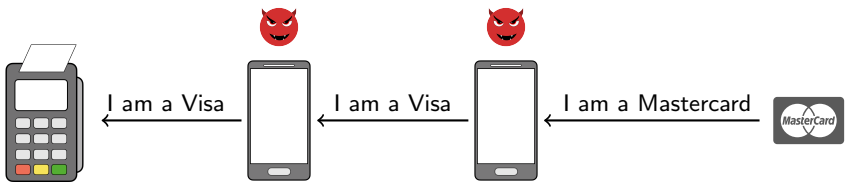
- Before we said that common Mastercard **transactions** are **secure**
- Does this mean that Mastercard **cardholders** are **safe**?

What about Mastercard?

- Before we said that common Mastercard **transactions** are **secure**
- Does this mean that Mastercard **cardholders** are **safe**?
- **NO**: There is another attack!

PIN bypass attack targeting masteracard

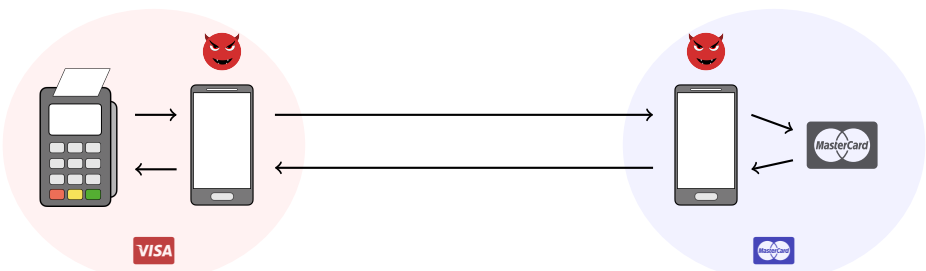
Problem: lack of integrity protection for card data (AIDs) that determines the EMV protocol version (a.k.a. kernel) to use.
Attack idea: replace card's AIDs with the Visa AID to deceive the terminal into activating the Visa kernel.



PIN bypass attack targeting masteracard

Problem: lack of integrity protection for card data (AIDs) that determines the EMV protocol version (a.k.a. kernel) to use.
Attack idea: replace card's AIDs with the Visa AID to deceive the terminal into activating the Visa kernel.

- Simultaneously perform a Visa transaction with the terminal and a Mastercard transaction with the card.
- For Visa transaction, apply previously described attack on Visa!



Security of EMV contactless

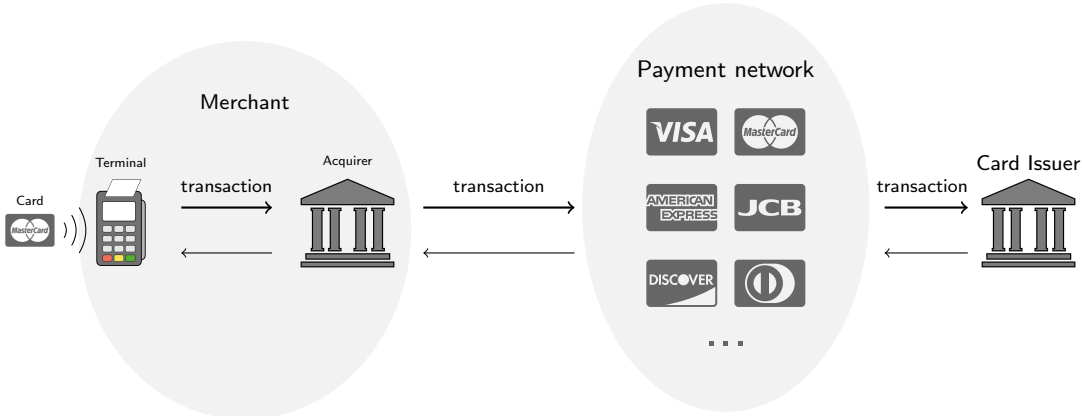
Target Model	exec.	bank accepts	auth. to terminal	auth. to bank
Visa_EMV_Low	✓	✓	×(1)	×(1)
Visa_EMV_High	✓	✓	×(1)	×(1)
Visa_DDA_Low	✓	×(2)	×(2)	✓
Visa_DDA_High	✓	✓	✓	✓
Mastercard_SDA_OnlinePIN_Low	✓	×(2)	×(2)	✓
Mastercard_SDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_SDA_NoPIN_Low	✓	×(2)	×(2)	✓
Mastercard_SDA_NoPIN_High	–(3)	–	–	–
Mastercard_DDA_OnlinePIN_Low	✓	×(2)	×(2)	✓
Mastercard_DDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_DDA_NoPIN_Low	✓	×(2)	×(2)	✓
Mastercard_DDA_NoPIN_High	–(3)	–	–	–
Mastercard_CDA_OnlinePIN_Low	✓	✓	✓	✓
Mastercard_CDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_CDA_NoPIN_Low	✓	✓	✓	✓
Mastercard_CDA_NoPIN_High	–(3)	–	–	–

Legend:
✓: property verified ×: property falsified –: not applicable
(1): disagrees with card on CVM (2): disagrees with card on AC
(3): high-value transactions without CVM are not completed contactless
bold: satisfies all 4 properties

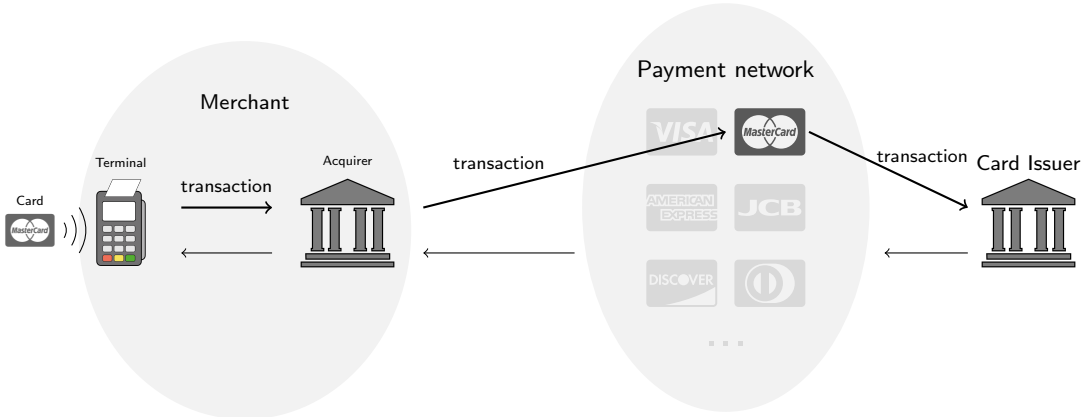
- Common Mastercard transactions are **secure**

Why did we not capture the Card Brand Mixup attack previously?

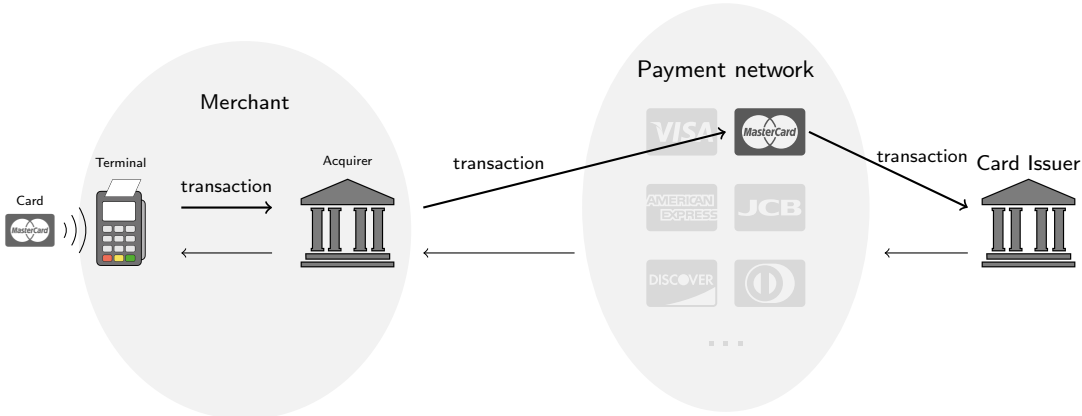
Online authorization and routing



Online authorization and routing

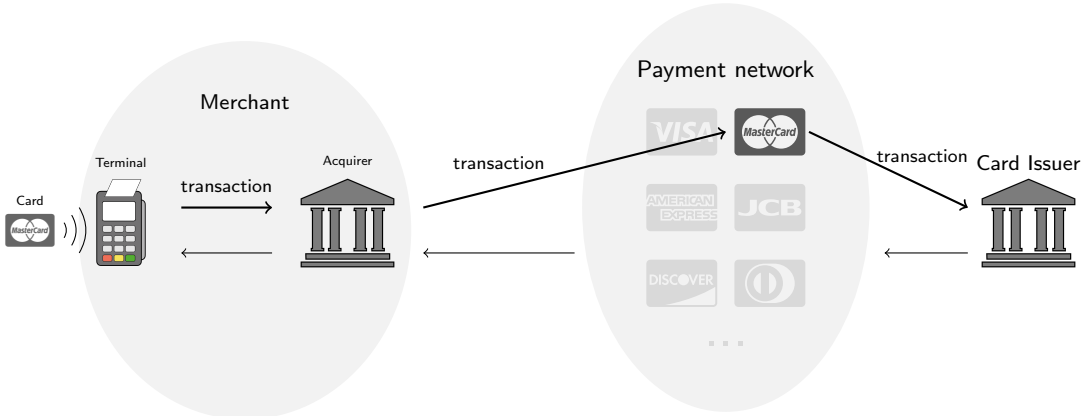


Online authorization and routing



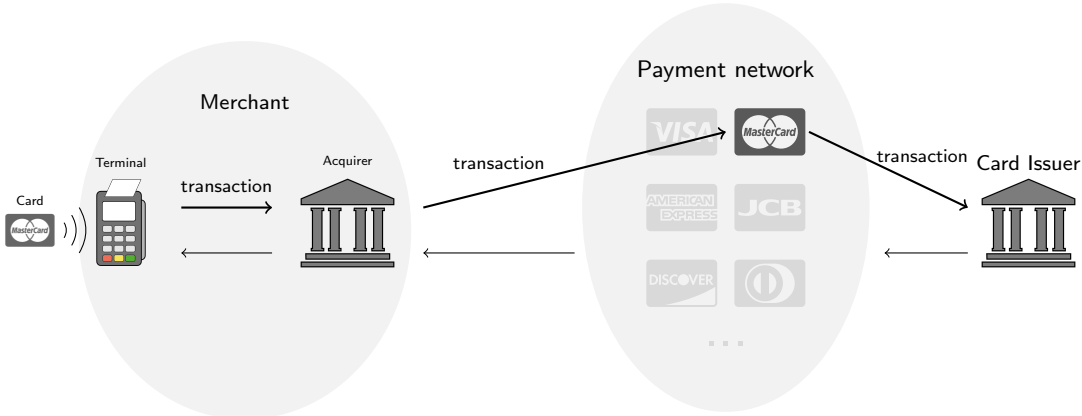
But what card data does the merchant use to determine the payment network?

Online authorization and routing



But what card data does the merchant use to determine the payment network?
The *Application Identifier (*AID*)* or the *Primary Account Number (*PAN*)*?

Online authorization and routing



But what card data does the merchant use to determine the payment network?
The *Application Identifier (*AID*)* or the *Primary Account Number (*PAN*)*?
Previous model: AID, New model: PAN

Good News

Following our disclosure, Mastercard deployed countermeasures at network level!

Mastercard Cards are now secure

Right?...

Mastercard Cards are now secure

Right?...

Well....

Bypassing Cardholder Verification for Mastercard

- Card announces **supported CVMs** in the `CVM List`
- The card authenticates the `CMV List` to the terminal using its signature which is authenticated by the **card's certificate** (signed by the issuer)
- What if this authentication fails?

Certificate verification

- Terminal has a **list of root certificates**
- Root CAs provide certificate for card issuers
- Card issuers provide **certificates stored on cards**
- Card sends signature, certificates, and information on CA to Terminal
- Terminal **looks up the root CA certificate** in its database according to:
  - Registered Application Provider Identifier, which is derived from the Application Identifier (AID)
  - the **CA Public Key Index**

Hidden in the Specifications...

- On Page 255 of the Mastercard kernel, there are some suspicious lines:

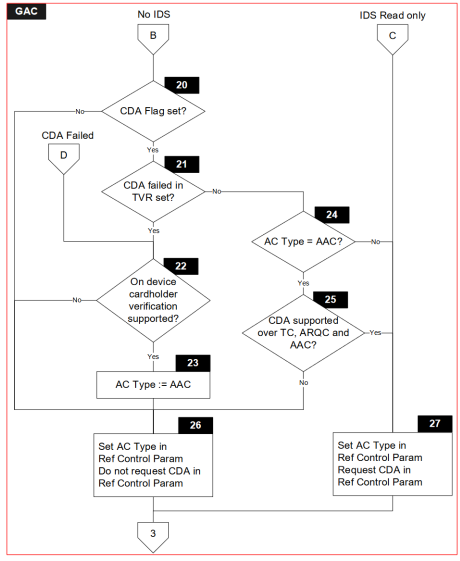
IF [The *CA Public Key Index (Card)* is not present in the CA Public Key Database]
THEN
SET 'CDA failed' in *Terminal Verification Results*
ENDIF

Hidden in the Specifications...

- On Page 255 of the Mastercard kernel, there are some suspicious lines:

IF [The *CA Public Key Index (Card)* is not present in the CA Public Key Database]
THEN
SET 'CDA failed' in *Terminal Verification Results*
ENDIF

- We see the effect on page 435:

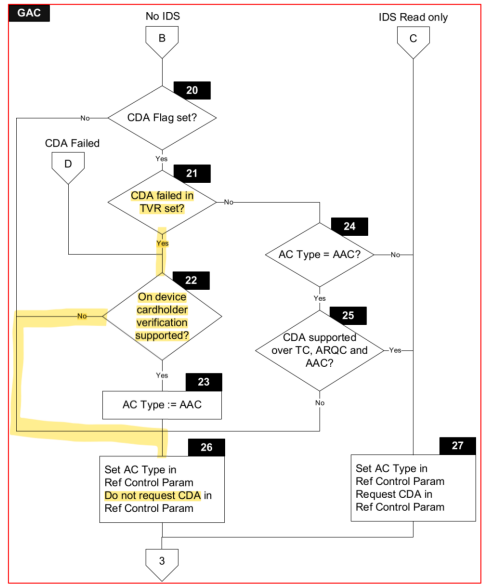


Hidden in the Specifications...

- On Page 255 of the Mastercard kernel, there are some suspicious lines:

IF [The *CA Public Key Index (Card)* is not present in the CA Public Key Database]
THEN
SET 'CDA failed' in *Terminal Verification Results*
ENDIF

- We see the effect on page 435:
- "Do not request CDA" $\Leftrightarrow$ "No signature verificaiton is performed"

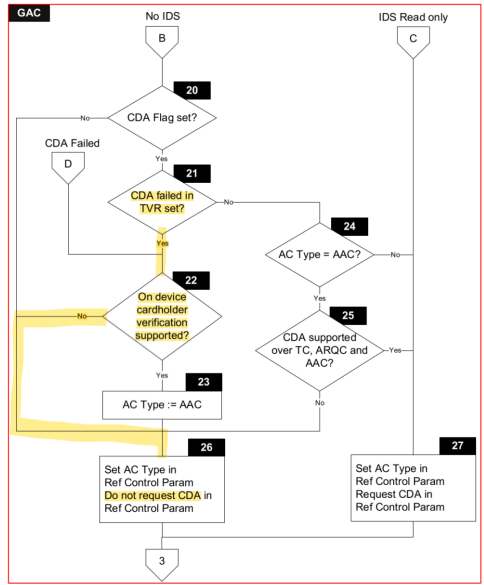


Hidden in the Specifications...

- On Page 255 of the Mastercard kernel, there are some suspicious lines:

IF [The *CA Public Key Index (Card)* is not present in the CA Public Key Database]
THEN
SET 'CDA failed' in *Terminal Verification Results*
ENDIF

- We see the effect on page 435:
- "Do not request CDA" $\Leftrightarrow$ "No signature verificaiton is performed"
- This can happen, because the CA Public Key Index is not cryptographically protected



Inducing Authentication Failure

Providing an **invalid CA Public Key Index** and some additional changes will result in the **terminal accepting** the transaction **without verifying the PIN** although the card would require it.

Role of Tamarin

- Previous models did not capture this attack as they abstracted the terminal's decision tree.
- Tamarin was used to verify proposed counter measures.

Conclusion

- **If you are building critical infrastructure, you have to get it right!**
- **Formal automated verification is a necessity**
  We (humans) cannot cover the full execution space that complex systems have
- **Existing verification tools are up to the task**
  Tamarin, ProVerif, etc... have been used to analyse TLS, 5G AKA, etc...
- **Systems must be verified as a whole and not by parts separately**
  Separate system parts may be secure but composition may be insecure
- **Ambiguity and redundancy should be avoided in system specification**
  Critical mechanisms (e.g. routing) of the system should be unambiguously specified

About this work

- **The EMV Standard: Break, Fix, Verify**, published at the 42nd IEEE Symposium on Security and Privacy (S&P 2021)
- **Card Brand Mixup Attack: Bypassing the PIN in non-Visa cards by Using Them for Visa Transactions**, published at the 30th USENIX Security Symposium (USENIX Security 21)
- **Inducing Authentication Failures to Bypass Credit Card PINs**, published at the 32nd USENIX Security Symposium (USENIX Security 23)
- Webpage: `https://emvrace.github.io`
- Team:


David Basin


Ralf Sasse


Jorge Toro


Patrick Schaller