Card Brand Mixup Attack: Bypassing the PIN in non-Visa cards by Using Them for Visa Transactions

David Basin Ralf Sasse **Jorge Toro**

ETH Zurich

30th USENIX Security Symposium
August 2021

Outline

EMV standard

- EMV is the protocol standard for **smartcard payments**
- Founded by **E**uropay, **M**astercard, and **V**isa,
  and later Amex, JCB, Discover, and UnionPay joined the consortium too
- **9+ billion** EMV cards in circulation worldwide

EMV security

Cardholder protection

Low-value purchases do not require a PIN

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

Credits: https://pngtree.com/so/

EMV security

Cardholder protection

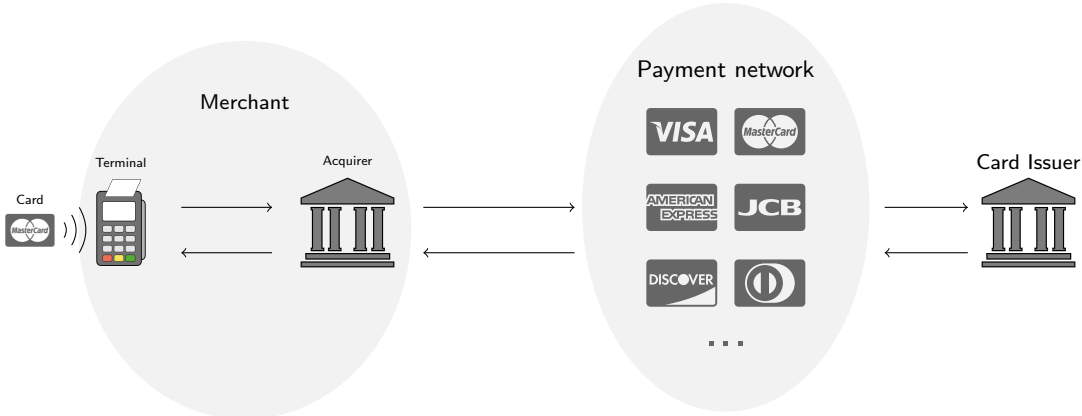
Low-value purchases do not require a PIN

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

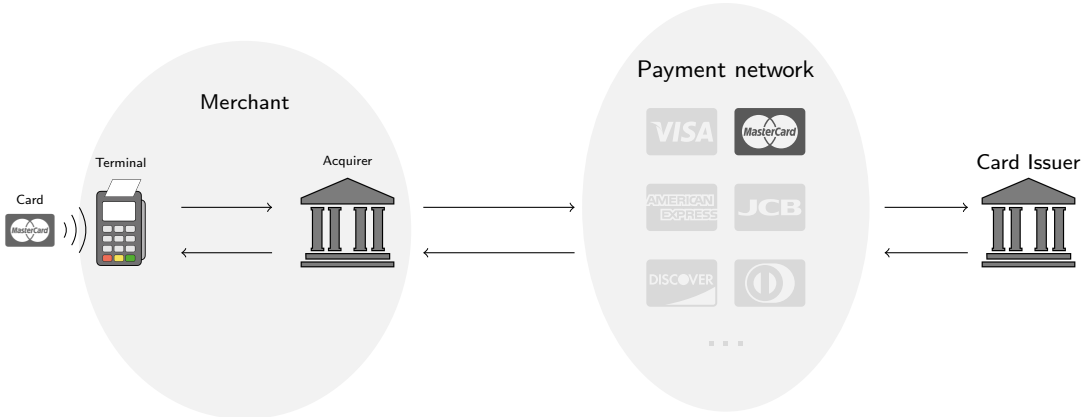
We'll show that they are **not**

Credits: https://pngtree.com/so/

Online authorization and routing

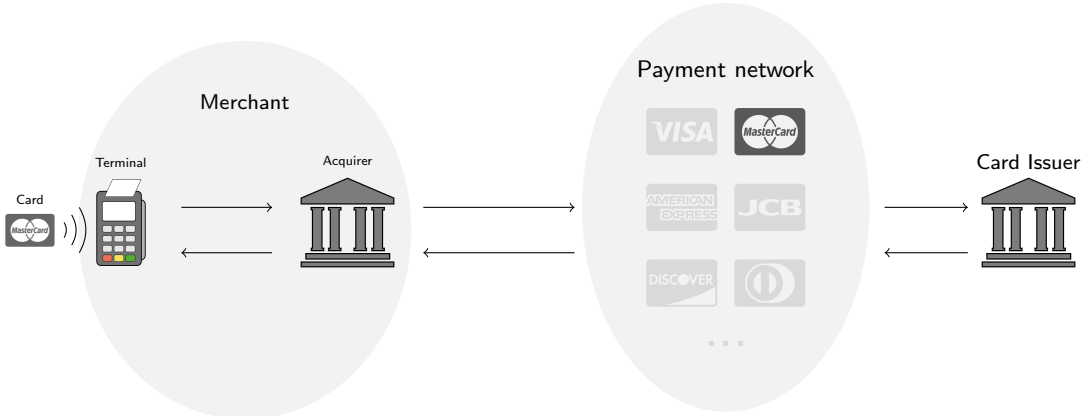


Online authorization and routing



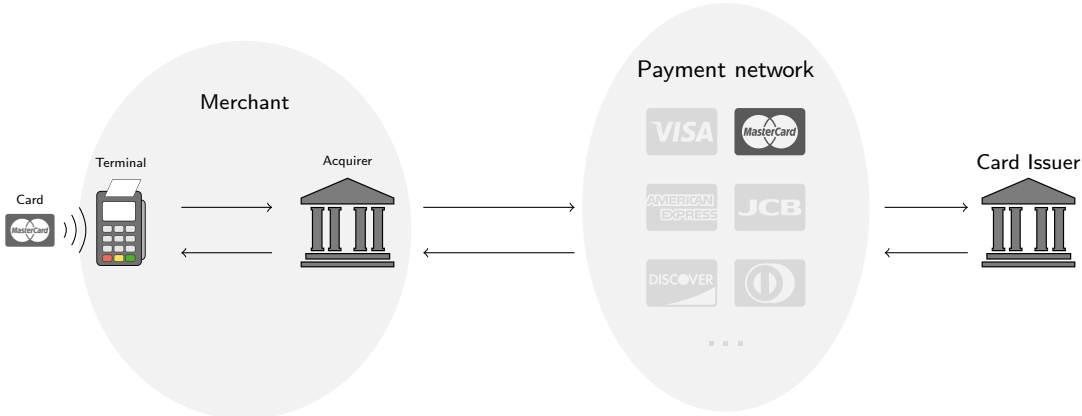
What card data does the merchant use to determine the payment network?

Online authorization and routing



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



What card data does the merchant use to determine the payment network?

The *Application Identifier* (**AID**) or the *Primary Account Number* (**PAN**)?

Why multiple choices? Do they always indicate the same payment network?

Contributions

- **Extended our Tamarin model of EMV to account for different routing choices**
  - Develop an EMV model with PAN-based routing
  - Model permits transactions where merchant and issuer don't agree on the card brand

Contributions

- **Extended our Tamarin model of EMV to account for different routing choices**
  - Develop an EMV model with PAN-based routing
  - Model permits transactions where merchant and issuer don't agree on the card brand
- **Identified the card brand mixup attack**
  - Attacker induces mismatch between the issuer and the merchant's views of the card brand
  - Leads to PIN bypass for non-Visa cards

Contributions

- **Extended our Tamarin model of EMV to account for different routing choices**
  - Develop an EMV model with PAN-based routing
  - Model permits transactions where merchant and issuer don't agree on the card brand
- **Identified the card brand mixup attack**
  - Attacker induces mismatch between the issuer and the merchant's views of the card brand
  - Leads to PIN bypass for non-Visa cards
- **Mechanized the attack and showed it is effective and easy to carry out**
  - Bypassed the PIN for a transaction of over **USD 400** with a Maestro card

Contributions

- **Extended our Tamarin model of EMV to account for different routing choices**
  - Develop an EMV model with PAN-based routing
  - Model permits transactions where merchant and issuer don't agree on the card brand
- **Identified the card brand mixup attack**
  - Attacker induces mismatch between the issuer and the merchant's views of the card brand
  - Leads to PIN bypass for non-Visa cards
- **Mechanized the attack and showed it is effective and easy to carry out**
  - Bypassed the PIN for a transaction of over **USD 400** with a Maestro card
- **Disclosed issues to vendor and proposed verified fixes**
  - Disclosure process led to Mastercard deploy countermeasures at network level

Outline

Analysis results for EMV with AID-based routing

Basin et al. *"The EMV Standard: Break, Fix, Verify."* IEEE S&P 2021

Target Model	exec.	issuer accepts	auth. to terminal	auth. to issuer
Visa_EMV_Low	✓	✓	×	×
Visa_EMV_High	✓	✓	×	×
Visa_DDA_Low	✓	×	×	✓
Visa_DDA_High	✓	✓	✓	✓
Mastercard_SDA_OnlinePIN_Low	✓	×	×	✓
Mastercard_SDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_SDA_NoPIN_Low	✓	×	×	✓
Mastercard_SDA_NoPIN_High	–	–	–	–
Mastercard_DDA_OnlinePIN_Low	✓	×	×	✓
Mastercard_DDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_DDA_NoPIN_Low	✓	×	×	✓
Mastercard_DDA_NoPIN_High	–	–	–	–
Mastercard_CDA_OnlinePIN_Low	✓	✓	✓	✓
Mastercard_CDA_OnlinePIN_High	✓	✓	✓	✓
Mastercard_CDA_NoPIN_Low	✓	✓	✓	✓
Mastercard_CDA_NoPIN_High	–	–	–	–

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

- Issuer **agrees** with terminal on all the data for every transaction with a Mastercard card

Analysis results for EMV with PAN-based routing

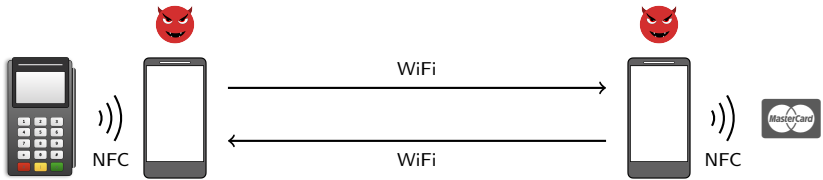
Target Model	exec.	issuer accepts	auth. to terminal	auth. to issuer
Visa_EMV_Low	✓	✓	×	×
Visa_EMV_High	✓	✓	×	×
Visa_DDA_Low	✓	×	×	✓
Visa_DDA_High	✓	✓	✓	✓
Mastercard_SDA_OnlinePIN_Low	✓	×	×	×
Mastercard_SDA_OnlinePIN_High	✓	✓	✓	×
Mastercard_SDA_NoPIN_Low	✓	×	×	×
Mastercard_SDA_NoPIN_High	×	–	–	–
Mastercard_DDA_OnlinePIN_Low	✓	×	×	×
Mastercard_DDA_OnlinePIN_High	✓	✓	✓	×
Mastercard_DDA_NoPIN_Low	✓	×	×	×
Mastercard_DDA_NoPIN_High	×	–	–	–
Mastercard_CDA_OnlinePIN_Low	✓	✓	✓	×
Mastercard_CDA_OnlinePIN_High	✓	✓	✓	×
Mastercard_CDA_NoPIN_Low	✓	✓	✓	×
Mastercard_CDA_NoPIN_High	×	–	–	–

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

- Attacker induces **disagreement** on the card brand: issuer knows the card is a Mastercard but terminal thinks it's a Visa

Weaponizing: PIN bypass attack

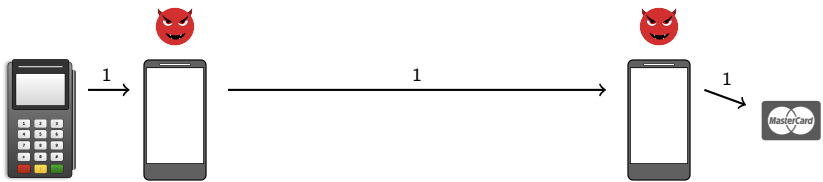
Man-in-the-middle attack built on top of a **relay attack** architecture:



Weaponizing: PIN bypass attack

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

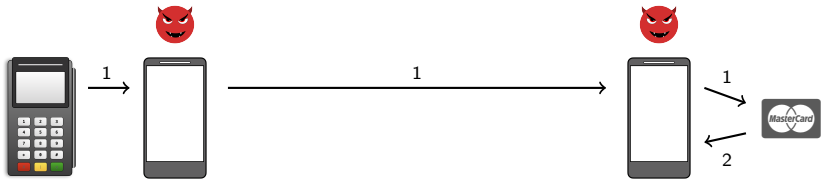
1. Terminal sends SELECT command



Weaponizing: PIN bypass attack

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

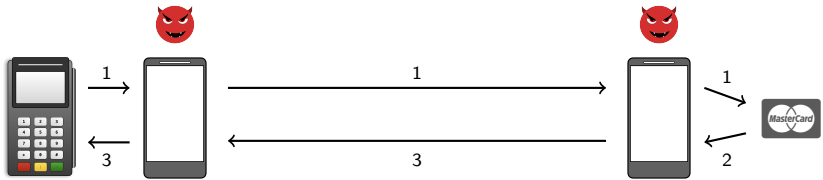
1. Terminal sends SELECT command
2. Card responds with I AM A MASTERCARD



Weaponizing: PIN bypass attack

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

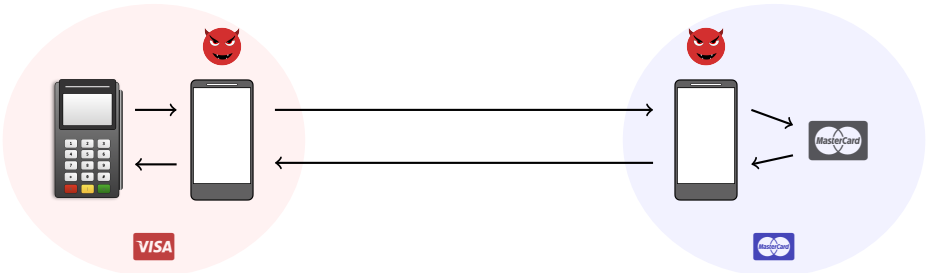
1. Terminal sends SELECT command
2. Card responds with I AM A MASTERCARD
3. Attacker replaces response with I AM A VISA



Weaponizing: PIN bypass attack

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

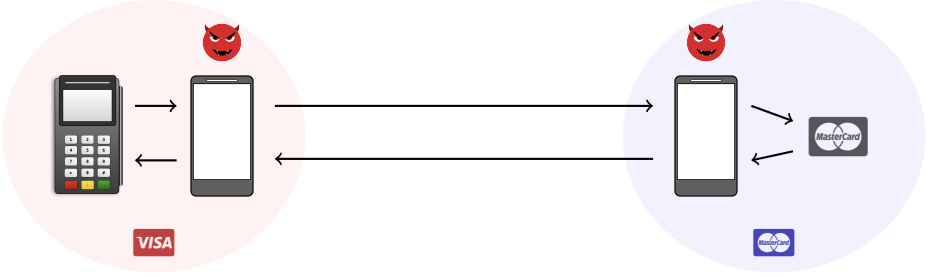
1. Terminal sends SELECT command
2. Card responds with I AM A MASTERCARD
3. Attacker replaces response with I AM A VISA
4. Transaction continues in two simultaneous sessions:
   - Terminal & Attacker running the Visa protocol
   - Attacker & Card running the Mastercard protocol



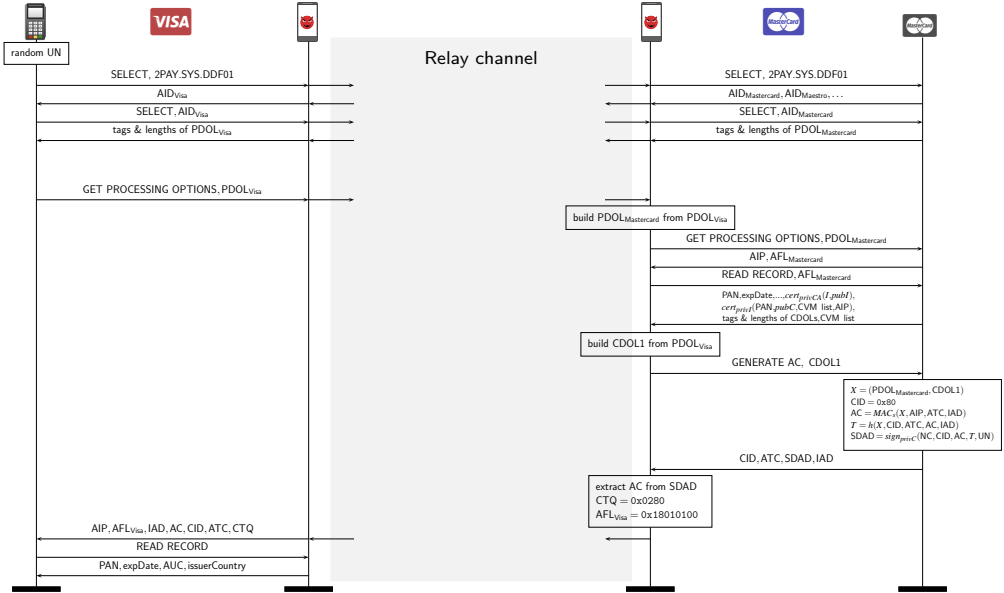
Weaponizing: PIN bypass attack

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

1. Terminal sends SELECT command
2. Card responds with I AM A MASTERCARD
3. Attacker replaces response with I AM A VISA
4. Transaction continues in two simultaneous sessions:
   - Terminal & Attacker running the Visa protocol
   - Attacker & Card running the Mastercard protocol
5. Attacker applies PIN bypass on Visa [see our S&P paper]



The attack in technical detail



Demo

Available at:

- https://youtu.be/8d7UgIiMRBU
- https://emvrace.github.io

Countermeasures

- We verified that our countermeasure[1] to the PIN bypass on Visa **does prevent** our Mastercard-Visa brand mixup

[1] Basin et al. *"The EMV Standard: Break, Fix, Verify."* IEEE S&P 2021

Countermeasures

- We verified that our countermeasure[1] to the PIN bypass on Visa **does prevent** our Mastercard-Visa brand mixup
- We also proposed and machine-checked new **intra-kernel countermeasures**

[1] Basin et al. *"The EMV Standard: Break, Fix, Verify."* IEEE S&P 2021

Countermeasures

- We verified that our countermeasure[1] to the PIN bypass on Visa **does prevent** our Mastercard-Visa brand mixup
- We also proposed and machine-checked new **intra-kernel countermeasures**
- Mastercard implemented their own defenses at **network level**, which we experimentally confirmed as effective against our attack

[1] Basin et al. *"The EMV Standard: Break, Fix, Verify."* IEEE S&P 2021

Outline

Conclusion

- **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
- **Formal automated verification is a necessity**
  We (humans) cannot cover the full execution space that complex systems have

Webpage of this work: `https://emvrace.github.io`