Inducing Authentication Failures to Bypass Credit Card PINs

David Basin

Patrick Schaller

Jorge Toro-Pozo

Institute of Information Security ETH Zurich

32nd Usenix Security Symposium

Anaheim, August 10th, 2023

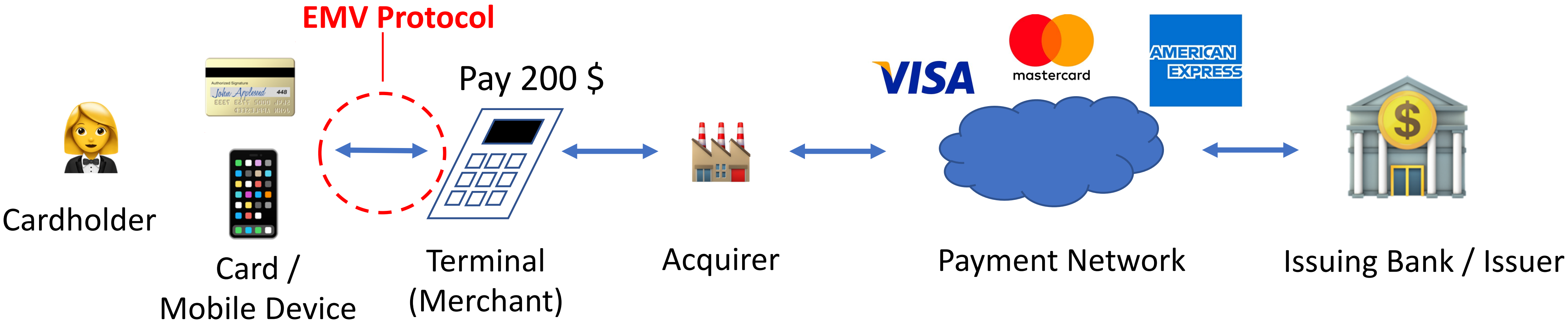
Background

- EMV (Europay, Mastercard, VISA): Standard for smartcard payment
- 9+ billion EMV cards in circulation globally
- Data on Integrated Circuit Chips (ICCs)

- EMV standard describes the communication between cards and terminals (payment terminal, ATM)
- Cards either physically inserted (card reader) or communicate *contactless* using Near Field Communication (NFC)

Ecosystem

- Card Issuer (payment network, bank, or a certified organization)
- Payment processing network (e.g., Mastercard, Visa,…)
- Acquirer (e.g., SumUp)
- Merchant
- Cardholder



Steps: Contactless Protocol

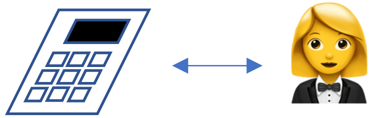
- **Application Selection**

- How can I communicate with the card?
- Where can I find the information on the card?

- **Synchronization**

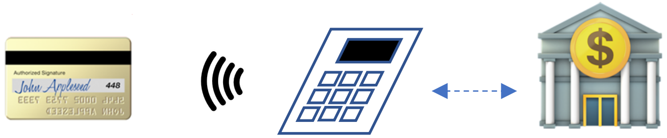
- What information does the issuer need to complete the transaction (amount, currency,…)?
- What Cardholder Verification Methods are supported?

- **Cardholder Verification**



- Is this the legitimate cardholder?
- If CVM limit is exceeded request supported CVM

- **Authentication/Authorization**



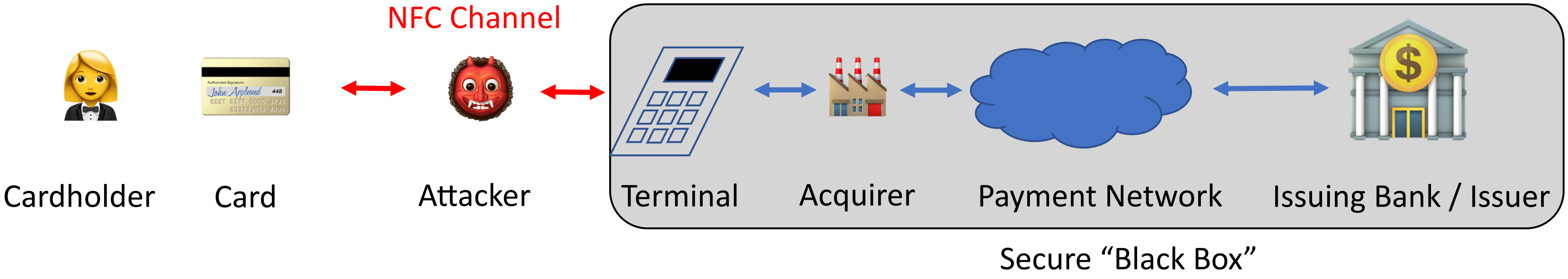
- Are all requirements met to settle the transaction?
- (In addition, the acquirer and the payment network may use fraud detection systems and block suspicious transaction.)

Security: Contactless Protocol

Authentication / Authorization

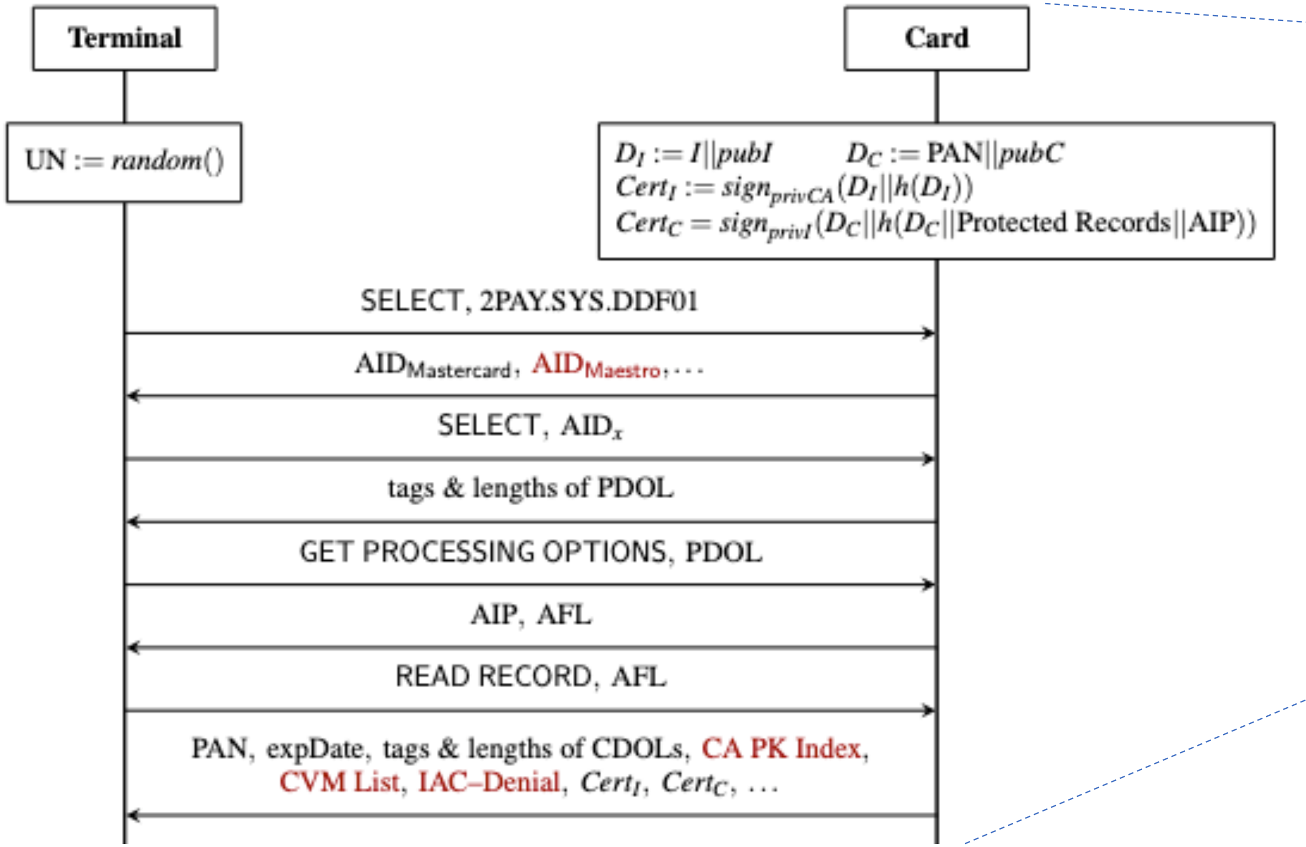
- Offline (terminal, card)
  - Uses public key cryptography (signatures)
  - Every card has an RSA key pair and a corresponding certificate of the issuer
  - Terminal has a list of root certificates, checks if certificates provided by the card are valid and verifies parameters (e.g., CVM list)
- Online (issuer/bank)
  - Based on a shared key between issuer (bank) and card
  - Card creates a Message Authentication Code over transaction elements
  - Terminal sends data and MAC to the issuer for authorization

Attacker Model & Attacker’s Goal



- **Attacker’s Goal**: Execute arbitrary payments with a victim’s card, without (or with downgraded) cardholder verification
- **Prerequisite**: The attacker has an NFC connection to the victim’s card
  - The card is stolen or lost (but not yet revoked)
  - The attacker relays an NFC channel between the victim’s card (still in victim’s possession) and a terminal of his choice

The Mastercard Protocol



Terminal

Card

UN := $random()$

$D_I := I||pubI$ $D_C :=$ PAN$||pubC$
$Cert_I := sign_{privCA}(D_I||h(D_I))$
$Cert_C = sign_{privI}(D_C||h(D_C||\text{Protected Records}||\text{AIP}))$

SELECT, 2PAY.SYS.DDF01

$\text{AID}_{\text{Mastercard}}$, $\text{AID}_{\text{Maestro}}, \ldots$

SELECT, AID_x

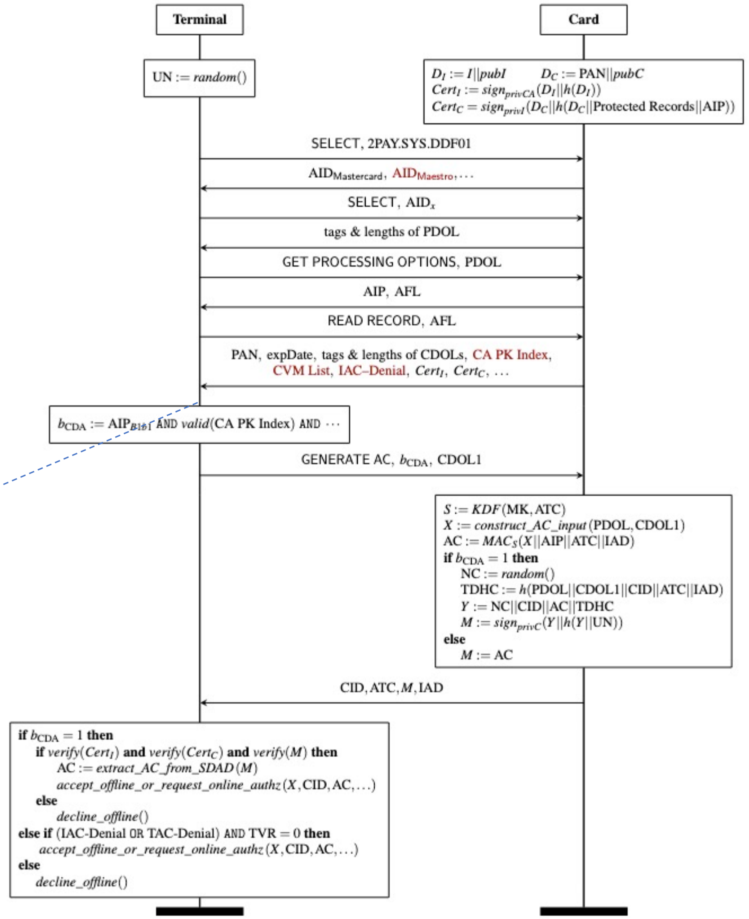
tags & lengths of PDOL

GET PROCESSING OPTIONS, PDOL

AIP, AFL

READ RECORD, AFL

PAN, expDate, tags & lengths of CDOLs, CA PK Index, CVM List, IAC–Denial, $Cert_I$, $Cert_C$, …



Terminal

Card

UN := $random()$

$D_I := I||pubI$ $D_C :=$ PAN$||pubC$
$Cert_I := sign_{privCA}(D_I||h(D_I))$
$Cert_C = sign_{privI}(D_C||h(D_C||\text{Protected Records}||\text{AIP}))$

SELECT, 2PAY.SYS.DDF01

$\text{AID}_{\text{Mastercard}}$, $\text{AID}_{\text{Maestro}}, \ldots$

SELECT, AID_x

tags & lengths of PDOL

GET PROCESSING OPTIONS, PDOL

AIP, AFL

READ RECORD, AFL

PAN, expDate, tags & lengths of CDOLs, CA PK Index, CVM List, IAC–Denial, $Cert_I$, $Cert_C$, …

$b_{\text{CDA}} := \text{AIP}_{B1b1}$ AND $valid$(CA PK Index) AND ⋯

GENERATE AC, b_{CDA}, CDOL1

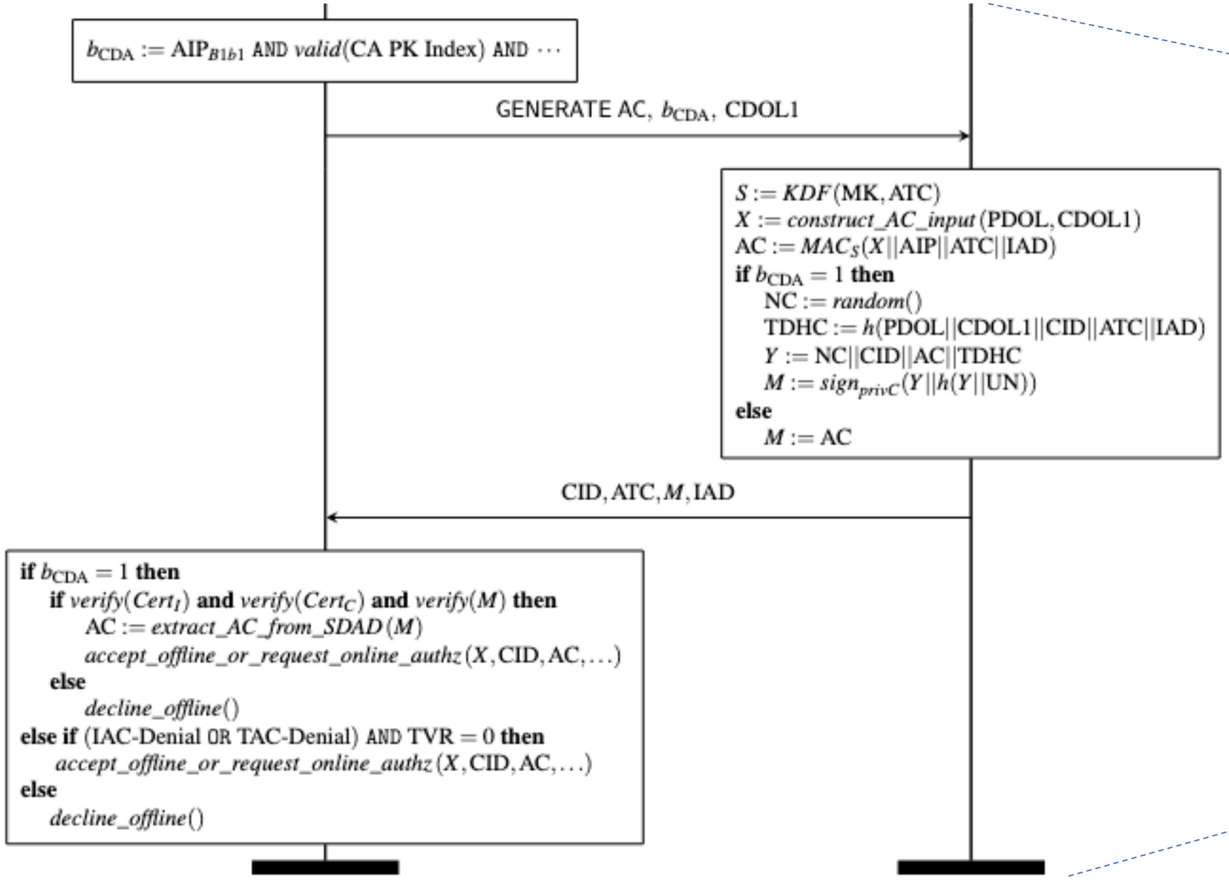
```
$S := KDF(\text{MK}, \text{ATC})$
$X := construct\_AC\_input(\text{PDOL}, \text{CDOL1})$
$\text{AC} := MAC_S(X||\text{AIP}||\text{ATC}||\text{IAD})$
if $b_{\text{CDA}} = 1$ then
    $\text{NC} := random()$
    $\text{TDHC} := h(\text{PDOL}||\text{CDOL1}||\text{CID}||\text{ATC}||\text{IAD})$
    $Y := \text{NC}||\text{CID}||\text{AC}||\text{TDHC}$
    $M := sign_{privC}(Y||h(Y||\text{UN}))$
else
    $M := \text{AC}$
```

CID, ATC, M, IAD

```
if $b_{\text{CDA}} = 1$ then
    if $verify(Cert_I)$ and $verify(Cert_C)$ and $verify(M)$ then
        $\text{AC} := extract\_AC\_from\_SDAD(M)$
        $accept\_offline\_or\_request\_online\_authz(X, \text{CID}, \text{AC}, \ldots)$
    else
        $decline\_offline()$
else if (IAC-Denial OR TAC-Denial) AND TVR $= 0$ then
    $accept\_offline\_or\_request\_online\_authz(X, \text{CID}, \text{AC}, \ldots)$
else
    $decline\_offline()$
```

PDOL: Processing Options Data Object List (e.g., amount, currency,…)
CDOL: Card Risk Management Data Object List (e.g., CVM results, UN, …)
IAC: Issuer Action Code (Denial, Default, Online)

The Mastercard Protocol



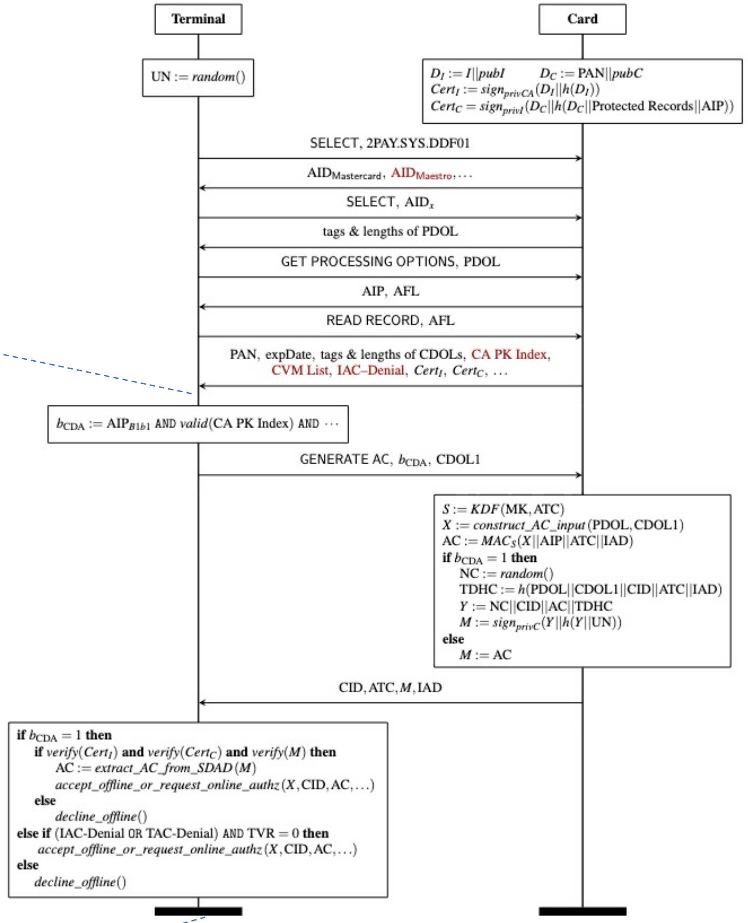
$b_{\text{CDA}} := \text{AIP}_{B1b1}$ AND $valid$(CA PK Index) AND $\cdots$

GENERATE AC, b_{CDA}, CDOL1

```
$S := KDF(\text{MK}, \text{ATC})$
$X := construct\_AC\_input(\text{PDOL}, \text{CDOL1})$
$\text{AC} := MAC_S(X||\text{AIP}||\text{ATC}||\text{IAD})$
if $b_{\text{CDA}} = 1$ then
    $\text{NC} := random()$
    $\text{TDHC} := h(\text{PDOL}||\text{CDOL1}||\text{CID}||\text{ATC}||\text{IAD})$
    $Y := \text{NC}||\text{CID}||\text{AC}||\text{TDHC}$
    $M := sign_{privC}(Y||h(Y||\text{UN}))$
else
    $M := \text{AC}$
```

$\text{CID}, \text{ATC}, M, \text{IAD}$

```
if $b_{\text{CDA}} = 1$ then
    if $verify(Cert_I)$ and $verify(Cert_C)$ and $verify(M)$ then
        $\text{AC} := extract\_AC\_from\_SDAD(M)$
        $accept\_offline\_or\_request\_online\_authz(X, \text{CID}, \text{AC}, \ldots)$
    else
        $decline\_offline()$
else if (IAC-Denial OR TAC-Denial) AND $\text{TVR} = 0$ then
    $accept\_offline\_or\_request\_online\_authz(X, \text{CID}, \text{AC}, \ldots)$
else
    $decline\_offline()$
```



$\text{UN} := random()$

$D_I := I||pubI$ $D_C := \text{PAN}||pubC$
$Cert_I := sign_{privCA}(D_I||h(D_I))$
$Cert_C = sign_{privI}(D_C||h(D_C||\text{Protected Records}||\text{AIP}))$

SELECT, 2PAY.SYS.DDF01

$\text{AID}_{\text{Mastercard}}$, $\text{AID}_{\text{Maestro}}, \cdots$

SELECT, AID_x

tags & lengths of PDOL

GET PROCESSING OPTIONS, PDOL

AIP, AFL

READ RECORD, AFL

PAN, expDate, tags & lengths of CDOLs, CA PK Index, CVM List, IAC–Denial, $Cert_I$, $Cert_C$, …

$b_{\text{CDA}} := \text{AIP}_{B1b1}$ AND $valid$(CA PK Index) AND $\cdots$

GENERATE AC, b_{CDA}, CDOL1

```
$S := KDF(\text{MK}, \text{ATC})$
$X := construct\_AC\_input(\text{PDOL}, \text{CDOL1})$
$\text{AC} := MAC_S(X||\text{AIP}||\text{ATC}||\text{IAD})$
if $b_{\text{CDA}} = 1$ then
    $\text{NC} := random()$
    $\text{TDHC} := h(\text{PDOL}||\text{CDOL1}||\text{CID}||\text{ATC}||\text{IAD})$
    $Y := \text{NC}||\text{CID}||\text{AC}||\text{TDHC}$
    $M := sign_{privC}(Y||h(Y||\text{UN}))$
else
    $M := \text{AC}$
```

$\text{CID}, \text{ATC}, M, \text{IAD}$

```
if $b_{\text{CDA}} = 1$ then
    if $verify(Cert_I)$ and $verify(Cert_C)$ and $verify(M)$ then
        $\text{AC} := extract\_AC\_from\_SDAD(M)$
        $accept\_offline\_or\_request\_online\_authz(X, \text{CID}, \text{AC}, \ldots)$
    else
        $decline\_offline()$
else if (IAC-Denial OR TAC-Denial) AND $\text{TVR} = 0$ then
    $accept\_offline\_or\_request\_online\_authz(X, \text{CID}, \text{AC}, \ldots)$
else
    $decline\_offline()$
```

CDA: Combined DDA/Application Cryptogram Generation
DDA: Dynamic Data Authentication

Bypassing Cardholder Verification

- The supported cardholder verification methods are announced by the card (to the terminal) in the field `CVM List`
- The `CVM List` field is integrity protected by the card's certificate
  - The field is contained in the card's certificate signed by the issuer
- What if offline authentication fails?
  - On page 255 of [1] there is a suspicious pseudo-code fragment:

```
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
```

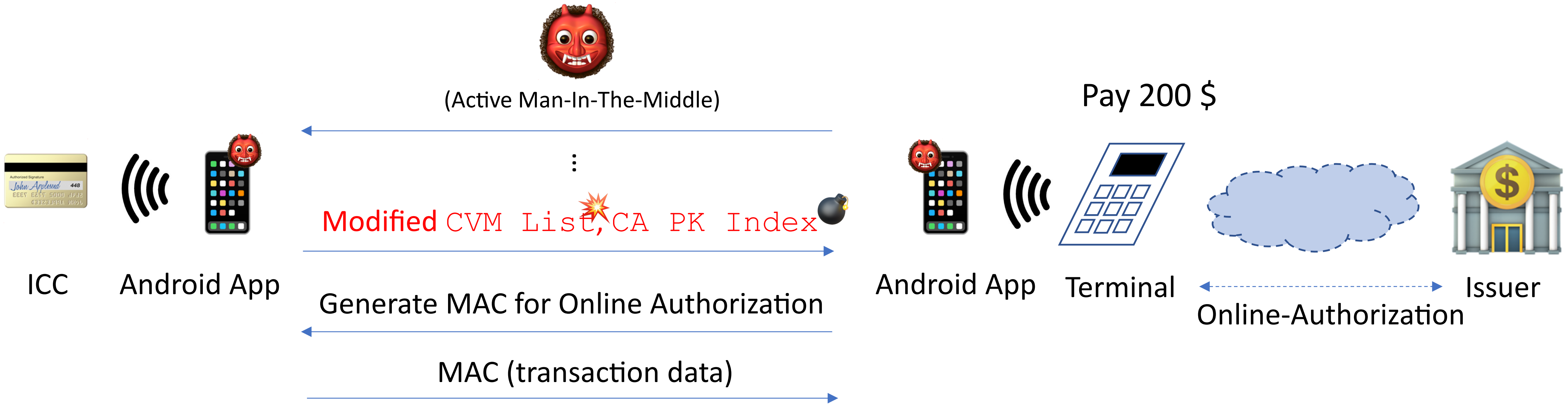
  - Furthermore, on page 435 of [1], the specification says:

```
IF 'CDA failed' in Terminal Verification Results AND On Device Cardholder Verification is not
supported THEN Do not request CDA
```

[1]: "EMV Contactless Specification for Payment Systems", Book C-2, Kernel 2 Specification, Version 2.10

Bypassing Cardholder Verification

Attack Concept


(Active Man-In-The-Middle)
Pay 200 $
⋮
Modified CVM List, CA PK Index
Generate MAC for Online Authorization
MAC (transaction data)
ICC
Android App
Android App
Terminal
Online-Authorization
Issuer

💣 Inexistent `CA PKA Index` turns off offline-authentication

💥 Arbitrary modification of `CVM List` possible

Results 💣

- 💥 We have tested our findings in real-world payments with 7 different cards issued by three different banks from two countries on different terminal models
- 💥 We have successfully bypassed PIN verification in 9 transactions using 5 different cards of two issuers
- 💂 For one issuer, the fraud detection system in the online authorization phase prevented our attack
- 💂 One terminal type (exclusively used in public transportation) seems not to be vulnerable to our attack

Summary

- EMV is a complex protocol executed between a card/device and a terminal
- Specification and protocol description are (at least for humans) difficult to analyze
- Multiple stakeholders involved, who might influence the outcome of a transaction, i.e., accept or decline transactions
- Results presented are from a specification that allows malicious modifications of critical protocol parameters
- Vulnerability verified in real-world transactions
- Attack trace re-discovered in a Tamarin model of the EMV-protocol
- Security of the countermeasures formally proved in Tamarin