Smart Cards

NFC Tools

read and write NFC tags

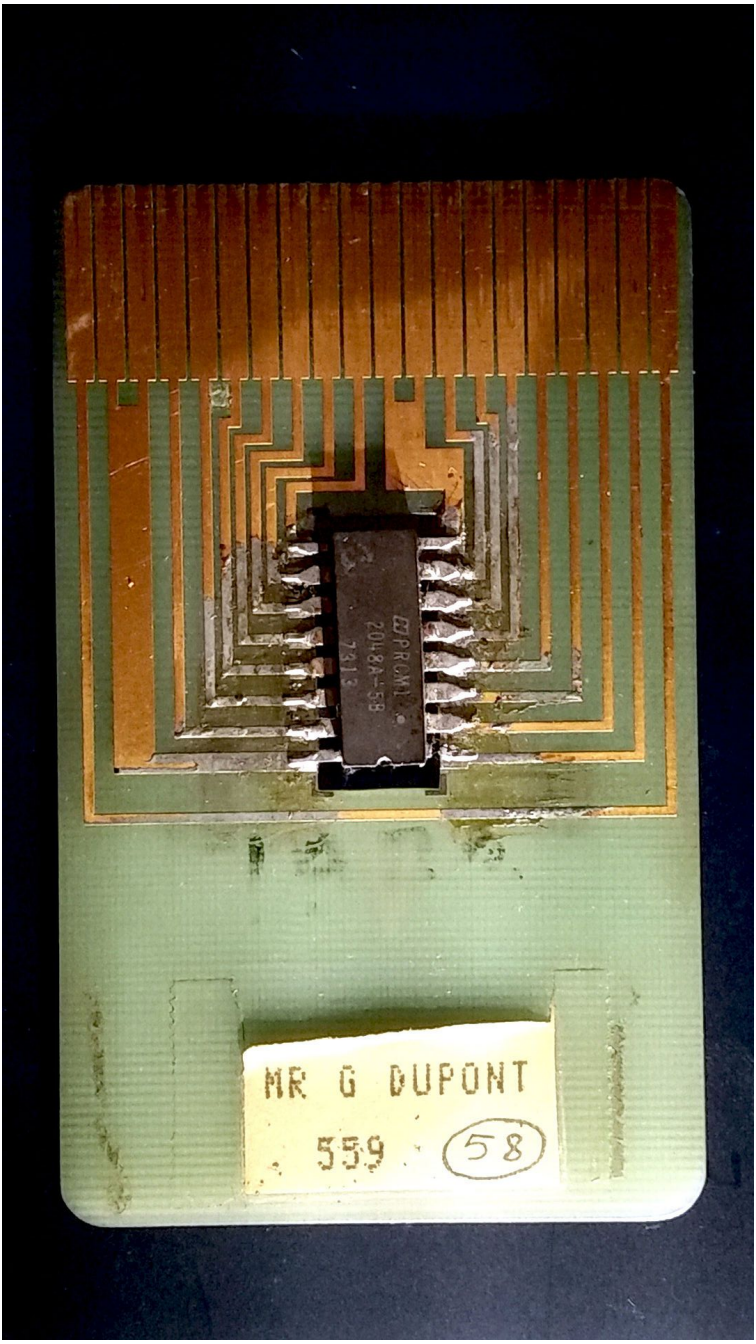
by *wakdev*

App Store

Play Store

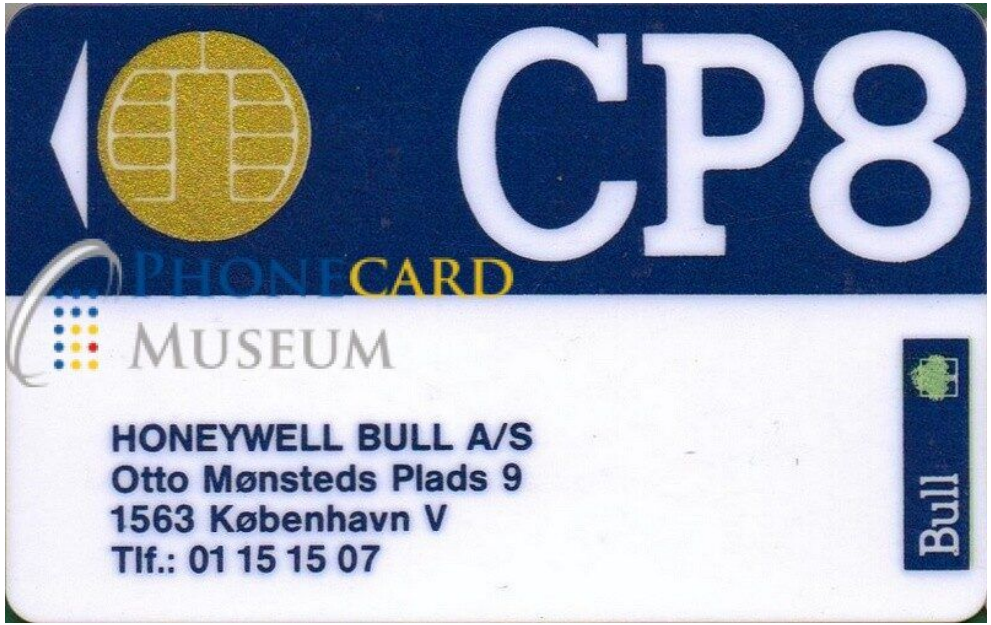
The Beginning of smart cards

- Mid 1970s: first smart card
  - Storage device
- 1979: Michel Ugon from Bull invents the first microprocessor smart card with two chips: “Bull CP8"
  - Storage + Processor
- Early 1980s: smart cards spread to Europe
- 1983: Card access pay phones in Europe
- 1985: U.S. becomes interested in smart cards
- Early 1990s: Smart cards spread to other parts of the world
- In Europe, nearly all bank cards have been converted to smart cards
- Smart cards today: credit and debit cards, electronic cash systems, secure authentication and identification systems, …


PROM
2048A-5B
7313
MR G DUPONT
559
58

The Beginning of smart cards

- Mid 1970s: first smart card
  - Storage device
- 1979: Michel Ugon from Bull invents the first microprocessor smart card with two chips: “Bull CP8"
  - Storage + Processor
- Early 1980s: smart cards spread to Europe
- 1983: Card access pay phones in Europe
- 1985: U.S. becomes interested in smart cards
- Early 1990s: Smart cards spread to other parts of the world
- In Europe, nearly all bank cards have been converted to smart cards
- Smart cards today: credit and debit cards, electronic cash systems, secure authentication and identification systems, …


CP8
PHONECARD
MUSEUM
HONEYWELL BULL A/S
Otto Mønsteds Plads 9
1563 København V
Tlf.: 01 15 15 07
Bull

The Beginning of smart cards

- Mid 1970s: first smart card
  - Storage device
- 1979: Michel Ugon from Bull invents the first microprocessor smart card with two chips: “Bull CP8"
  - Storage + Processor
- Early 1980s: smart cards spread to Europe
- 1983: Card access pay phones in Europe
- 1985: U.S. becomes interested in smart cards
- Early 1990s: Smart cards spread to other parts of the world
- In Europe, nearly all bank cards have been converted to smart cards
- Smart cards today: credit and debit cards, electronic cash systems, secure authentication and identification systems, …

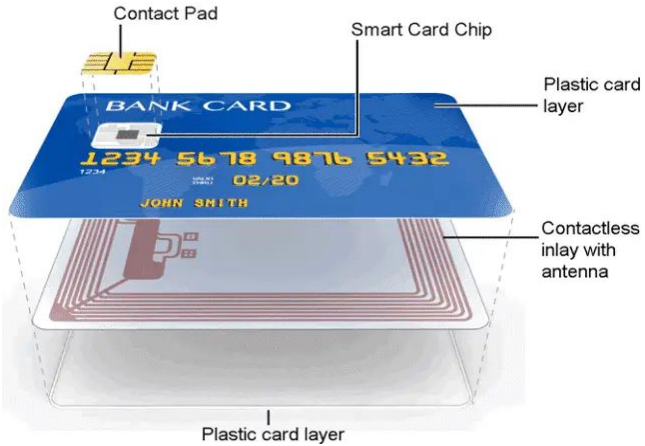
Magnetic Stripe Cards

- Storing data on magnetic material attached to card
- Content can be updated
- Read by swiping it past a magnetic reading head
- Common in credit cards, identity cards, transportation tickets
- Various security flaws
- Data not protected by encryption
- Vulnerable to “skimming”

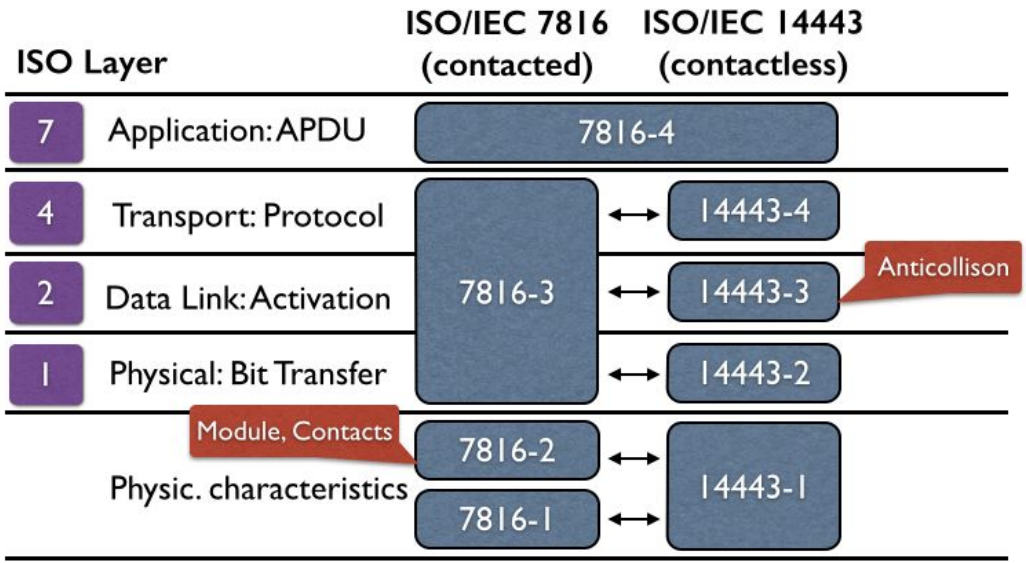
The Beginning of smart cards

- Mid 1970s: first smart card
  - Storage device
- 1979: Michel Ugon from Bull invents the first microprocessor smart card with two chips: “Bull CP8"
  - Storage + Processor
- Early 1980s: smart cards spread to Europe
- 1983: Card access pay phones in Europe
- 1985: U.S. becomes interested in smart cards
- Early 1990s: Smart cards spread to other parts of the world
- In Europe, nearly all bank cards have been converted to smart cards
- Smart cards today: credit and debit cards, electronic cash systems, secure authentication and identification systems, …

Structure


Contact Pad
Smart Card Chip
Plastic card layer
BANK CARD
1234 5678 9876 5432
02/20
JOHN SMITH
Contactless inlay with antenna
Plastic card layer

ISO Layers


ISO Layer
ISO/IEC 7816 (contacted)
ISO/IEC 14443 (contactless)
7
Application: APDU
7816-4
4
Transport: Protocol
14443-4
2
Data Link: Activation
7816-3
14443-3
Anticollison
1
Physical: Bit Transfer
14443-2
Module, Contacts
Physic. characteristics
7816-2
7816-1
14443-1

Contacted: ISO 7816-1 and 7816-2

- ISO 7816-1:
  - Physical characteristics
  - Mechanical characteristics
  - Environmental characteristics
- ISO 7816-2:
  - Location and size of contact area
  - Form and material of contacts
  - Contact arrangement

Contactless ISO 14443-1

- ISO 14443-1
  - Physical characteristics of contactless cards
  - Dimensions and tolerances of the card and antenna
  - Frequency range and modulation
  - Power level requirements
  - Test procedures for evaluating the card's performance

Types of Smart Cards

Contact Smart Cards

- Require physical contact with a card reader. When inserted:
  - Card powers up
  - Communicates with reader
- Common in debit and credit cards
  - Card needs to be inserted into a reader and then enter their pin code

Contactless Smart Cards

- These cards use RFID / NFC to communicate with a card reader
- Transportation cards, Access control, Electronic wallets

RFID

- “Radio-Frequency Identification”
- One-way communication between an active reader and passive tag.
- Uses different frequencies, including 125 kHz, 13.56 MHz, and 860-960 MHz.
- Longer communication range, up to several meters.

NFC

- Evolved from RFID and supports RFID Type A, Type B.
- Enables two-way communication, allowing peer-to-peer data exchange.
- Operates at 13.56 MHz frequency.
- Shorter communication range, typically up to 4 cm.
- Common applications include mobile payments, transit ticketing, and data sharing between devices.

Dual-interface smart cards

- Both contact and contactless interfaces
- Increasingly popular for banking applications
- Flexible
- Work for both interfaces
- Payments, transportation and access control

Host Card Emulation (HCE)

- Most modern phones have a NFC antenna
- Allows Device to read and emulate various NFC cards
- Functionality is locked behind a strict API
  - Usually has a private emulation address space (08 XX XX XX)
  - iOS also limits access to very specific use cases
  - can be bypassed by Jailbreaking/Rooting the device
- Technology that powers Apple Pay and Google Pay
  - Payments at any payment terminal that accepts traditional cards

Communication

APDU: Application Protocol Data Unit

- Communication protocol
- Data transfer between Card and Reader
- Command APDU
- Response APDU

Command APDU

<table>
<tr><td colspan="6">Command APDU</td></tr>
<tr><td colspan="4">Command APDU Header</td><td rowspan="2">Lc</td><td rowspan="2">Data</td><td rowspan="2">Le</td></tr>
<tr><td>CLA</td><td>INS</td><td>P1</td><td>P2</td></tr>
<tr><td colspan="7">CLA: Class byte (command-ID), INS: Instruction,
P1, P2: Parameter, Lc: Length of command data,
Data: Command data, Le: Length of expected data</td></tr>
</table>

- CLA (1 Byte): type of command
- INS (1 Byte): specifies command
- P1 - P2 (2 Byte): parameters
- Lc (0, 1 or 3 Bytes): encodes the number of bytes of the command data:
- Data / Nc:
  - Variable length (Lc)
  - Instruction data
- Le (0, 1, 2 or 3 Bytes): expected length of response

Response APDU

Response APDU		
Data	SW1	SW2
Data: Response data, SW1, SW2: Status Word		

- Variable data length followed by 2 bytes
- Data: response data for reader device
- SW: status of command
  - Success:
    - SW1: ‘90’
    - SW2: ‘00’
  - Failure:
    - SW1: error code
    - SW2: additional information about error

UID

- “Unique Identifier”: unique identification number assigned to a contactless smart card in its first sector
- Generated by manufacturer and cannot be changed
- The use of UID as a form of security is limited
- Often used for simple access control systems

Demo Time!

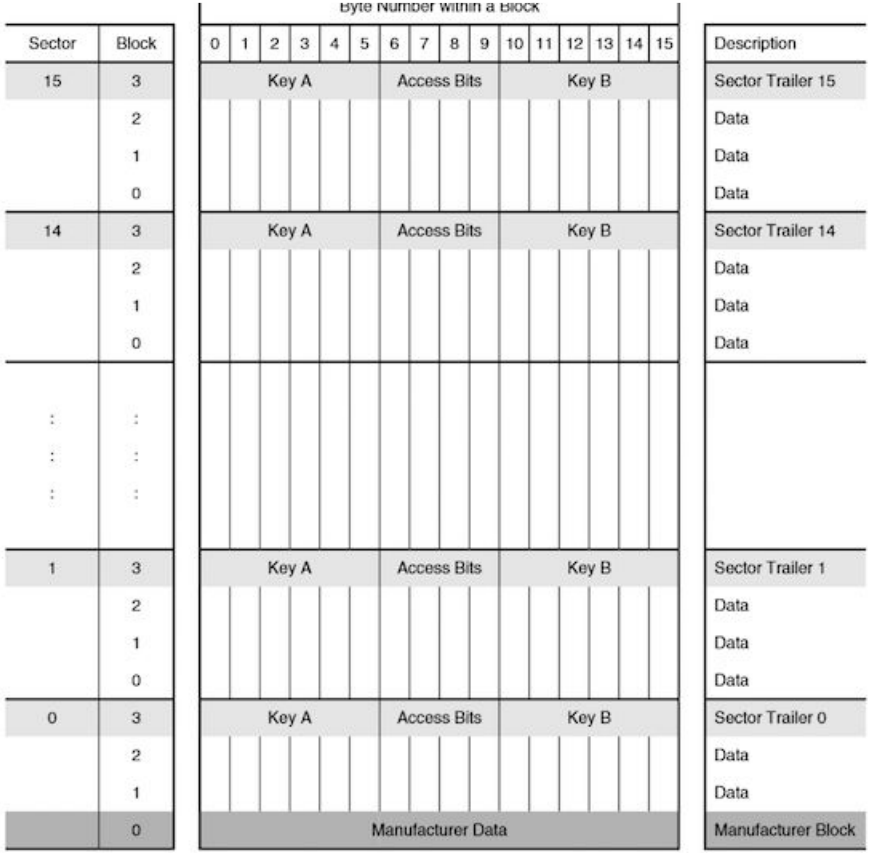
(Access Control)

“Crypto” Cards

- Security-wise more sophisticated than UID-based systems
- Have an onboard crypto chip for key authentication
- To be able to read or write, you need to provide the correct key(s)
- Useful for public transport, vending machines, hotel cards etc.

MIFARE Classic

- First card since the 90s
  - very safe (at first)
- Data organized in blocks and sectors
  - Data Blocks
  - UID Block
  - Sector Trailer Blocks
    - authentication keys
    - access control



MIFARE Classic

- Access Bits
  - describe the allowance of the keys
  - stored in 3 Bytes: reversed, normal and mixed

- Example: $C1_3$=1, $C2_3$=1, $C3_3$=1
  - A & B sector read only

Table 6. Access conditions

Access Bits	Valid Commands		Block	Description
$C1_3$, $C2_3$, $C3_3$	read, write	→	3	sector trailer
$C1_2$, $C2_2$, $C3_2$	read, write, increment, decrement, transfer, restore	→	2	data block
$C1_1$, $C2_1$, $C3_1$	read, write, increment, decrement, transfer, restore	→	1	data block
$C1_0$,$C2_0$, $C3_0$	read, write, increment, decrement, transfer, restore	→	0	data block

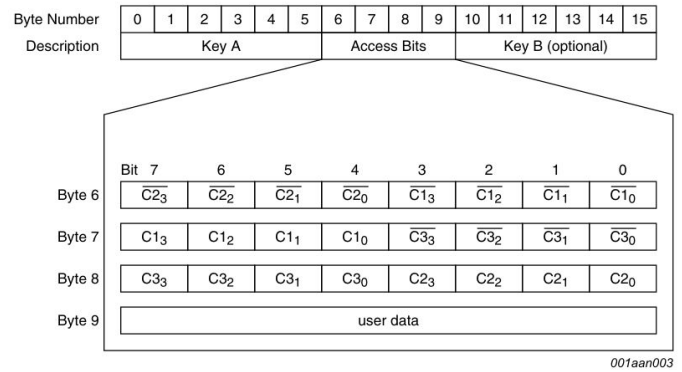


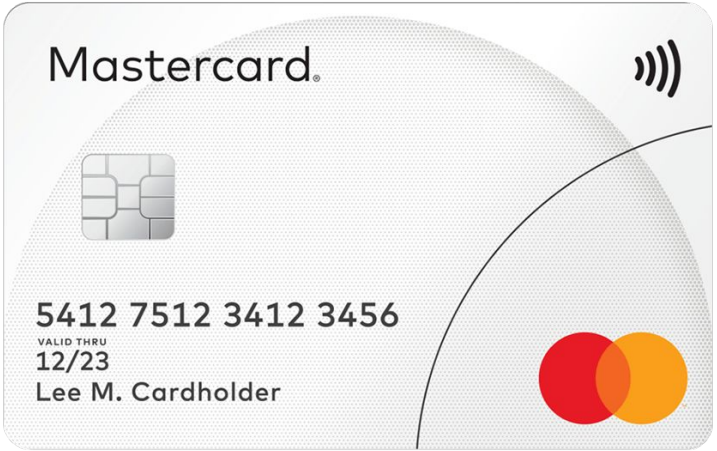
Fig 10. Access conditions

MIFARE Classic

- Crypto-1:
  - Designed by NXP
- Data not readable without authentication

EMV Standard: Introduction

- EMV: Europay, Mastercard, Visa collaboration
- Global standard for chip-based payment cards
- Enhanced security over magnetic stripe cards
- Widely adopted, reduces fraud and counterfeiting
- Chip stores cardholder data securely
- Enables secure online and offline transactions

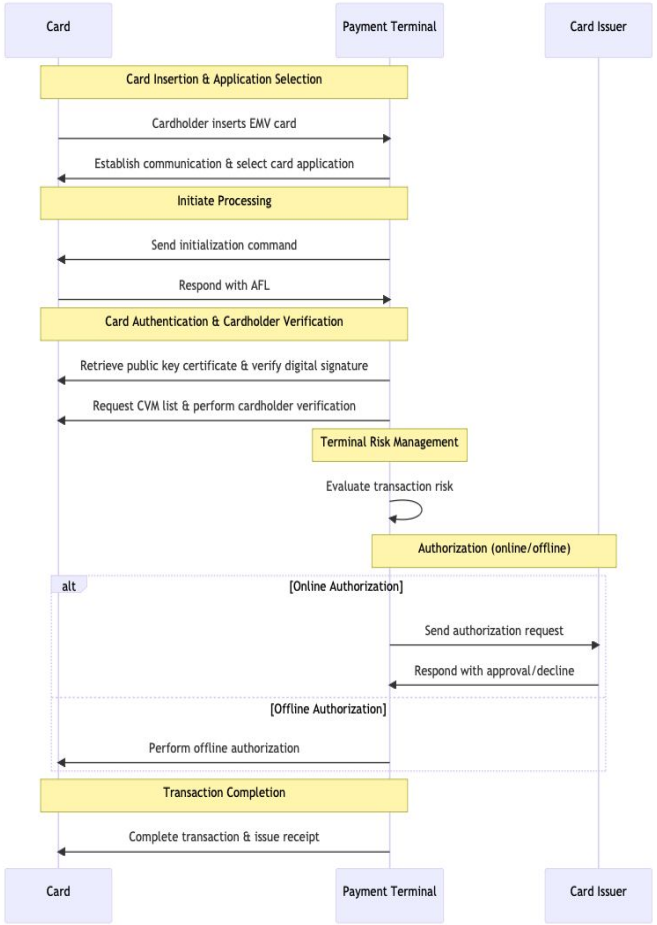


EMV Transaction Flow (1/3)

- Cardholder inserts EMV card into payment terminal, initiating transaction
- Payment terminal establishes communication with card's chip for data exchange
- Terminal assesses card applications, selects appropriate app (e.g., debit or credit) based on transaction type and its own capabilities
- Terminal sends initialization command, card responds with Application File Locator (AFL), providing files and records needed for transaction

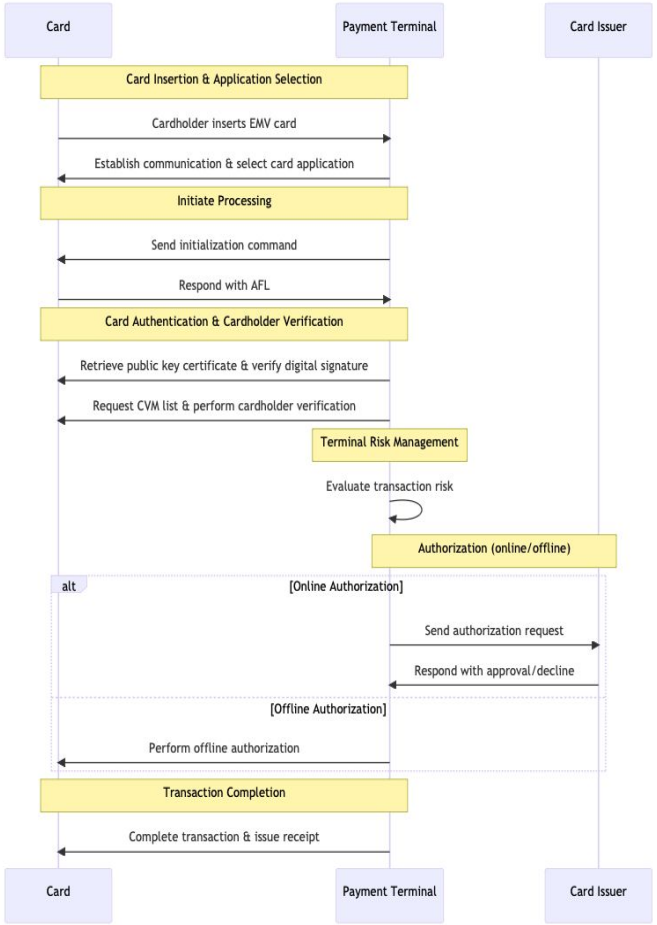
EMV Transaction Flow (2/3)

- Terminal retrieves card's public key certificate
  - verifies authenticity by validating digital signature
- Terminal requests Cardholder Verification Method (CVM) list from card
  - chooses suitable CVM
  - verifies cardholder identity
- Terminal evaluates online and offline transaction based on risk management parameters
  - floor limit checks,
  - random transaction selection for online authorization



EMV Transaction Flow (3/3)

- Online authorization
  - terminal sends request to card issuer, issuer evaluates, responds with approval/decline
- Offline authorization
  - terminal uses card's risk management capabilities, cryptographic techniques for approval
- Approved transaction leads to completion, receipt issuance, and potentially a Transaction Certificate (TC) proof of authenticity



Cryptography in EMV - Asymmetric Cryptography

- Public/private key pairs essential for securing digital signatures and card authentication
- Card's private key never leaves the chip, public key shared via certificate
- RSA: popular choice in EMV, large prime numbers offer strong security
- ECC: more efficient than RSA, smaller key sizes save computational power and memory in devices like smart cards

Cryptography in EMV - Symmetric Cryptography

- Symmetric algorithms protect sensitive data during card-terminal communication
- Secret key shared between card and terminal for data encryption/decryption
- Triple DES (3DES): widely used in EMV for “secure” messaging and session key derivation
- AES: faster and more secure than 3DES, adoption in EMV gradually increasing for enhanced security

Cryptography in EMV - Key Management

- Effective key management crucial for EMV security
- Static keys: consistent throughout card's lifecycle, stored securely in chip, used for card authentication
- Dynamic keys: generated on-the-fly during transactions for specific tasks (e.g., secure messaging, session key derivation), temporary and discarded once transaction is completed
- EMV key management processes ensure secure key generation, storage, and usage

Attack vectors on smart cards

UID-Cloning

- Simple Access Control Systems only check for a matching UID
- UID is placed in memory sector 0, which is not writeable (on “genuine” cards)
- As only NXP knows how to manufacture RFID tags, this system is safe

de.aliexpress.com

Verkaufen auf ali express | Hilfe | Käuferschutz | mobile | / Deutsch / EUR | Wunschliste | Konto

AliExpress

nfc magic cards

0

Kategorien

Sicherheit und Schutz

AliExpress Mobile App

Suchen überall und jederzeit!

Scannen oder klicken Sie zum Download

Aliexpress > Sicherheit und Schutz > **"nfc magic cards"**

Preis: Min. - Max. Plus Kostenloser Versand ★★★★☆ oder mehr

Sortieren nach: **Beste Übereinstimmung** | Bestellungen | Preis | Anzeigen können die Rangliste beeinflussen. Erfahren Sie ... | Sehen:

€1.22
63 verkauft ★5
5 teile/los UID Veränderbar NFC K...
+Versand: € 1.96
Shenzhen Lanhong company Store

€0.25
26 verkauft ★4
1pc NFC Tag NFC215 504 Bytes IS...
+Versand: € 1.61
Shenzhen Lanhong company Store

€4.75
3 verkauft ★5
6 teile/los UID veränderbar nfc kar...
+Versand: € 0.63
SZ WELCOME Store

€1.42
2 verkauft
5 stücke 13,5 MHZ UID Veränderb...
+Versand: € 2.03
Shenzhen Lanhong company Store

You last purchased this item on 14 Apr 2023
Colour Name: **Pack Of 10** | View order details

Roll over image to zoom in

KDL Smart RFID 13.56MHz Card Rewritable UID Removable PVC Material for MF1 1K S50 Card Clone Block 0 S0 S0 Empty, UIDcard-10

Brand: Kadongli

4.1 ★★★★☆ 27 ratings

Amazon's Choice for "mifare classic 1k uid changeable"

€7.36

✓prime

Prices for items sold by Amazon include VAT. Depending on your delivery address, VAT may vary at Checkout. For other items, please see details.

Colour Name: **Pack Of 10**

€7.36 ✓prime	€26.21 ✓prime	€17.14

- 1, Betriebsfrequenz: 13,56 MHz.
- 2, Eigenschaften: lesbar und wiederbeschreibbar. UID änderbar.
- 3, Protokoll: ISO 14443-A.
- 4, Material: PVC-Kunststoff.
- 5, Größe: 86 * 54 * 0,84 mm.

› See more product details

Report incorrect product information.

Do you want to recycle your electrical and electronic equipment for free? Learn more

€7.36

✓prime

FREE delivery **Tuesday, May 9**. Order within 13 hrs 20 mins

Deliver to Emanuel - Anthering 5102

In stock

Quantity: 1

Add to Basket

Buy Now

Payment	Secure transaction
Dispatches from	Amazon
Sold by	Kadongli
Returns	Returnable within …

Details

For further information, company details, terms and conditions, and cancellation rights, please click on the seller's name.

Add gift options

UID Cloning - Magic Cards

- Chinese Clones exist
- They do not have this artificial limitation
- As Sector 0 is writeable, the UID can be easily changed (eg. using libnfc)
- Attack only needs brief physical “access” to a valid RFID tag: https://youtu.be/cbgHZgO6wiE?t=3320

Demo Time!

(UID Cloning)

UID Cloning - Mitigations

- Reader device attempts to write to Sector 0 of the card
- Deny access if successful, indicating detection of a magic card
- Invalidate suspected magic cards by writing all 0x00 to it (optional)
- Magic cards can however be configured to be read-only or block write attempts
- Limit reliance on UID for security-critical operations

MIFARE Classic - How to not implement your Crypto

- MIFARE Classic cards use the CRYPTO1 cipher
- Proprietary Stream Cipher designed by NXP, they decided to keep the implementation secret
- More than 3,5 billions cards was produced over the years
- Dec. 2007: Nohl & Plötz present Crypto-1 reverse engineering at CCC.
- Mar. 2008: Radboud Univ. fully reverse engineers Crypto-1; NXP attempts to block publication.
- Jul. 2008: Court allows paper publication on free speech grounds.
- Oct. 2008: Radboud Univ. publishes open-source Crypto-1 implementation (GNU GPL v2).
- Public exploits emerge, compromising Mifare Classic card reputation.

MIFARE Classic - Weaknesses of CRYPTO-1

- Keys: 48-bit length, brute-force possible with FPGA (~10h for one key).
- LFSR (Linear Feedback Shift Register) in RNG is predictable (constant initial condition); random numbers depend on clock cycles.
- Attacker can control generated random numbers by manipulating protocol, enabling key recovery.

Different attacks have emerged

- Card-Only Attacks:
  - Nested Attack: Introduced 2009 by Nijmegen Oakland (MFOC tool).
  - Dark-Side Attack: Introduced 2009 by Nicolas Courtois (MFCUK tool).
- Proxmark3 + Active Sniffing:
  - Proxmark3 allows emulation of Mifare cards by sniffing & replaying communication.

Proxmark3 + Active Sniffing:

- Proxmark3 is considered the “eierlegende Wollmilchsau” for RFID pentesting, analysis and research
- Attacker intercepts communication between MIFARE card & reader.
- Attacker obtains UID & keys for emulation and key recovery.
- Requires close proximity to card & reader for successful capture.

MIFARE Classic - Nested Attack (Overview)

- Authenticate to the block with default key and read tag's Nonce Nt (determined by LFSR)
- Authenticate to the same block with default key and read tag's Nonce Nt' (determined by LFSR)
- Compute “timing distance” (number of LFSR shifts)
- Guess the next Nt value, calculate ks1, ks2 and ks3 and try authenticate to a different block.

MIFARE Classic - Dark-Side-Attack (Overview)

- During authentication, when the reader sends its Nonce {Nr} and Key {Ar}, the tag checks the parity bits before checking the correctness of Ar. If one of the eight parity bits is incorrect, the tag does not respond.
- However,if all eight parity bits are correct, but the response Ar is incorrect, the tag will respond with a 4-bit error code 0x5 (NACK) indicating a transmission error. Moreover, this 4-bit error code is sent encrypted.
- If the attacker combine (XOR) the error code 0x5 value (known plaintext) with its encrypted version, he can recover four keystream bits.

Demo Time!

(MIFARE Classic)

If interested, tools used and more details can be found here:
https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf
https://github.com/nfc-tools/mfoc
https://github.com/nfc-tools/mfcuk

MIFARE Classic - Now what?

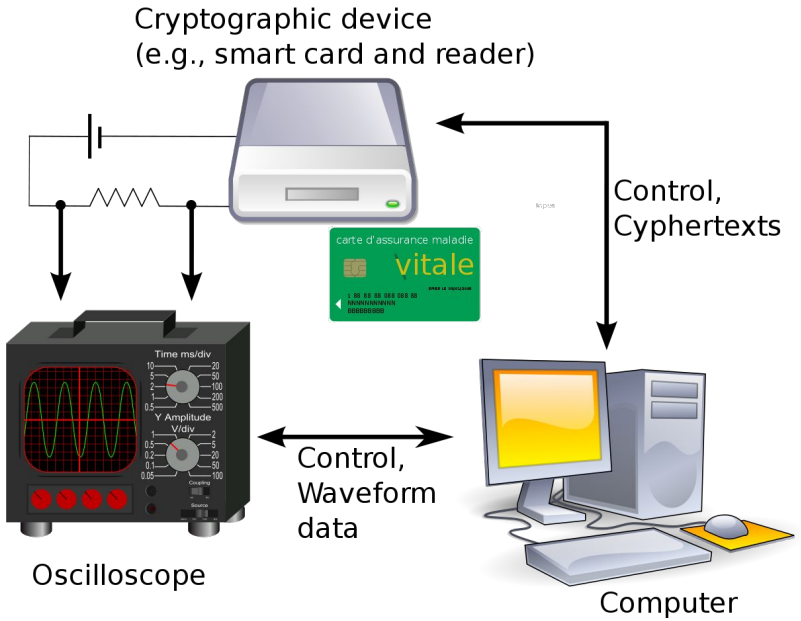
- NXP responded with "hardened" cards like MIFARE Classic EV1 (released around 2011),
  - in 2015, a new attack could recover secret keys from hardened variants
- NXP recommends migrating to higher security products.
  - MIFARE DESFire: Side-channel attack discovered in 2010; NXP claims difficulty in replication.
  - MIFARE Ultralight: Fare card manipulation demonstrated by Intrepidus in 2012.
  - MIFARE Ultralight EV1: Introduced with three decrement-only counters to address reloading attacks.
- Basically, do not use it
  - However, migration costs $$$ (quite a lot of that)
  - therefore still widely used today: https://en.wikipedia.org/wiki/MIFARE#Places_that_use_MIFARE_products

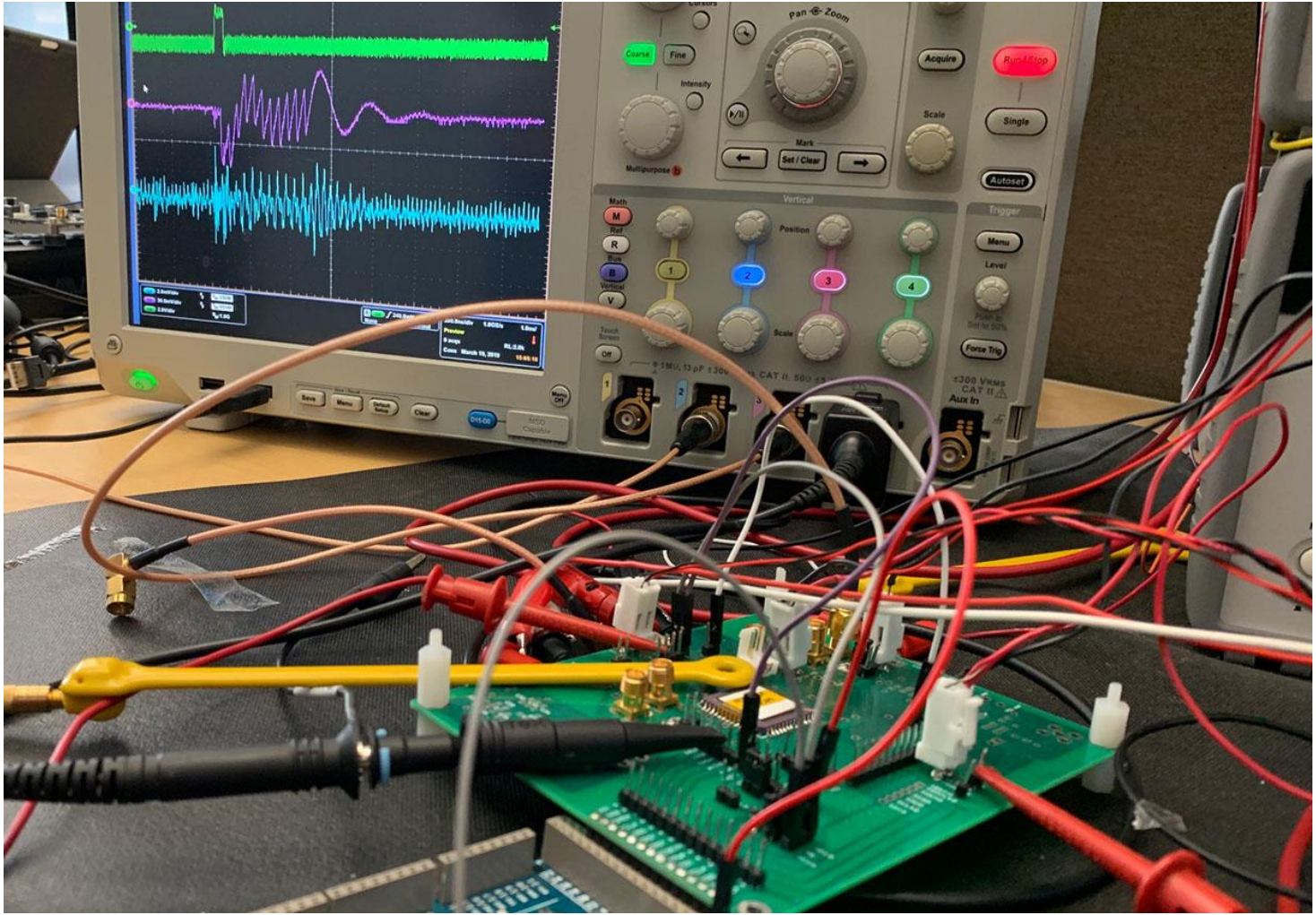
Sophisticated Attacks - for EMV and similar cards

- Store essential information like cardholder details, card number, expiration date, and a dynamic security code
- Security-wise far more advanced than typical smart cards
- Cryptographic operations are performed locally, Authentication secrets never leave the chip
- Combination of symmetric and asymmetric cryptography for secure communication and transaction authorization makes it difficult or impossible to sniff in on communication
- Primary Goal: Extract secrets like Private Keys, PIN or dynamic security codes from the chip
- Use case for the following methods: I have “acquired” a very high value smart card, but need an additional factor for authentication, which is verified by the card itself.

Side Channel Attacks

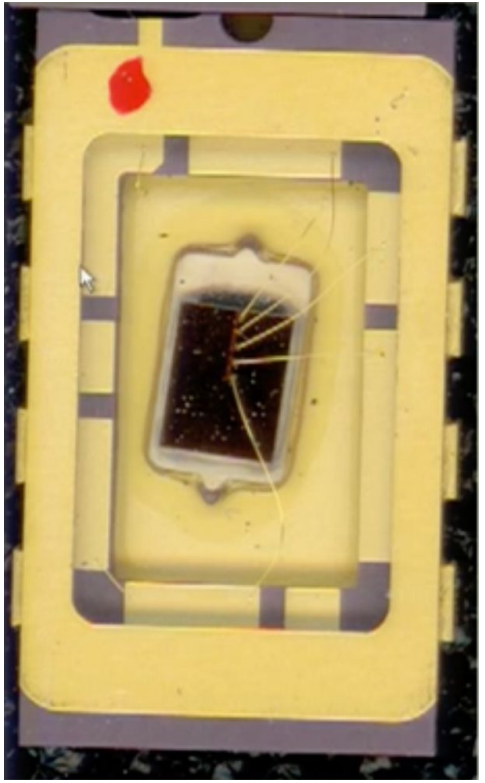
- Exploiting Unintended Information Leakage
- Types: Simple Power Analysis (SPA), Differential Power Analysis (DPA), Electromagnetic Analysis (EMA)
- Targeting power consumption, electromagnetic emissions, and timing information
- Revealing cryptographic keys or sensitive data
- Countermeasures: adding noise, randomizing timing of operations



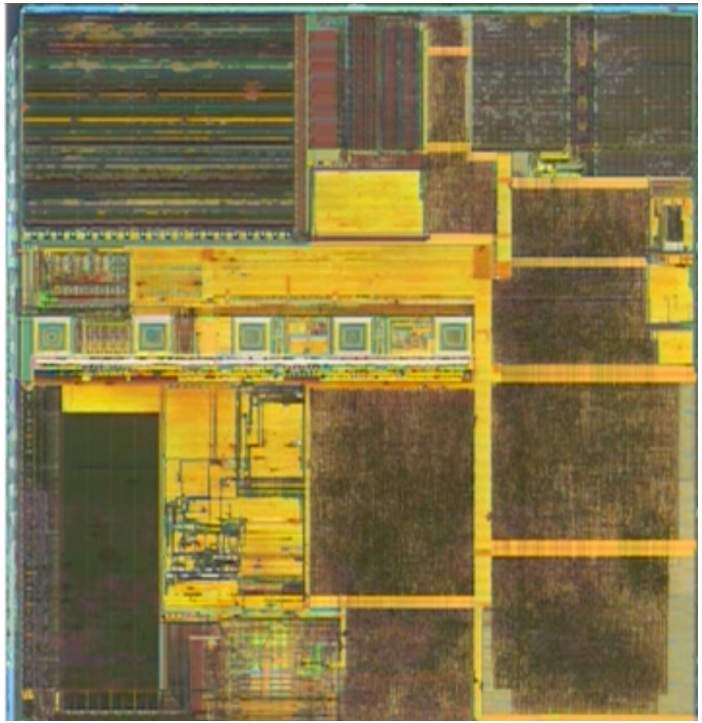

Pan
Zoom
Coarse
Fine
Intensity
Multipurpose
Acquire
Run/Stop
Single
Scale
Mark
Set / Clear
Autoset
Vertical
Math
Position
Trigger
Menu
Level
Force Trig
Aux In

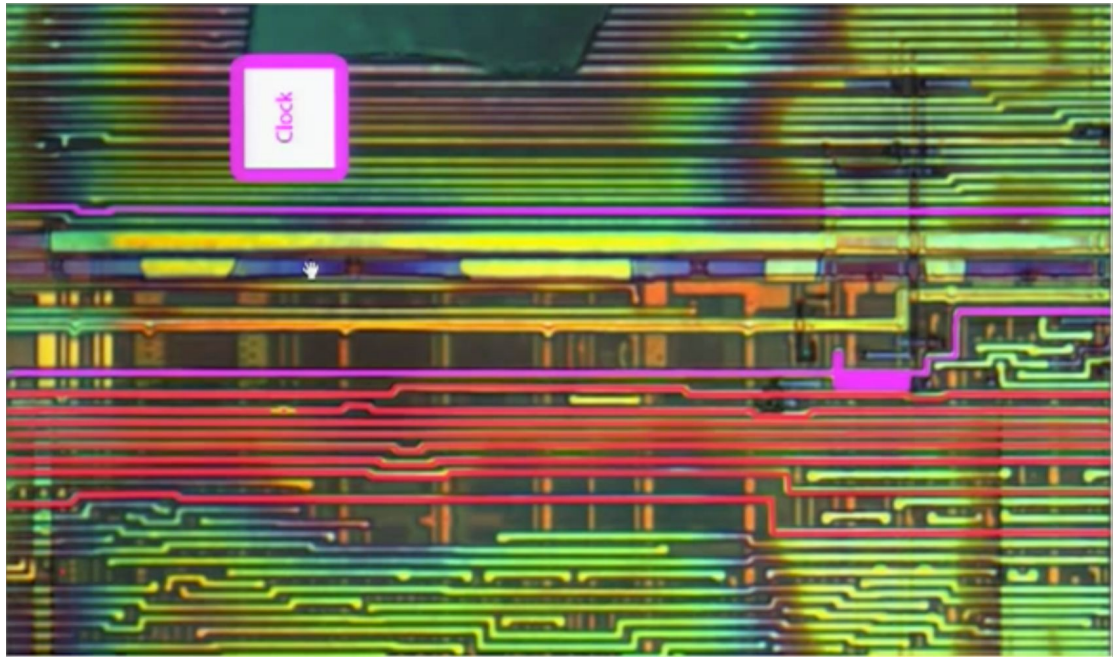
Microprobing

- Physically accessing chip's internal components using microscopic needles
- Monitoring or manipulating signals to reveal sensitive information or bypass security
- Reverse engineering chip design to identify targets for microprobing
- Requires high skill, specialized equipment, and access to the target chip
- Potentially damaging the chip or triggering tamper-evident mechanisms
- Less common and more challenging compared to other attacks due to technical barriers



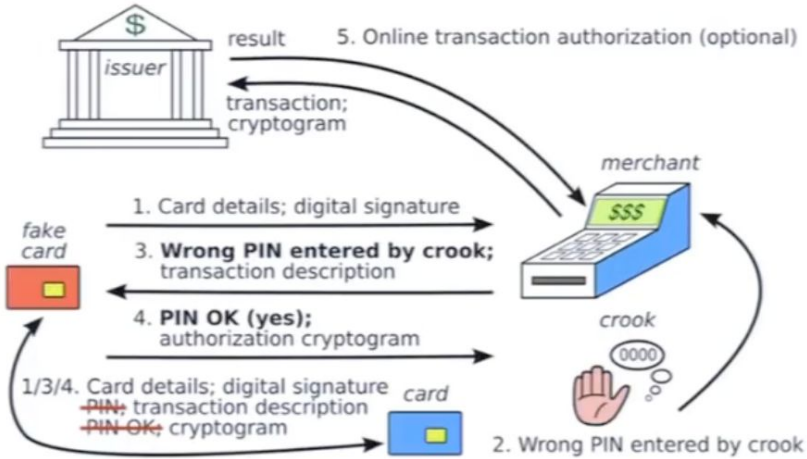
If interested, here is a very detailed blackhat talk on the topic:
https://www.youtube.com/watch?v=62DGIUpscnY




Clock

EMV Protocol Attacks - No-PIN Attack

- Bypassing PIN authentication by manipulating transaction data
- Tricking terminal into believing the correct PIN has been entered
- Enabling unauthorized transactions, compromising payment system security
- Demonstrated in BlackHat talk "How Smartcard Payment Systems Fail"
- Protecting against No-PIN attacks: proper security measures & monitoring transaction data
- See: https://youtu.be/ET0MFkRorbo?t=1671



Bypassing all of that - Skimming EMV Cards

Despite not spitting out PINs or Private Keys, it is shocking how much information a EMV card provides without any authentication at all. This levels the ground for skimming devices.

- Small, illicit devices (“skimmers”) placed over or inside card readers
- Capturing card data, including number, expiration date, and cardholder's name
- Stolen data used for fraudulent transactions or sold on the dark web
- Protecting against skimming: cardholder vigilance & inspecting card readers
- Merchants' role: security measures, tamper-evident seals & regular inspections

Demo Time!

(Card Skimming)


Thank you for listening!