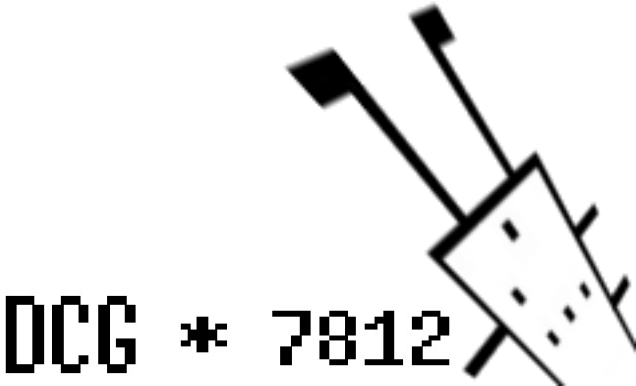
Modern payments security: EMV, NFC, etc.?

Nikita Abdullin

nabdullin@gmail.com

19.11.2012



Modern payments security: EMV, NFC, etc.?

- Intro: Payment Cards
- The EMV standard
- Attacks on EMV
- Intro: NFC
- EMV & NFC = ?
- Attacks on EMV & NFC
- Future

Modern payments security: EMV, NFC, etc.?

- **Intro: Payment Cards**
- The EMV standard
- Attacks on EMV
- Intro: NFC
- EMV & NFC = ?
- Attacks on EMV & NFC
- Future

About me

Not a black khat :)

Intro: Payment cards

- What will we cover today:
  - Payment technologies from the real world
    - EMV (Europay, MasterCard and Visa)
      - EMV-enabled integrated circuit cards & terminals
    - NFC (Near Field Communication)
      - Payment applications of NFC
  - Attacks and countermeasures
    - Classification
    - Known vectors
    - New vectors

Intro: Payment cards

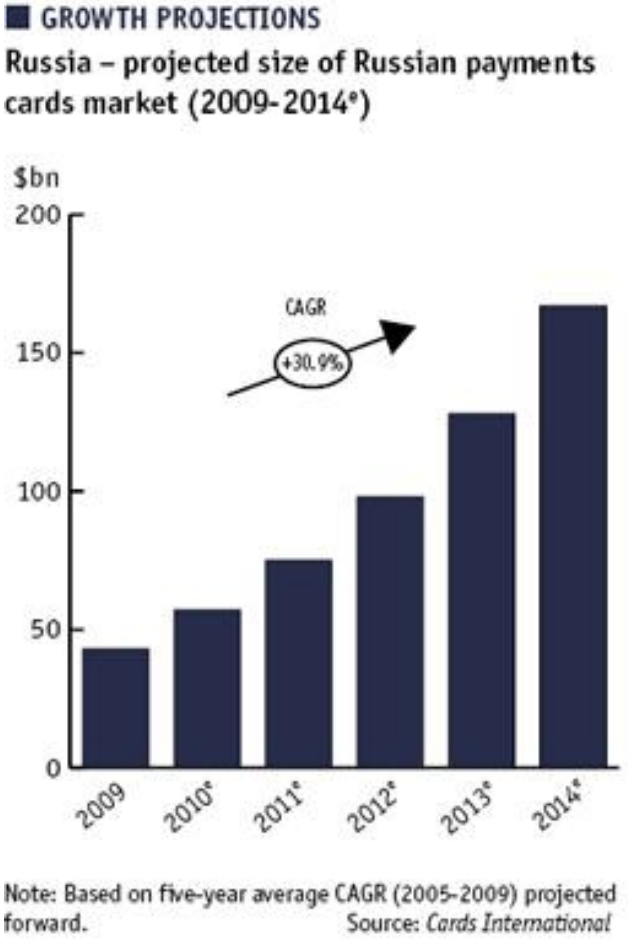
- Why talk about it?
  - Real-world means:
    - Financial institutes – obscure and weird
    - Ubiquity
    - Hardware
    - Attacks in space and time
  - Strict standardization
  - Purely virtual payment technologies are all different and rapidly changing
    - Anyone can implement his own
  - And we are talking about serious business

Intro: Payment cards

- Nilson Report, 2011
  - The total number of purchases on all major worldwide card issuers (American Express, Diners Club, JCB, MasterCard, UnionPay and Visa) increased to a total of 135.33 billion, up 12.1 percent from 2010 on an additional 14.56 billion transactions, the report said.

Intro: Payment cards

- Cards International:
  - Predict 30% annual growth of Russian payment cards market
  - $ 100 Billion by 2012



Intro: Payment cards

- As of early 2011, 1.2 billion EMV cards were deployed across the globe along with 18.7 million EMV terminals (via IBID)
- Over a billion smartphones sold by 2012
- By 2014, 44% of smartphones will be NFC-compatible (via)
- Payment card users in Russia: Spring 2011 to Spring 2012: from 49% to 56% (via GfK Rus).

Intro: Payment cards

- History
  - Origins: 1890s
  - Appearance: 1920s
  - Popularity: Mid XX century
  - 1950: Diners Club
  - 1958: American Express
  - 1958: Bank of America BankAmericards (now Visa)
  - 1966: InterBank Card Association (now MasterCard)
  - 1967: Cash dispencer
  - 1969: First ATM and magnetic stripe

Meet the Card

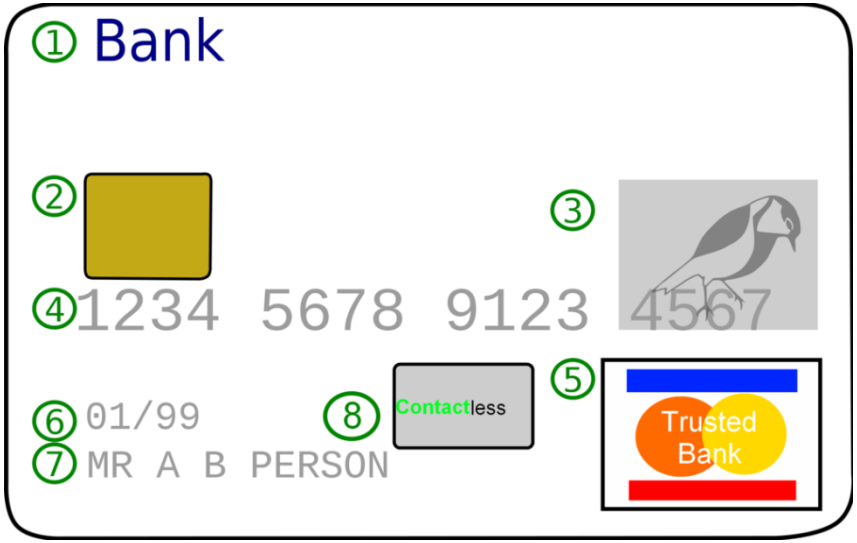
Card standards

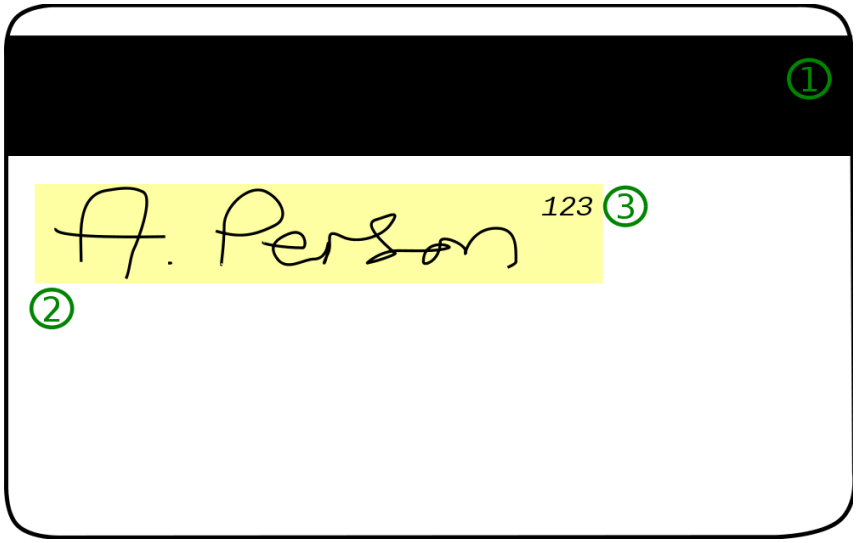
- Standards family ISO/IEC 781X
- 7810: Physical characteristics of credit card size document
- 7811-1: Embossing
- 7811-2: Magnetic stripe–low coercitivity
- 7811-3: Location of embossed characters
- 7811-4: Location of tracks 1 & 2
- 7811-5: Location of track 3
- 7811-6: Magnetic stripe-high coercitivity
- 7813: Financial transaction cards

Card exterior

Front: PAN(4), expiry date(6), Cardholder name(7)

Back: Magnetic stripe (1), cardholder signature(2), CVV2 (2)





PAN

- PAN Personal Account Number
  - From 13 to 19 digits
  - First 4 to 6 digits = BIN
    - Bank identification number
  - Last digit is a checksum digit (Luhn digit)
    - Checksum is calculated with Luhn algorithm

Magnetic Stripe

- LoCo (Low coercitivity)
- HiCo (High coercitivity)
- Tracks
  - Track 1:
  - Track 2:
  - (Track 3) – mostly unused

Magnetic Stripe

Data entity	Track 1	Track2
PAN	+	+
Cardholder name	+	
Expiry date	+	+
Service code	+	+
Discretionary data:		
PVKI	+	+
PVV	+	+
CVC-1 (CVV-1)	+	+

Meet the Terminal

- Terminal types:
  - ATM (Automated Teller Machine)
  - POS (Point Of Sale)
  - Imprinter
  - Others
    - SSD

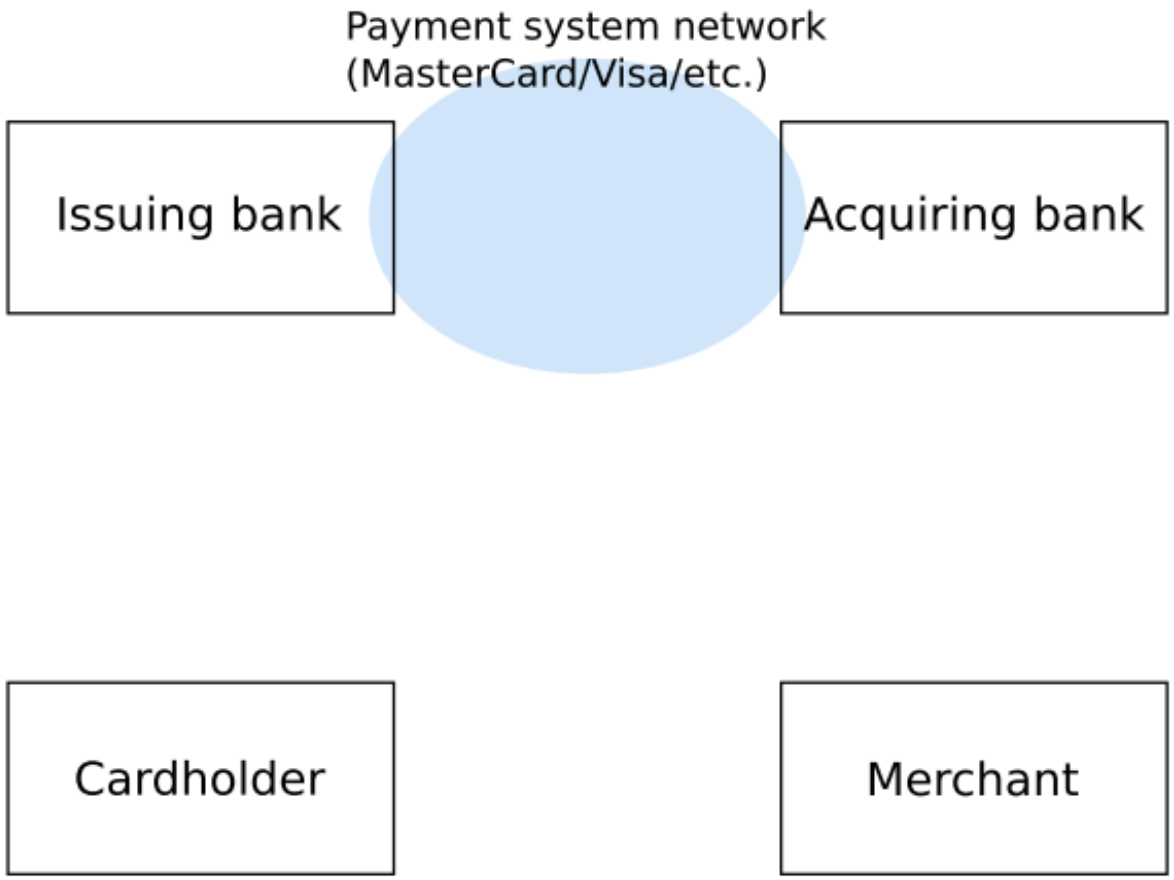
Terminal Hardware

- All devices:
  - Card Reader
  - PED (PIN Entry Device)
  - Receipt printer
  - Screen
- ATM:
  - Note cassettes inside a safe box
  - Note dispencer
  - (Note acceptor)

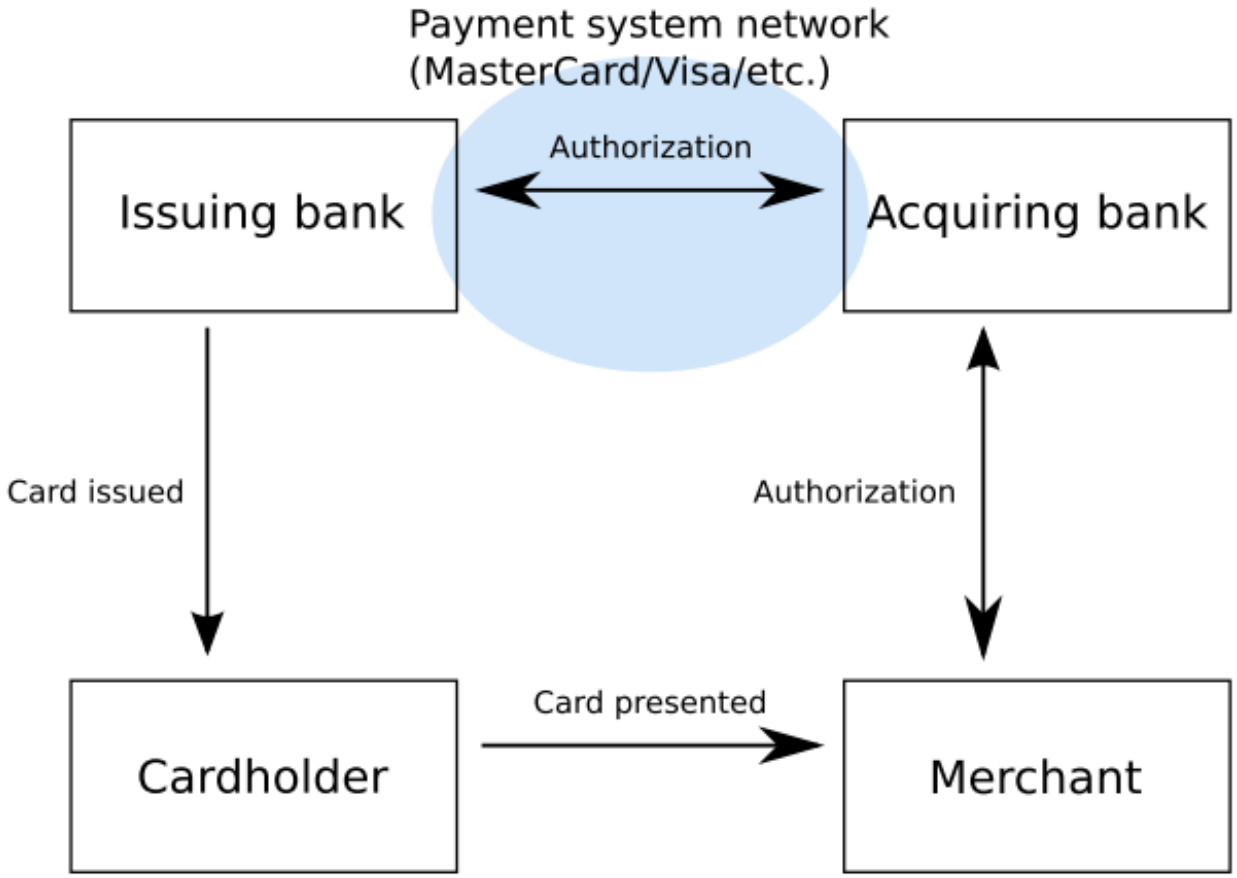
Payment Systems

- Why?
  - If N banks around the world want to accept each other's cards, how many connections they would need? (Hint: $\frac{N(N-1)}{2}$)
- IPS bring standards & interoperability
  - Each IPS defines its own protocols and procedures
- Direct connections are also used
  - Member bank connects directly to the IPS
  - Affiliates connect to the Member
  - IPS can act as an acquirer for the largest retailers

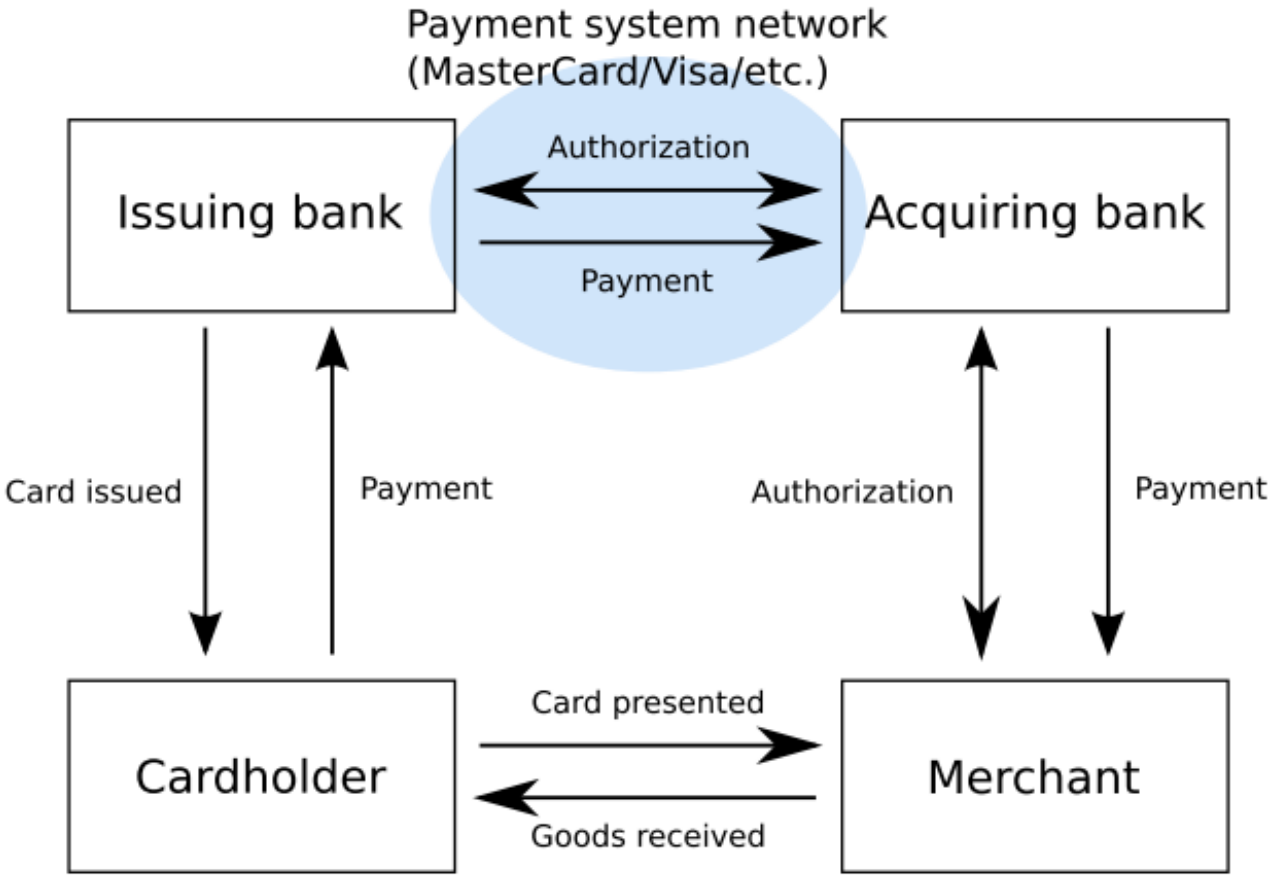
Payment Systems



Payment Systems



Payment Systems



Payment Systems

- Notable IPS (International Payment Systems)
  - Visa
  - MasterCard (MC)
  - Japan Credit Bureau (JCB)
  - Diners Club (DC)
  - American Express (AMEX)
  - China Union Pay (CUP)

Cryptography & Security

- Plastic
  - Holograms
  - Watermarks
- Cryptography
  - DES (Replaced by DES)
  - 3DES
    - 3DES, mode: EDE, 2 keys: ABA

Cryptography & Security

- Cardholder Authentication (Verification)
  - PIN
  - PVK (PIN Verification Key)
  - PVV (PIN Verification Value)
  - PVV = ENC(PVK)[f(PAN, PIN)] by issuer
- Card Authentication (Verification)
  - CVV/CVC and CVV2/CVC2
  - CVK (Card Verification Key)
  - CVV = ENC(CVK)[f(PAN || ExpDate || SvcCode)] by issuer
  - CVV2 = ENC(CVK)[f(PAN || ExpDate || ‘000’)] by issuer

Cryptography & Security

- Encryption
  - PEK (PIN Encryption Key)
  - TPK (Terminal PIN Key)
  - TMK (Terminal Master Key)
  - Domain encryption
    - ZMK/ZCMK (Zone (Control) Master Key)
    - AWK (Acquirer Working Key)
    - IWK (Issuer Working Key)
  - Proprietary measures
    - MAC by terminal
    - Transport-level encryption

Cryptography & Security

- HSM (Host Security Module)
  - Host command interface
  - Console admin interface
    - Smart cards for security officer authetication and master key storage
  - PKCS#11 API
  - LMK (Local Master Key)
  - Standards compliance
    - FIPS 140-1, FIPS 140-2/140-3
- PIN Printer
  - A secure printer directly connected to HSM

Processing cycle

- Cardholder
  - Receive a card and sign it manually
  - Open PIN Envelope, read it and burn it
- Issuer
  - Personalization
  - Embossing
  - Encoding
  - Issuer’s Host software
    - Authorization processing
    - Presentment processing
- Card
  - Card is just a static read-only piece of plastic

Processing cycle

- Acquirer
  - Manages terminals and provides services to merchants
  - Acquirer's host software
    - Authorization processing
    - Presentment processing
- Terminal
  - Reads card
  - Talks to acquirer's host

Processing cycle

- Transaction phases
  - Authorization
  - Clearing
  - Settlement
  - Dispute resolution

Authorization

- Terminal reads card
- If cardholder enters PIN:
  - Terminal calculates a PIN Block inside PED
  - PIN Block is encrypted under corresponding TPK
- Auth message is sent to Acquirer's host
- Acquirer processes it and sends to IPS
- IPS processes it and sends to Issuer
- Issuer approves or rejects it and sends the answer back

Clearing

- Terminal reconciliation
- Acquirer demands satisfaction from the issuer and sends the clearing presentments through the IPS
- IPS processes them and sends them to the Issuer
- Issuer may not respond, money transfer is automatically performed at the next stage

Settlement

- All parties settle their financial positions through the IPS
  - Consolidated funds transfer

Dispute resolution

- **Presentment**: Original Sale
- **First Chargeback**: A customer disputes a charge to his or her credit card company or bank and the bank responds with a retrieval request to dispute the transaction.
- **Second Presentation or Re-presentment**: This is when the merchant has an opportunity to respond to the first chargeback.
- **Second Chargeback**: If the second presentment is rejected by the cardholder, the issuing bank files a second chargeback.
- **IPS Arbitration**: IPS staff handle the case manually

Data transfer

- ISO 8583 Standard
  - Binary protocol
  - Presence of a fields is determined by bitmap
    - N x 64-bit bitmaps
  - Fields may be fixed or variable
  - Data may be encoded in raw binary, ASCII, BCD, etc.
    - The same for variable fields length

Terminal protocols

- Terminals usually talk to acquirer's host in their special protocols
  - ATM
  - POS
  - SSD
- But some are built over ISO8583

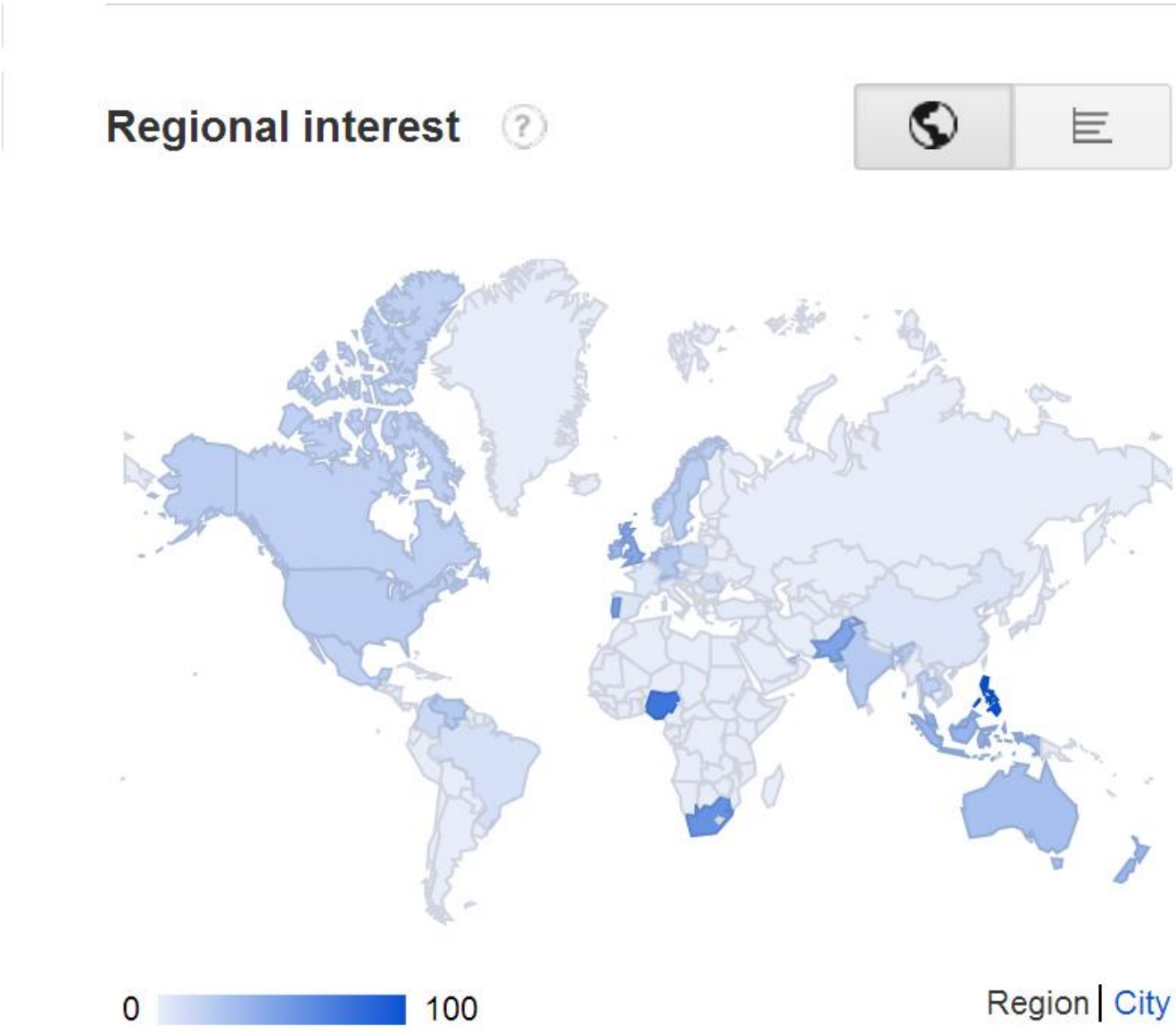
Transaction types

- ATM
- Retail
- CNP Retail
- Note Acceptance
- Special
  - Balance request
  - PIN Set/PIN Change
  - Address Verification

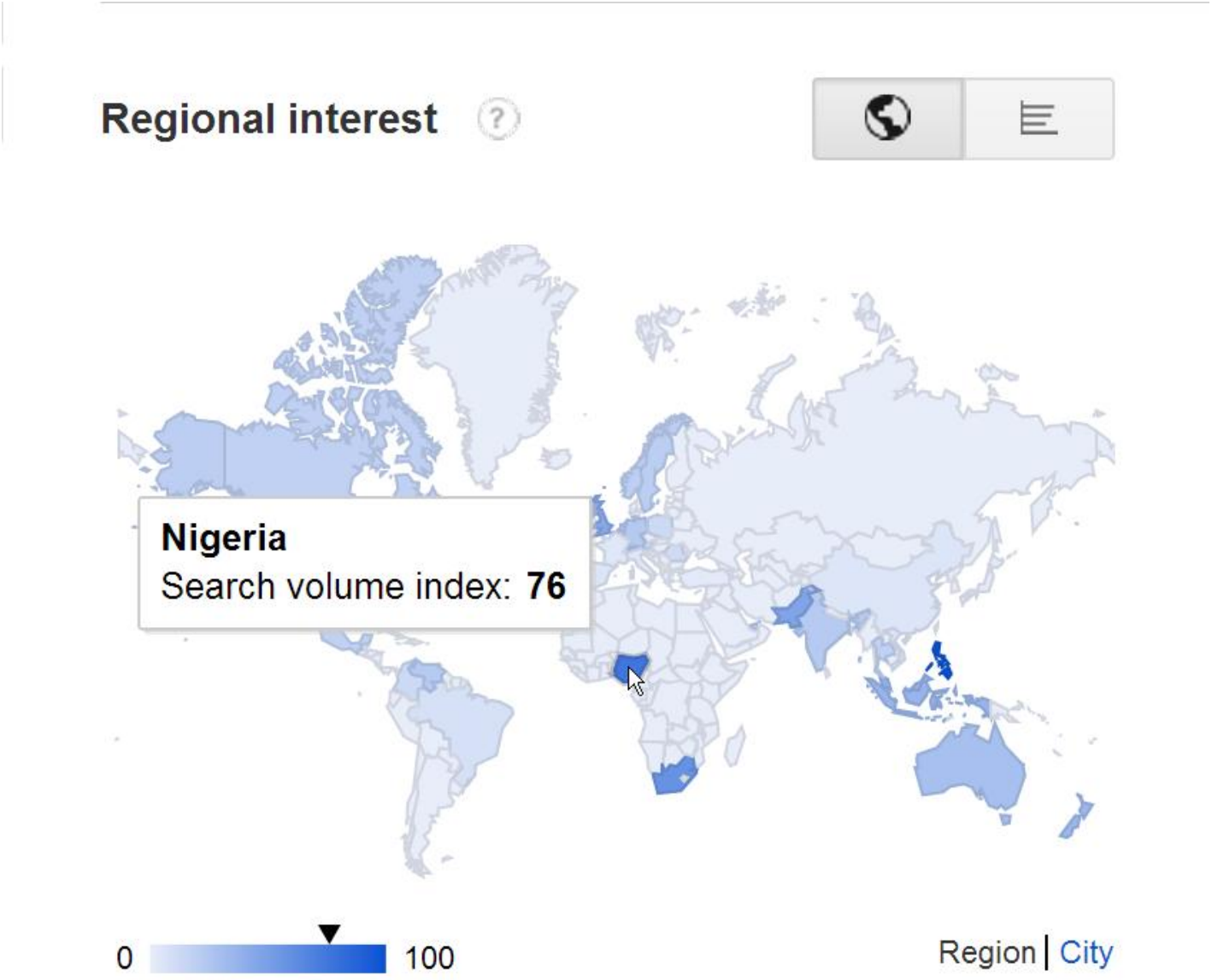
Fraud

- PAN + Exp Date + CVV2 = enough for CNP fraud
  - CNP Fraud
- Skimming
  - Cloning of magstripe with and w/o stealing the PIN
  - Clone is identical to the original card
  - http://www.google.com/trends/explore?#q=skimming
- Other methods

http://www.google.com/trends/explore?#q=skimming



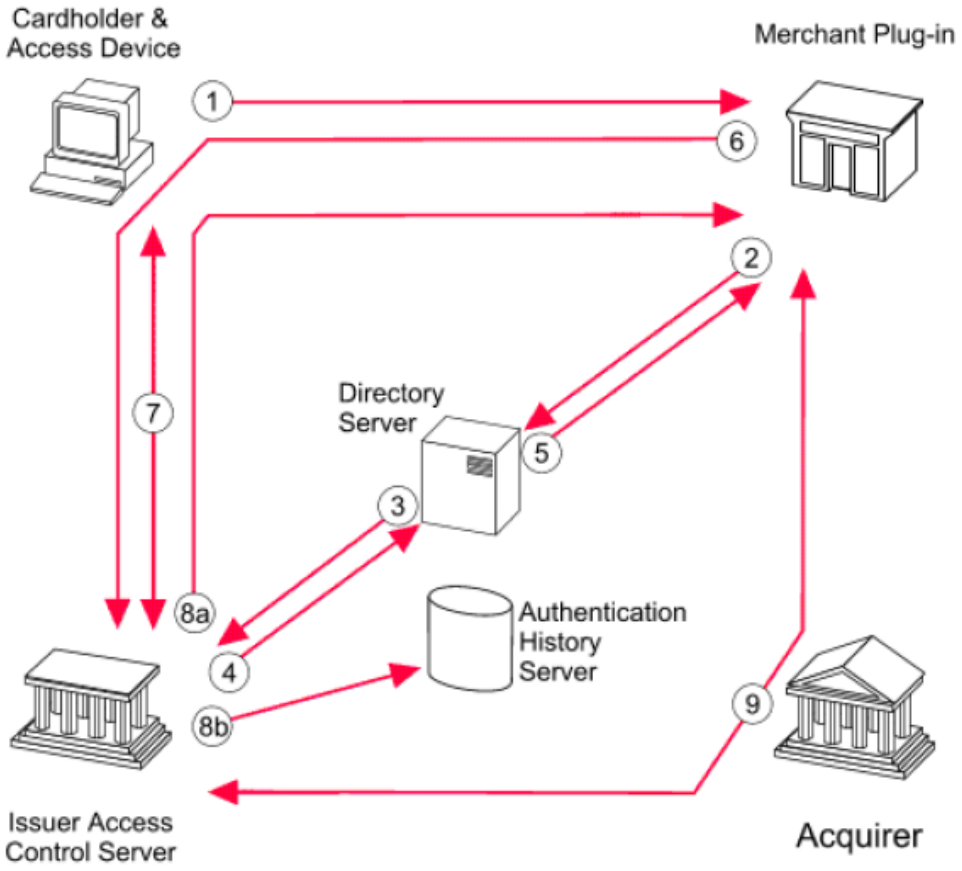
http://www.google.com/trends/explore?#q=skimming



Advances & countermeasures

- DUKPT
  - Derived Unique Key Per Transaction
- Anti-skimming
  - Terminal-only
  - Card and terminal
    - Magstipe is analog, not digital
- e-commerce
  - (SET)
  - 3-D Secure
- Finally, smart cards (ICC)

3-D Secure



(2),(3) – VEReq (PAN)
(4),(5) – VERes (ACS Url)
(6) – PAReq
(8a) – PARes (CAVV)
(9) – ISO 8583 Message
(CAVV)

Modern payments security: EMV, NFC, etc.?

- Intro: Payment Cards
- **The EMV standard**
- Attacks on EMV
- Intro: NFC
- EMV & NFC = ?
- Attacks on EMV & NFC
- Future

The EMV standard

- What?
  - A protected microcontroller inside a card
  - Since 1993
- Why?
  - New interactive products
  - Liability Shift
- The Four Books
  - ICC to Terminal Interface
  - Security and Key Management
  - Application Specification
  - Other Interfaces
- ISO 7816

The EMV standard

- What does the card use:
  - DES/3DES
  - RSA
  - SHA-1
- What does the card have:
  - Several kilobytes of EEPROM
  - Firmware
    - Java Card
    - MultOS
    - …
  - 1 Serial I/O port and a system of commands

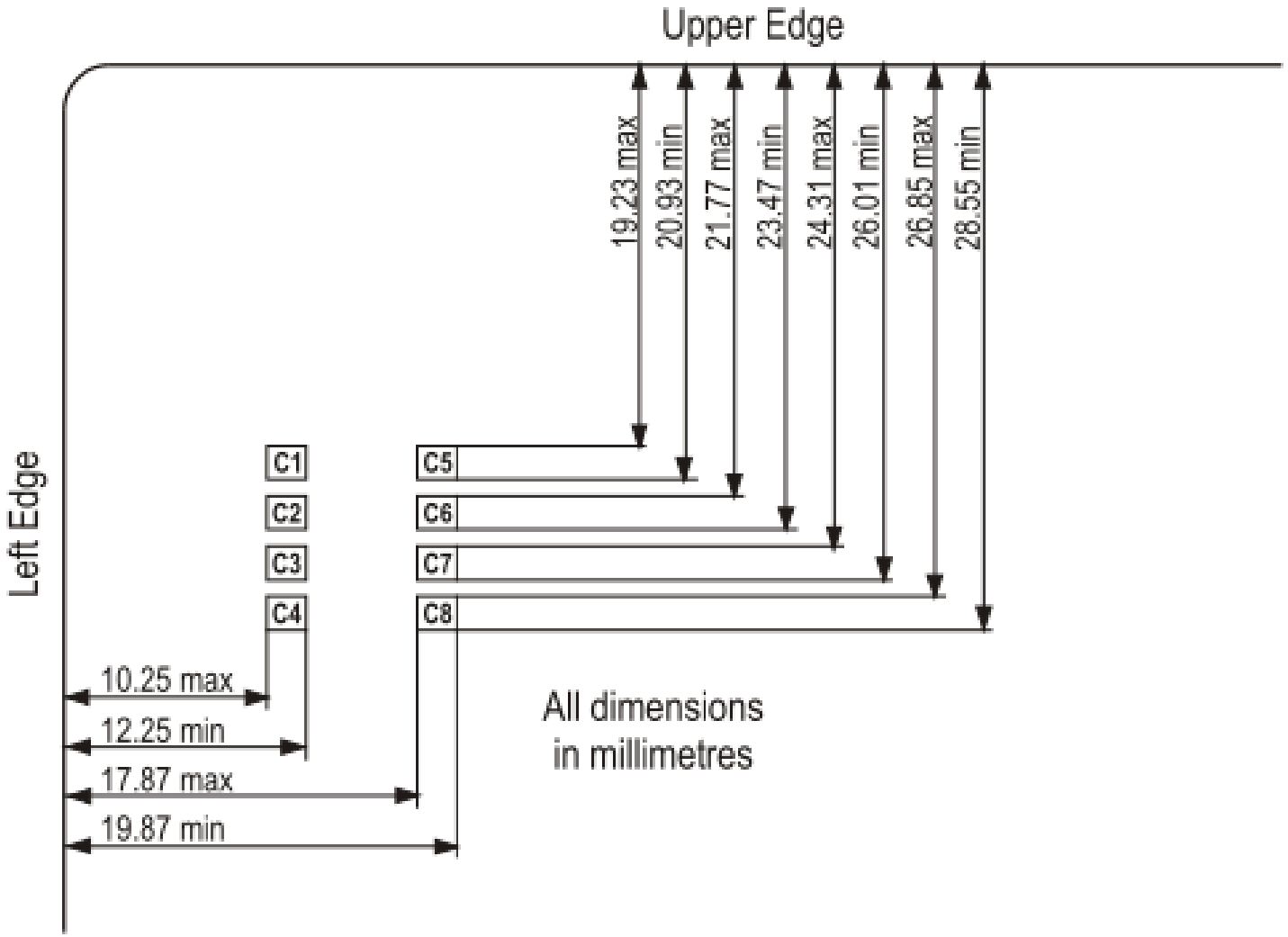
The EMV standard

- EMV Lifecycle
  - EMV Personalization
    - Pre-personalization
  - Interactivity
    - Card makes the decision
    - New cardholder authentication methods
      - Biometrics
    - Issuer scripts and data storage
      - Counters
      - Card-level risk management

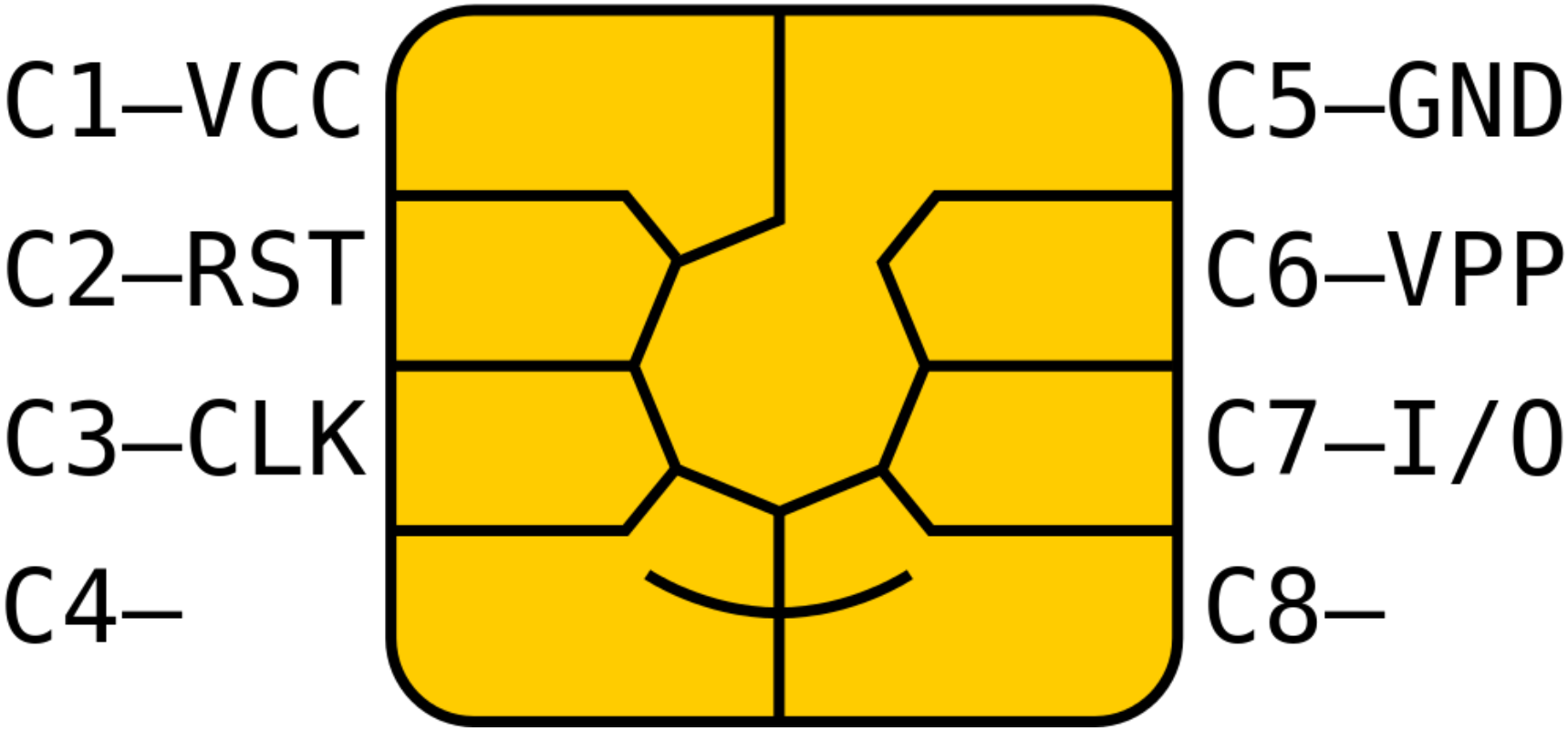
EMV basics

- Physical specs
- I/O
- Files
- Commands
- Applications

Physical specs



Physical specs



Physical specs

Symbol	Conditions	Minimum	Maximum	Unit
V_{CC}	Class A Class B Class C	4.50 2.70 1.62	5.50 3.30 1.98	V
I_{CC}	Class A Class B Class C		50 50 30	mA
The maximum current consumptions shown apply when operating at any frequency within the range specified in section 5.3.4.				

Supported Classes	ICC Shall Operate	ICC May Operate	Unit
A and B	4.50–5.50 2.70–3.30	3.30–4.50	V
A, B, and C	4.50–5.50 2.70–3.30 1.62–1.98	3.30–4.50 1.98–2.70	V

- Voltage: 3 classes of operation
  - A
  - B
  - C

I/O

- Insertion of the ICC into the IFD
  - connection and activation of the contacts.
- Reset of the ICC
  - establishment of communication between the terminal and the ICC.
- Execution of the transaction(s).
- Deactivation of the contacts and removal of the ICC

I/O

- Contact activation
  - Vcc level validation for 200 cycles
- ICC Reset
  - Cold
    - > 200 cycles and pull up RST
  - Warm
    - > 200 cycles, pull down RST, > 200 cycles, pull up RST

I/O

Rx (Card to Terminal)

Symbol	Conditions	Minimum	Maximum	Unit
V_{IH}		0.7 x V_{CC}	V_{CC}	V
V_{IL}		0	0.8	V
t_R and t_F		—	1.0	µs
The ICC shall not be damaged by signal perturbations on the I/O line in the range –0.3 V to V_{CC} + 0.3 V.				

class A cards until end December 2013; see Table 1

Symbol	Conditions	Minimum	Maximum	Unit
V_{IH}		0.7 x V_{CC}	V_{CC}	V
V_{IL}		0	0.2 x V_{CC}	V
t_R and t_F		—	1.0	µs
The ICC shall not be damaged by signal perturbations on the I/O line in the range –0.3 V to V_{CC} + 0.3 V.				

new card values from January 2014; see Table 1

Tx (Terminal to Card)

Symbol	Conditions	Minimum	Maximum	Unit
V_{OH}	–20 µA < I_{OH} < 0, V_{CC} = min.	0.7 x V_{CC}	V_{CC}	V
V_{OL}	0 < I_{OL} < 1 mA, V_{CC} = min.	0	0.4	V
t_R and t_F	$C_{IN\ (terminal)}$ = 30 pF max.	—	1.0	µs

class A cards until end December 2013; see Table 1

Symbol	Conditions	Minimum	Maximum	Unit
V_{OH}	–20 µA < I_{OH} < 0	0.7 x V_{CC}	V_{CC}	V
V_{OL}	Class A: 0 < I_{OL} < 1 mA	0	0.08 x V_{CC}	V
	Classes B and C: 0 < I_{OL} < 0.5 mA	0	0.15 x V_{CC}	
t_R and t_F	$C_{IN\ (terminal)}$ = 30 pF max.	—	1.0	µs

new card values from January 2014; see Table 1

Files

- All data on card is stored as records listed in files
- Mandatory
  - Application Expiry Date
  - Application Primary Account Number (PAN)
  - Card Risk Management Data Object List 1 (CDOL1)
  - Card Risk Management Data Object List 2 (CDOL2)
- Application Elementary Files
  - Referenced by SFI
  - Contain only BERTLV data objects

Commands

- Command APDU
  - CLA = Class Byte of the Command Message
  - INS = Instruction Byte of Command Message
  - P1 = Parameter 1
  - P2 = Parameter 2

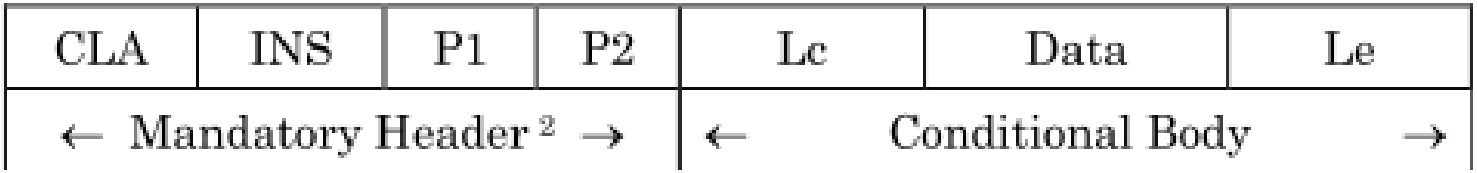


Figure 1: Command APDU Structure

Response

- Response APDU
  - Status bytes
    - SW1
    - SW2

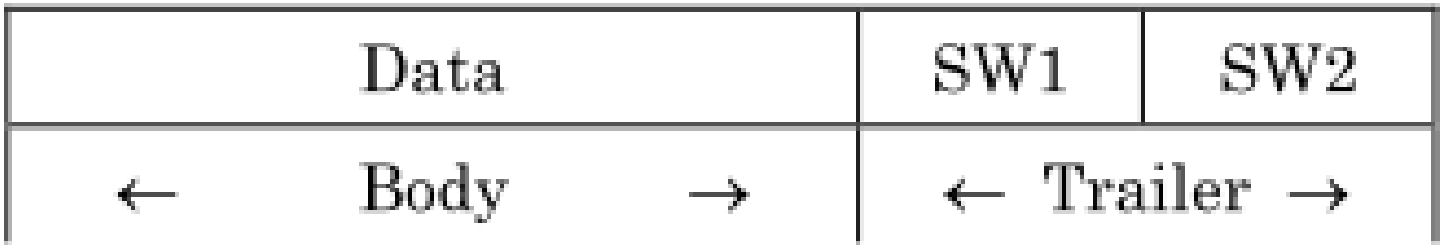


Figure 2: Response APDU Structure

Commands

- APPLICATION BLOCK (post-issuance command)
- APPLICATION UNBLOCK (post-issuance command)
- CARD BLOCK (post-issuance command)
- EXTERNAL AUTHENTICATE – verify a cryptogram
- GENERATE APPLICATION CRYPTOGRAM
- GET CHALLENGE
- GET DATA
- GET PROCESSING OPTIONS
- INTERNAL AUTHENTICATE – calculation of SDA
- PIN CHANGE/UNBLOCK (post-issuance command)
- READ RECORD
- VERIFY – verify PIN data

EMV crypto primitives

- MK_{AC} that it shares with the issuer, derived from the issuer's master key MK_I .
- Session key SK_{AC} can be computed, based on the transaction counter.
- The issuer has a public-private key pair (P_I , S_I), and the terminal knows this public key P_I
- Cards that support asymmetric crypto also have a public-private key pair (P_{IC} , S_{IC}).

EMV Transaction Flow

- Initialization
- Card/Data authentication – optional
- Cardholder verifiifcation – optional
- Actual transaction step

Initialization

- Command flow
  - T → C: SELECT APPLICATION
  - C → T: [PDOL]
  - T → C: GET PROCESSING OPTIONS [(data specified by the PDOL)]
  - C → T: (AIP, AFL)
  - Repeat for all records in the AFL:
  - T → C: READ RECORD (i)
  - C → T: (Contents of record i)
- Return AFL and AIP

Card/Data authentication

- SDA (Static Data Authentication)
  - Card provides Signed Static Application Data (SSAD)
- DDA (Dynamic Data Authentication)
  - SDA + Sign(S_{IC})[ICC Dynamic Data, Hash(ICC Dynamic Data, data specified by DDOL)]
- CDA (Combined Data Authentication)
  - SDAD = Sign(S_{IC})[nonce_IC , CID, AC, TDHC, H(nonce_IC , CID, AC, TDHC, nonce_Terminal].

Cardholder verification

- CVM (Cardholder Verification Methods)
  - CVM List
- Online PIN
  - the bank checks the PIN
- Offline plaintext PIN
  - the chip checks the PIN
  - PIN is transmitted to the chip in the clear form
- Offline encrypted PIN
  - chip checks the PIN
  - PIN is encrypted before it is sent to the card

Offline plaintext PIN

- T → C: VERIFY(pin)
- C → T: Success/ (PIN failed, tries left) / Failed

Offline encrypted PIN

- T → C: GET CHALLENGE
- C → T: nonce_IC
- T → C: VERIFY(Encrypt (*PIC*)[PIN, nonce_IC , random padding])
- C → T: Success/ (PIN failed, tries left) / Failed

Transaction step

- Offline
  - card sends a Transaction Certificate (TC)
- Online
  - card sends an Authorisation Request Cryptogram (ARQC)
  - If issuer approves, card sends a TC
- If card itself refuses
  - Card provides Application Authentication Cryptogram (AAC)

Modern payments security: EMV, NFC, etc.?

- Intro: Payment Cards
- The EMV standard
- **Attacks on EMV**
- Intro: NFC
- EMV & NFC = ?
- Attacks on EMV & NFC
- Future

Attacks on EMV

- Classification
  - Hardware vs. Software
  - Active vs. Passive
  - Intrusive vs. Non-intrusive
  - By localization:
  - By methods used

Attacks on EMV

- Classification
  - By localization:
    - Malicious card
    - Malicious terminal
    - MITM

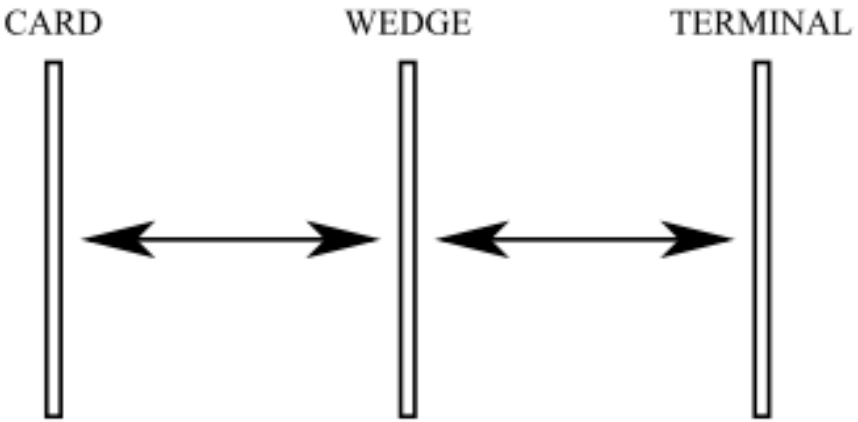
Attacks on EMV

- Classification
  - By methods used
    - Communication lines eavesdropping & tampering
    - Purely cryptoanalytical methods
    - Fault attacks
    - Side-channel attacks
      - Power analysis
        - » SPA (Single Power Analysis)
        - » DPA (Differential Power Analysis)
        - » DFA (Differential Fault Analysis)
      - TAA (Timing Analysis Attack)
    - Social Engineering

Known vectors

- Fallback to magstripe
- Relay attacks
- Replay attacks (“YES”-cards = clones of SDA card)
- MITM (Wedge) with CVM list downgrade
- Pre-play attack
- Joint encryption and signature
- Fault analysis
- Power analysis
- Attacking HSM's

MITM (Wedge) with CVM list downgrade



- Terminal might not check if authentication method is the same that the card approved
  - Only auth result is signed
- Make the card think it was a signature-based transaction
- Make the terminal think it was a PIN-based transaction
- Easily prevented
  - by correct terminal software
- Detected at host

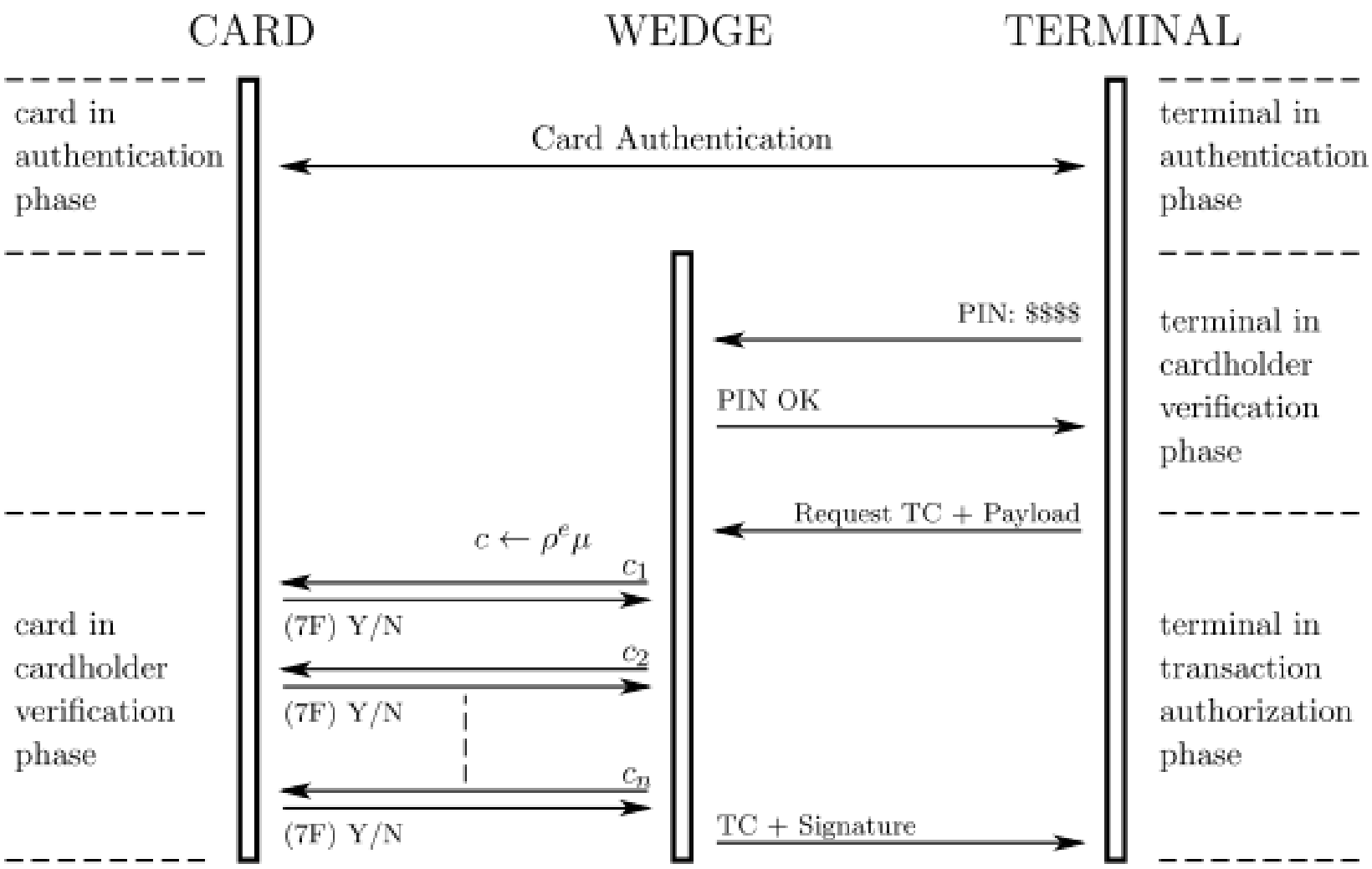
Pre-play attack

- Bond et al., Cambridge, 2012
- Random nonce sent by terminal?
- In reality it is not so random
  - Older implementations
- So a MITM device can gather a lot of cryptograms for known nonces
- Then just predict when this cryptogram will be correct and use it with fake transaction data

Joint encryption and signature attack

- Degabriele et al., CT-RSA 2012
- CDA cards
- Offline transaction, card verifies PIN
- Utilize known padding of encrypted EMV data
  - Bleichenbacher attack on RSA
- Same RSA keypair used for signature and encryption

Joint encryption and signature



Fault analysis

- Coron et al., CT-RSA 2010
- Currently CRT (Chinese Remainder Theorem) is used to reduce computational load on signer in RSA implementations
  - From *mod N* to *mod p* and *mod q*
  - Fault induced on one computation of two
  - "CJKNP" attack on RSA, 2009
    - Partially unknown plaintexts
- Consider EMV DDA:
  - Signed data includes partially known ASN.1 header
  - Attack uses orthogonal lattice techniques
  - Attack requires 10 faulty signatures to factor N under 1 second

Attacking HSM's

- EMV introduced new crypto primitives to be implemented on existing, non-flexible systems with decades of backward compatibility
  - The new crypto functions may have been implemented improperly
- An attack by Ben Adida et al. and Ron Rivest (2005) on 3DES CBC MAC
  - Inject chosen plaintext in the MAC'ed message
  - Disclose encryption key
  - Two implementations
    - IBM 4758
    - Thales RG7000
- Modern systems are not vulnerable

Countermeasures

- Technical
  - Improve terminal software (!)
  - Improve host software
  - Improve personalization restrictions
    - Obey payment systems' regulations
  - Distance Bounding
    - Saar Drimer and Steven J. Murdoch, Cambridge
  - Cardholder self-defence
    - Steven J. Murdoch, Cambridge
    - Invent an "Electronic attorney" – legitimate cardholder's shim (!?)
- Organizational
  - Verify from the business level
  - Improve standards coverage

Future

- Elliptic curves
  - ECIES (ISO/IEC 18033-2) for PIN
  - EC-DSA / EC-Schnorr (ISO/IEC 14888-3:2006) for signatures
- More complex chip applets
  - More authentication schemes
    - Interactive cards with keyboard and display
  - More bugs?
- Fast and more expensive ICC chips
  - Stronger crypto
  - Difficult and less practical hardware attacks

Modern payments security: EMV, NFC, etc.?

- Intro: Payment Cards
- The EMV standard
- Attacks on EMV
- **Intro: NFC**
- EMV & NFC = ?
- Attacks on EMV & NFC
- Future

Intro: NFC

- RFID – Radio Frequency Identification technologies
  - LF (Low frequency)
    - 125 KHz
    - 134 KHz
  - HF (High frequency)
    - 13.56 MHz
      - NFC
        - » ISO/IEC 18092 (ECMA-340)
        - » ISO/IEC 14443
        - » ISO/IEC 15693
  - Others

NFC

- NFC Devices
  - Tags
  - Smart cards
  - Readers
  - Mobile devices
- NFC Security
  - NFC Ready and NFC Secure
  - Secure Element
  - Authentication
  - Encryption

NFC Data Transfer

- NFC Roles by RF field source:

Device A	Device B	Description
Active	Active	RF field is generated by the device that sends data at the moment
Active	Passive	RF field is generated by Device A only
Passive	Active	RF field is generated by Device B only

- NFC Roles by protocol:

	Initiator	Target
Active	Possible	Possible
Passive	Not Possible	Possible

NFC Device Modes of Operation

- Data exchange (P2P – NFC peer-to-peer)
  - Duplex data exchange
  - WiFi, Bluetooth, P2P Payment, Contacts, vCards, …
- Reader/Writer mode (PCD – Proximity Coupling Device)
  - Mobile device reads tags/smartcards
  - WiFi Config, media linking
- Tag emulation (PICC – Proximity Card)
  - Reader cannot distinguish between smartcard & tag emulation
  - Handset may contain/emulate multiple smartcards (smartcard chips)

NFC Security

- Eavesdropping is easy (up to 10 meters in active mode)
- DoS is easy
- Datastream modification is possible
- MITM is possible using full relay (when Alice and Bob can not talk to each other at all)
  - No NFC shims, unless some RF-shielding nano-materials appear :)
  - A fast relay is a **practical** attack both for eavesdropping and data tampering
- Secure element
- Additional levels of security are out of scope of NFC standards
  - Proprietary implementations

Secure element

- Smart Card Alliance: *"The secure element (SE) is a **secure microprocessor (a smart card chip)** that includes a cryptographic processor to facilitate transaction authentication and security, and provide secure memory for storing payment applications (e.g., American Express, Discover, MasterCard, Visa and other payment applications). SEs can also support other types of secure transactions, such as transit payment and ticketing, building access, or secure identification."*

Secure element

- Secure elements in consumer devices
  - Contactless smart card
  - NFC SIM card + Handheld device
    - RF interface on handheld
    - Integrated RF interface
    - Flexible antenna
  - NFC SD Card + Handheld device
    - RF interface on handheld
    - Integrated RF interface
  - SE Embedded in a chip in a handheld device
    - RF interface on handheld

NFC Security

- Secure Element is as secure as a regular (contactless) smartcard
  - Same security features
  - Same weaknesses
    - Side channels
  - Main weakness: Relay attack
    - Cannot be prevented by application-layer cryptographic protocols
    - Timing requirements by ISO 14443 are too loose to prevent relay over longer channel
      - Real devices may be even more relaxed to produce less timeouts in real life for the customers

NFC Reality

- Mifare
  - Proprietary near-ISO compliant cards by Philips (NXP)
  - Worldwide deployment
    - European transport: subways, intercity trains...
    - Asia, South America, ...
    - Ski passes at modern ski resorts
    - ... finally, Moscow & Saint-Petersburg subway tickets

NFC Reality

- Mifare security
  - MIFARE Ultralight – no encryption
  - Mifare Classic
    - Uses a weak crypto algorithm “Crypto-1”, 48-bit key
    - First attacks in 2000’s
    - Algorithm fully reverse-engineered from chip by 2008
      - Insecure, minutes to retrieve secret key and fully clone card
  - Mifare DESFire
    - 3DES / AES
    - Successful DPA attack on 3DES Mifare DESFire in 2011

NFC Reality

- Vulnerable smartphones
  - Various
    - Attacks on NFC P2P
    - JSR-177
  - Android
    - Currently deployed custom stacks and drivers
    - Linux standard NFC stack
    - Userland vulnerabilites on handling NFC data

Modern payments security: EMV, NFC, etc.?

- Intro: Payment Cards
- The EMV standard
- Attacks on EMV
- Intro: NFC
- **EMV & NFC = ?**
- Attacks on EMV & NFC
- Future

EMV & NFC = ?

- EMV & NFC = ?
  - EMV-compliant chip is a secure element
  - So we have contactless payment cards:
    - Visa PayWave
    - MasterCard PayPass
    - etc.
  - Mostly: dual interface (contacts + coil) for backward compatibility (some even have magstripe)
  - Personalized by contact and contactless interfaces alike
  - New threats

EMV & NFC = ?

- Low-amount payments with little to no cardholder verification
  - Local transport tickets
  - Small retail purchases
  - Even cash withdrawal
  - …
- An EMV card embedded inside a smartphone
  - Total payment convergence
  - Smartphone’s screentouch screen
  - Multi-application EMV

Modern payments security: EMV, NFC, etc.?

- Intro: Payment Cards
- The EMV standard
- Attacks on EMV
- Intro: NFC
- EMV & NFC = ?
- **Attacks on EMV & NFC**
- Future

Attacks on EMV & NFC

- Known vectors
  - PAN Gathering for subsequent CNP online fraud
    - Fake point-of-sale device
  - Relay attacks
    - Two NFC-enabled smartphones
- New vectors
  - Power analysis
  - Smartphones

Known vectors

- PAN Gathering for subsequent CNP e-commerce fraud
  - Fake point-of-sale device, e.g. selling candies
  - Customers pays with his card
  - Card details are used in CNP e-commerce fraud
- Relay attacks
  - Two NFC-enabled smartphones
  - Implements known EMV attacks using the relay

New vectors

- Power analysis
  - Card draws power from the same RF field that is used for data transfer
- Smartphones
  - Direct access to secure element
  - Consider all those rooted Androids…

Modern payments security: EMV, NFC, etc.?

- Intro: Payment Cards
- The EMV standard
- Attacks on EMV
- Intro: NFC
- EMV & NFC = ?
- Attacks on EMV & NFC
- **Future**

Future

- Industry strengths
  - ~~Security by obscurity~~
- Industry weaknesses
  - Security by obscurity
- New technology
  - Stronger cryptography
- Perspectives
  - EMV
  - NFC
  - etc.?


?
ZERO
NIGHTS
DCG * 7812