Cryptography in Payment Systems

A Brief Introduction into Payment Cards' Security

SEAMS-UGM-ITB Summer Course on Coding Theory and Cryptography

Jakub Breier (jbreier@ntu.edu.sg)
Nanyang Technological University
Singapore

26 July 2019

Outline

- History of Payment Cards
- EMV Transactions
- EMV Certification Process
- Side-Channel Attacks on EMV Cards

Payment Card

- *Payment cards* are part of a payment system issued by financial institutions, to a customer that enables its owner (the cardholder) to access the funds in the customer's designated bank accounts, or through a credit account and make payments by electronic funds transfer and access automated teller machines (ATMs)[1].
- Further divided into:
  - Credit card
  - Debit card
  - Charge card
  - ATM card
  - Stored-value card
  - Fleet card

Source: The Guardian

1. About-Payments.com – Card Payments

Early Days

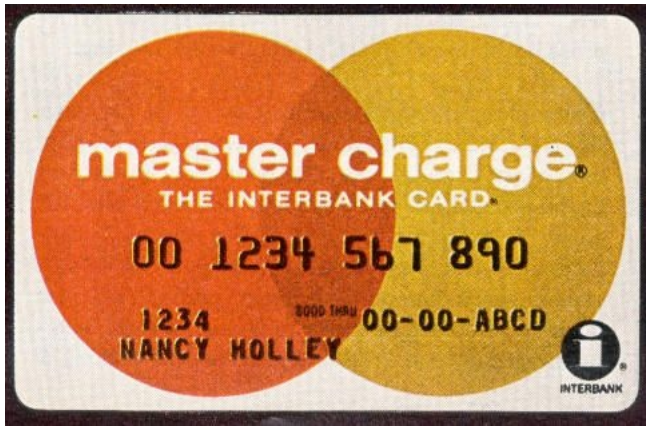
- 1949 – establishment of Diners Club – Frank McNamara was dining with his friends and realized he forgot his wallet
- 1951 – Diners membership reaches 42,000 as it expands to major US cities
- 1958 – Bank of America issues BankAmericard, which is the first credit card. Later that year American Express issues its first credit card
- 1959 – first embossed card (Amex)
- 1960 – IBM introduces mag-stripe – it takes 10 years to adopt it commercially

Source: Diners Club International

Source: Smithsonian National Postal Museum

Early Days

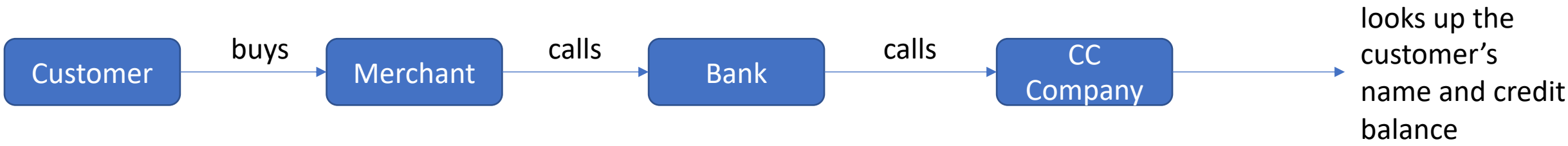
- 1966 – a group of banks establishes Master Charge to compete with BankAmericard
- 1970 – approximately 100 million credit cards have been issued in US
- 1973 – transaction system becomes computerized
- 1976 – BankAmericard licenses unite under the common brand – Visa



Source: DemocraticUnderground.com

Source: USAePay

First Credit Card Transactions



- Books with lists of stolen card numbers were distributed to merchants
- It was common to accept a charge below some threshold value without calling the bank
- Merchants that did not follow the verification procedures were liable for fraudulent charges
- Because of the cumbersome nature of the verification, merchants often assumed the risk of smaller transactions

Magnetic Stripe Transactions

- Similar procedure to classic tapes – instead of machine rotating the tape, card is swiped by hand
- The magstripe is made up of tiny iron-based magnetic particles in a plastic-like film
- There are three tracks on the magstripe, normally only 2 are used
- Following information is typically stored:
  - encrypted PIN,
  - country code,
  - currency units,
  - amount authorized

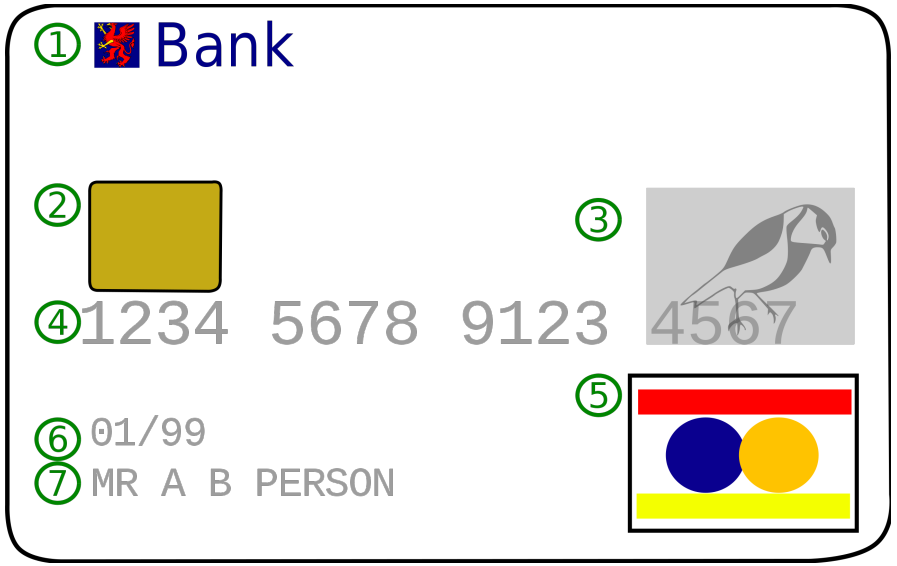
Source: ID Card Group

Security Issues

- Merchant had to verify the card
- If the transaction did not take place near the terminal (e.g. in a restaurant), the clerk had to take the card away. Dishonest employee could swipe the card through a cheap machine that instantly recorded the information on the card and stripe.
- Even at the terminal, a thief could bend down in front of the customer and swipe the card on a hidden reader
- This made illegal cloning of cards relatively easy, and a more common occurrence than before.

EMV in Europe

- Call verification from Europe to USA was expensive – another way to verify the transaction was demanded
- 1993 – Europay, MasterCard and Visa establish EMV, later joined by Discover, JCB, UnionPay and American Express to form EMVCo
- 1994 – the first EMV system is released in Europe



Source: Wikimedia Commons

1. Issuing bank logo
2. EMV chip
3. Hologram
4. Card number
5. Card brand logo
6. Expiration date
7. Cardholder's name

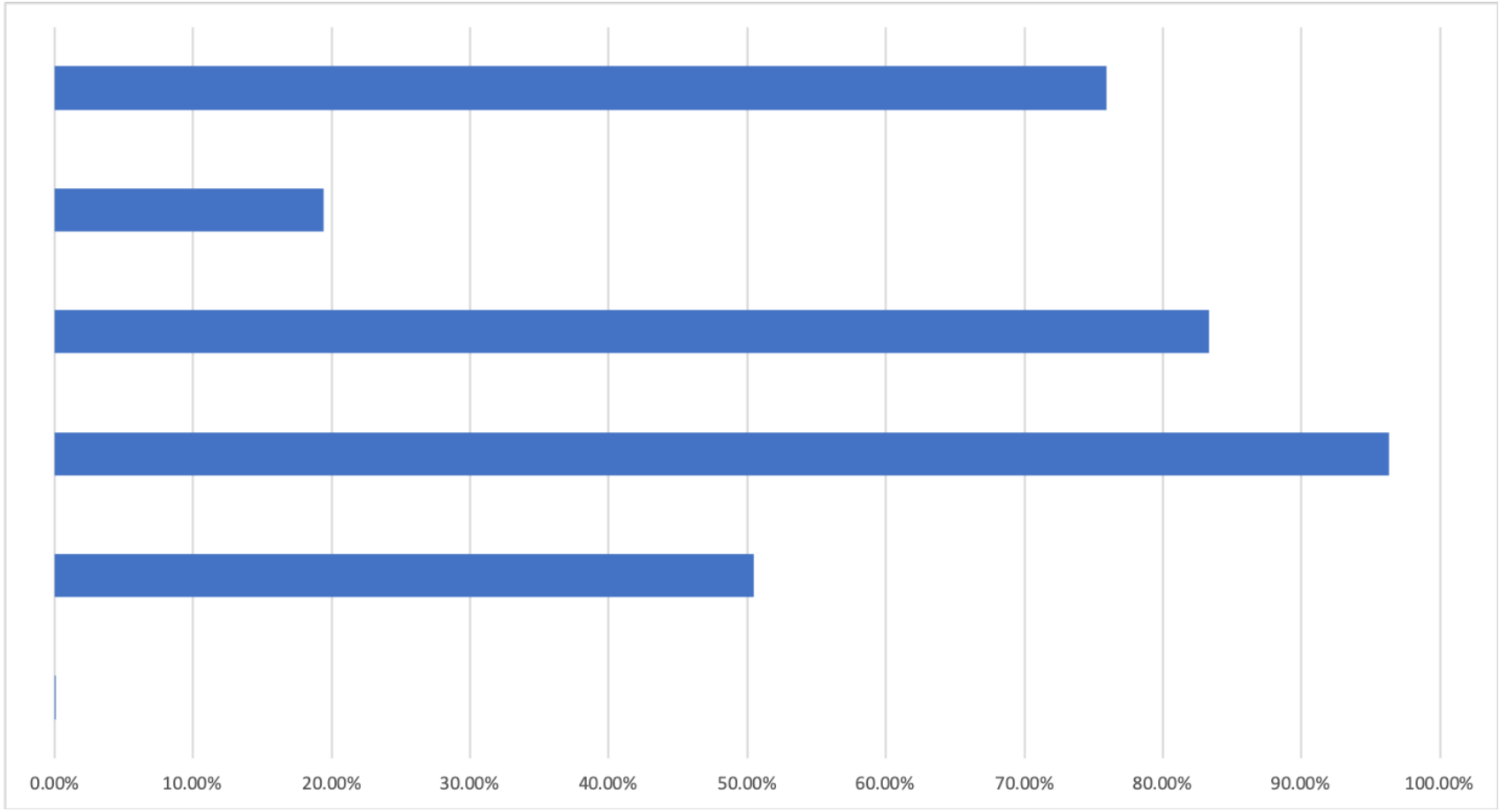
Source: EMVCo

EMV in USA

- Between 2004 and 2010, fraud using US-issued bank credit cards rose 70%.
- And in 2012 credit card losses in the United States totaled $5.33 billion, an increase of 14.5% from 2011.
- US began its massive migration to EMV only in 2014-2015.
- US is already seeing a 43 percent reduction of counterfeit fraud at chip-enabled merchants.
- All of the major card brands (Visa, MasterCard, American Express, and Discover) have shifted the liability for counterfeit card fraud losses, which used to be held largely by card issuers, to merchants and their acquirers unless both parties implement EMV (since 2015).

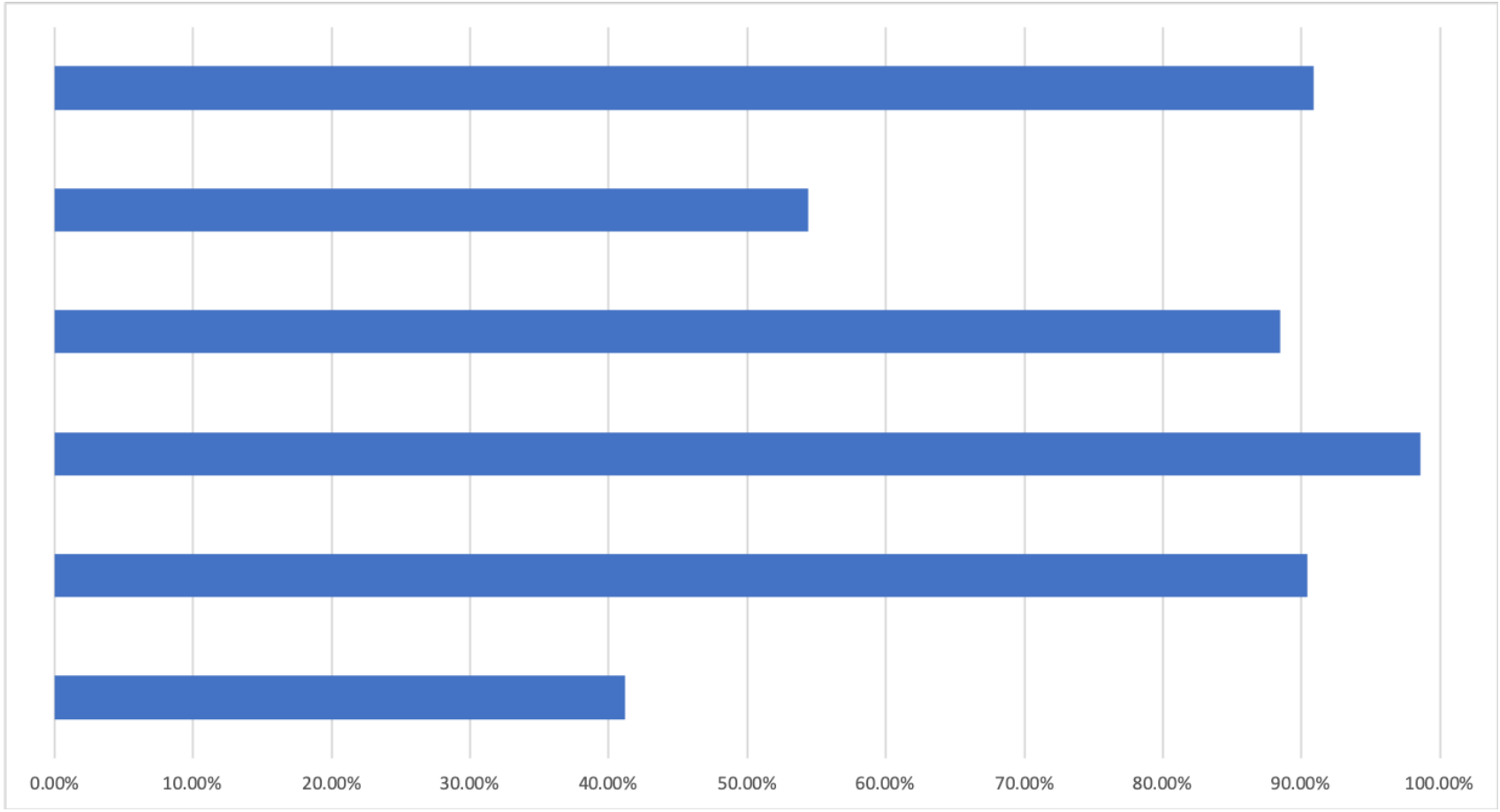
Source: Gemalto.com

Percentage of EMV transactions in 2014



Source: EMVco

Percentage of EMV transactions in 2017



Source: EMVco

Summary – Authentication Methods

Source: Elite Card Processing

1959 – embossing

Source: The Kiosk Simple Blog

1970 – mag-stripe

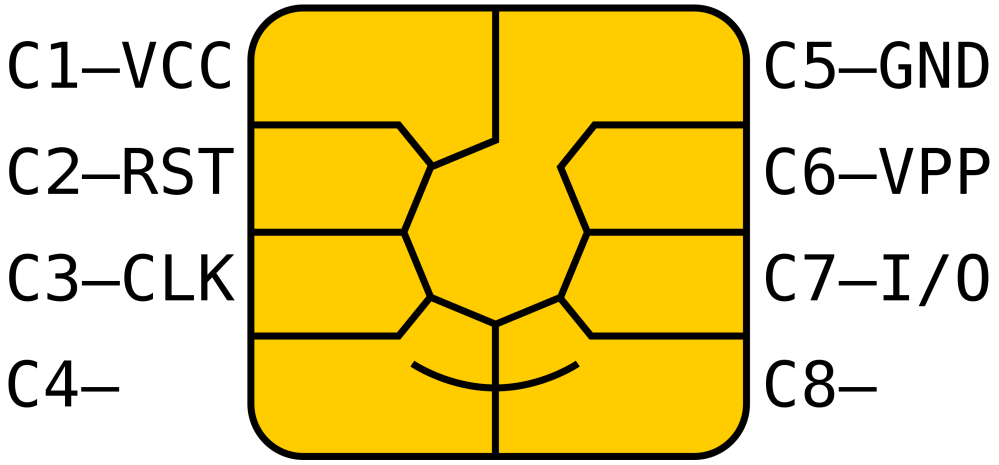
Source: Bancard Payment Systems

1993 – EMV

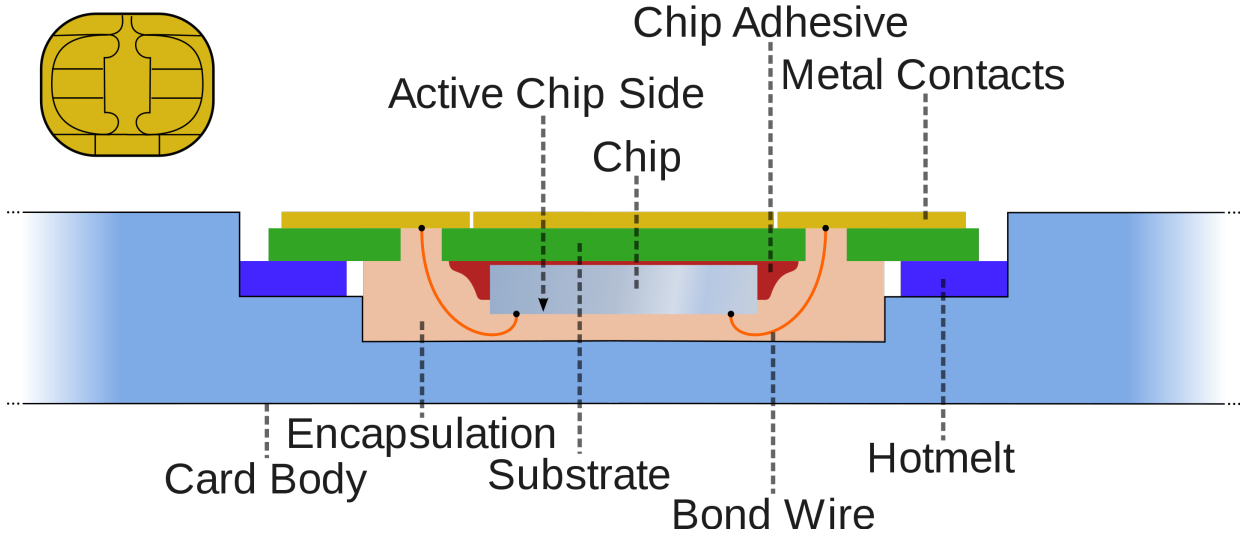
EMV Transactions

Benefits of EMV

- Security – usage of cryptography – TDES, RSA, SHA
- Multiple applications – credit, debit, transport, etc.
- Cloning of the card is not possible anymore



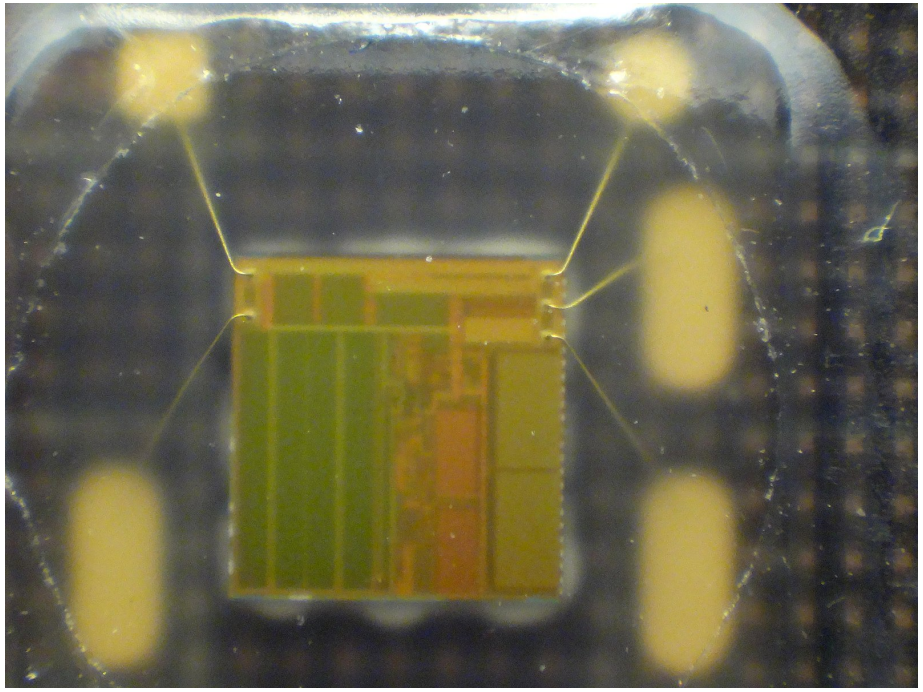
Source: Dacs, WhiteTimberwolf, Wikimedia Commons



Source: Justin Ormont, Wikimedia Commons

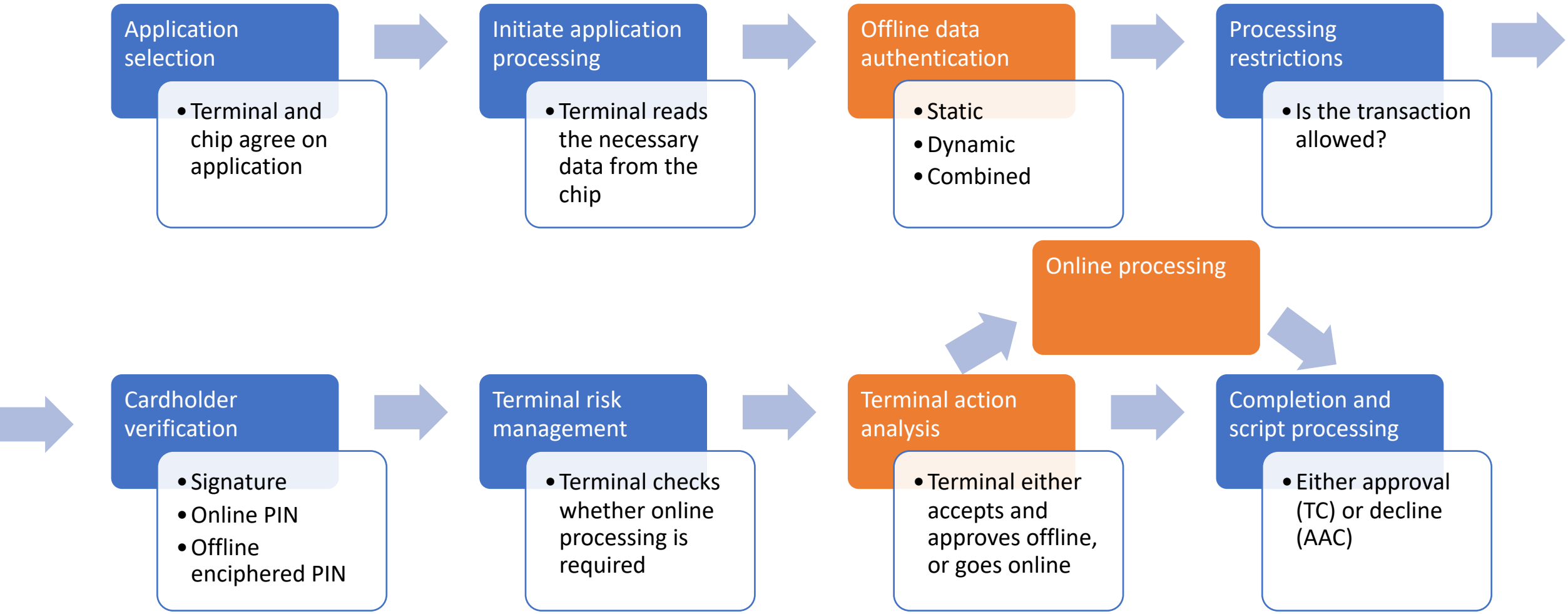
EMV Card is a Smart Card

- It contains embedded integrated circuit according to ISO/IEC 7810 and ISO/IEC 7816 series of standards.
- IC contains memory and general purpose microcontroller.
- JavaCard is often used as a platform - payment applications are then in the form of an applet.



Source: Janke, Wikimedia Commons

Steps for EMV Contact Transaction



Offline Data Authentication

Uses public key cryptography (RSA) and provides following options:

- Static (SDA): ensures data read from the card has been signed by the card issuer. This prevents modification of data, but does not prevent cloning.
  - Card contains the application data signed by the issuer’s private key.
  - When inserted into a terminal, the terminal verifies whether the signed application data is the same as the one present on the card.
- Dynamic (DDA): provides protection against modification of data and cloning.
  - Card contains RSA key pair, with PK certificate signed by the issuer.
  - Terminal sends a random number and the card signs it with its private key.
- Combined (CDA): combines DDA with the generation of a card's application cryptogram to assure card validity and transaction validity.

Terminal Action Analysis

- Terminal has to decide either to proceed the transaction offline, to go online, or to reject the transaction.
- Terminal sends the decision with the Generate Application Cryptogram command to the card.
- Card generates the Application Cryptogram by using symmetric cryptography (MAC Algorithm 3) and sends it back to the terminal.

Physical Attacks against EMV Cards

- Recovery of cryptographic keys:
  - RSA keys – can be recovered by using Simple Power Analysis (SPA), Simple Electromagnetic Analysis (SEMA), Safe-Error Analysis (SEA).
  - DES keys – can be recovered by using Differential Power Analysis (DPA) or Differential Electromagnetic Analysis (DEMA), Differential Fault Analysis (DFA).
- Recovery of PIN code:
  - SPA on RSA
- Switching the online transaction to offline:
  - By fault injection attack

EMV Certification Process

The formulations in this part were mostly taken from [2-4] to provide accurate description of the process.

Certification Steps

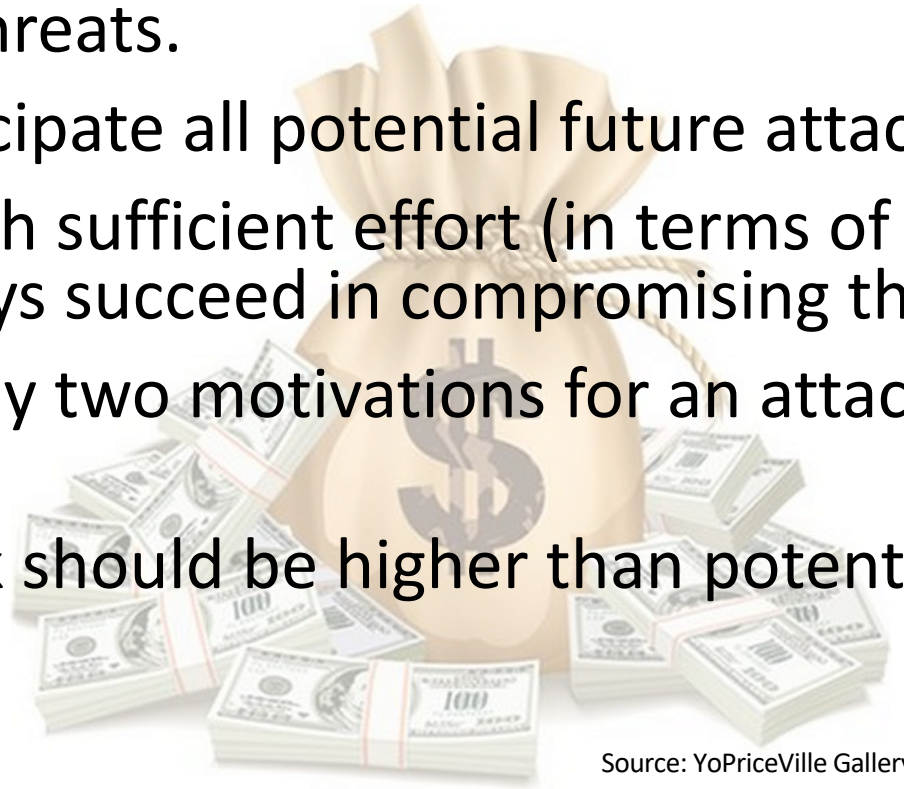
- Testing is performed by EMVCo accredited external test laboratories
- 3 components:
  - Terminal type approval:
    - Level 1: mechanical and protocol specifications for data transfer terminal ⟺ card.
    - Level 2: terminal application software.
  - Card type approval:
    - Assess whether the chip hardware and embedded EMV functionality sufficiently conforms to the electro-mechanical and functional requirements defined in the EMV Chip Specifications.
  - Chip security evaluation:
    - Assess whether a chip demonstrates sufficient assurance of certain minimum levels of security required for EMV chip payment, including security mechanisms and protections designed to withstand known attacks.

Payment Card Evaluation Process

- 3 different layers of security:
  - *Integrated Circuit (IC)* – includes the firmware and software routines required to access the security functions of the IC.
  - *Platform (IC + OS)* – includes the Integrated Circuit (IC) hardware with its dedicated software, Operating System (OS), Run Time Environment (RTE), and Platform environment on which one or more applications can be executed.
  - *Integrated Circuit Card (IC + OS + App)* – includes the IC, the Operating System, and the payment application(s) that reside(s) on the ICC.
- EMVCo supports the work of the *JIL Hardware Attack Subgroup (JHAS)* and related subgroups or initiatives working on specific security topics, to maintain a common set of current threats and attacks.

Risk Management

- There is no such thing as perfect security.
- Level of testing continuously increases to reflect state of the art attack potential – new products should offer a higher level of protection against the latest threats.
- No testing can anticipate all potential future attacks.
- An attack made with sufficient effort (in terms of skills, equipment, and time) will always succeed in compromising the assets.
- There are essentially two motivations for an attacker: publicity and reward.
- Effort for the attack should be higher than potential reward.



Source: YoPriceVille Gallery

Card Assets

- Primary assets:
  - PIN, PIN Try Counter, ATC
  - Cryptographic keys
  - Operating System (Platform) code, execution context, and registry data
  - State machine
- Secondary assets:
  - Application code
  - Application data(for example, cardholder-specific data, offline counters, and limits)
  - Transaction data (for example, log files)
  - Design information (for example, layout, process details, and test code)

Attack Vectors

- Physical attacks: reverse engineering, active and passive probing, FIB, etc.
- Overcoming sensors and filters
- Exploitation of test features (re-enter IC test mode)
- Perturbation attacks: laser or EM fault injection, voltage or frequency glitches
- Differential Fault Analysis (using single or multiple faults)
- Side channel analysis (SPA, DPA, EMA, template attacks, etc.)
- Attacks on RNG (operating conditions or physical manipulation, leakage analysis)
- Software attacks (protocol, man-in-the-middle, replay attacks)
- Logical attacks (application segregation, malicious and ill-formed applications)

JIL Hardware Attacks Subgroup (JHAS)

- Defines guidance metrics to calculate the attack potential required by an attacker to effect an attack.
- Factors: elapsed time, expertise, knowledge of the TOE, access to the TOE, equipment needed to carry out an attack, as well as whether or not open samples or samples with known secrets had been used.
- It may not be necessary to carry out all of the experiments to identify the full attack.
- In many cases, the evaluators will estimate the parameters for the exploitation phase, rather than carry out the full exploitation.

Identification and Exploitation

- Attack potential has to be calculated for both
- *Identification* part of an attack corresponds to the effort required to create the attack, and to demonstrate that it can be successfully applied to the TOE (including setting up or building any necessary test equipment).
- *Exploitation* part of an attack corresponds to achieving the attack on another instance of the TOE using the analysis and techniques defined in the identification part of an attack.
- Attack technique (and relevant background information) is available for the exploitation in the form of a script or a set of instructions defined during the identification of the attack.

Rating of Elapsed Time

	Identification	Exploitation
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*

Expertise

- *Expert* – familiar with:
  - Implemented algorithms, protocols, hardware structures, security behaviour, principles and concepts of security employed.
  - Techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc.
- *Proficient* – familiar with security behaviour, familiar with laboratory measurements and equipment: can for example apply logical attacks, probing attacks and do non invasive analysis using laser, oscilloscope and similar.
- *Laymen* – no particular expertise.

Extent of Expertise

Equipment:

- Oscilloscope
- Optical Microscope
- Chemistry (etching, grinding), Microprober
- Laser Cutter, Radiation
- Plasma (etching, grinding), Focused Ion Beam (FIB)
- Scanning Electron Microscope (SEM)
- Atomic Force Microscope (AFM)

Knowledge:

- Common Product information
- Common Algorithms, Protocols
- Common Cryptography
- Differential Power Analysis (DPA), Differential Fault Analysis (DFA), Electromagnetic Analysis (D/EMA)
- Reverse Engineering
- Smartcard or similar device specific hardware structures
- Principles and concepts of security

Rating of Expertise

	Identification	Exploitation
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6

Knowledge of TOE

- *Public information* – can be obtained by anyone.
- *Restricted information* - it is controlled within the developer organisation and distributed to other organisations under a non-disclosure agreement.
- *Sensitive information* – only available to discrete teams within the developer organisation.
- *Critical information* – only available to teams on strict need-to-know basis within the developer organisation. Physically and environmentally protected by high secure IT infrastructure.
- *Very critical information* – known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking.

Rating of Knowledge of TOE

	Identification	Exploitation
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical	9	*
Not practical	*	*

Rating of Access to TOE

	Identification	Exploitation
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*

Equipment

- *None*.
- *Standard* – this equipment can be readily obtained e.g., at a nearby store or downloaded from the Internet.
- *Specialized* – purchase of moderate amounts of equipment or development of more extensive attack scripts or programs.
- *Bespoke* – very expensive or specially produced equipment. Complex and dedicated software (e.g. advanced analysis tools that are not available for purchase) that has been developed during the identification phase can be considered as bespoke equipment.

Categorization of tools – Examples

Tool	Equipment
UV-light emitter	Standard
Voltage supply	Standard
PC or work station	Standard
UV light microscope and camera	Specialized
Laser equipment	Specialized
High-end digital oscilloscope	Specialized
Scanning electron microscope (SEM)	Bespoke
Atomic Force Microscope (AFM)	Bespoke
Focused Ion Beam (FIB)	Bespoke

Rating of Equipment

	Identification	Exploitation
None	0	0
Standard	1	2
Specialized*	3	4
Bespoke	5	6
Multiple Bespoke	7	8

* If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack this shall be rated as bespoke.

Open Samples/Samples with known Secrets

- Term *open samples* stands for samples where the evaluator can put applications on top of the platform at his own discretion that bypasses countermeasures prescribed in the platform guidance.
- The intention is to use test applications without countermeasures but not deactivate any platform inherent countermeasures.
- *Samples with known secrets* refers to a TOE for which the evaluator knows or can define one or more pieces of secret data, such as a PIN or key for performing either side-channel or fault attacks, yet without deactivating any countermeasures.

Knowledge of the TOE 1/2

- *Public*:
  - *Open samples*: No protection of the samples, delivered without control; or the platform is used in combination with non-secure applications.
  - *Samples with known secrets*: This concerns secrets easily deducible.
- *Restricted*:
  - *Open samples*: Typically protected as the user deemed specifications of the platform, as the data sheet of an IC, or delivered without additional control of the people having access to this kind of information.
  - *Samples with known secrets*: Typically applies to secrets where a specific decision and action is required to release the information, and where the recipient is made aware that the data is potentially useful to an attacker.

Knowledge of the TOE 2/2

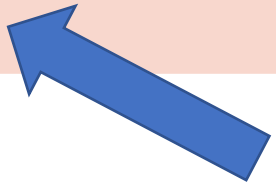
- *Sensitive*:
  - *Open samples*: Controlled within the developer organisation and distributed to other organisations under a non-disclosure agreement.
  - *Samples with known secrets*: Secrets are only shared by a limited number of clearly defined and identified people or devices, with strong access controls.
- *Critical*:
  - *Open samples*: Protected at the implementation level (source code, VHDL, layout).
  - *Samples with known secrets*: Secrets were generated inside the sample and are only owned by it, or in another module which does not make these secrets available outside the module (except to the sample).

Rating of Open Samples/Samples with Known Secrets

	Identification	Exploitation
Public/Not required	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Rating of Vulnerabilities and TOE Resistance

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High



EMVCo requirement

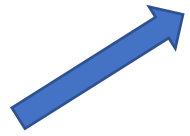
* final attack potential = identification + exploitation.

Example – Side-Channel Attack

- Attack vector: power measurement of supply voltage of the card with a digital oscilloscope.
- Threat: recovery of card's assets from information leaked through the power consumption of the chip.
- Attack method: SPA/DPA depending on the asset.
- Preconditions:
  - Good knowledge of cryptographic implementations.
  - Knowledge of side-channel attack methods and tools, and experience with the equipment.
  - Knowledge of communication protocols of the card.

Example – Assessment of SCA Attack

Factor	Details	Identification	Exploitation
Elapsed time	Collection and analysis of at least 30k traces, one week identification, one day exploitation	2	3
Expertise	Expert for identification, proficient for exploitation	5	2
Knowledge of TOE	Knowledge of communication protocol for identification	2	0
Access to TOE	Less than 10 samples required	0	0
Equipment	Digital oscilloscope - specialized	3	4
Open sample	Not required	0	0
Total		12 + 9 = 21	



Enhanced-Basic

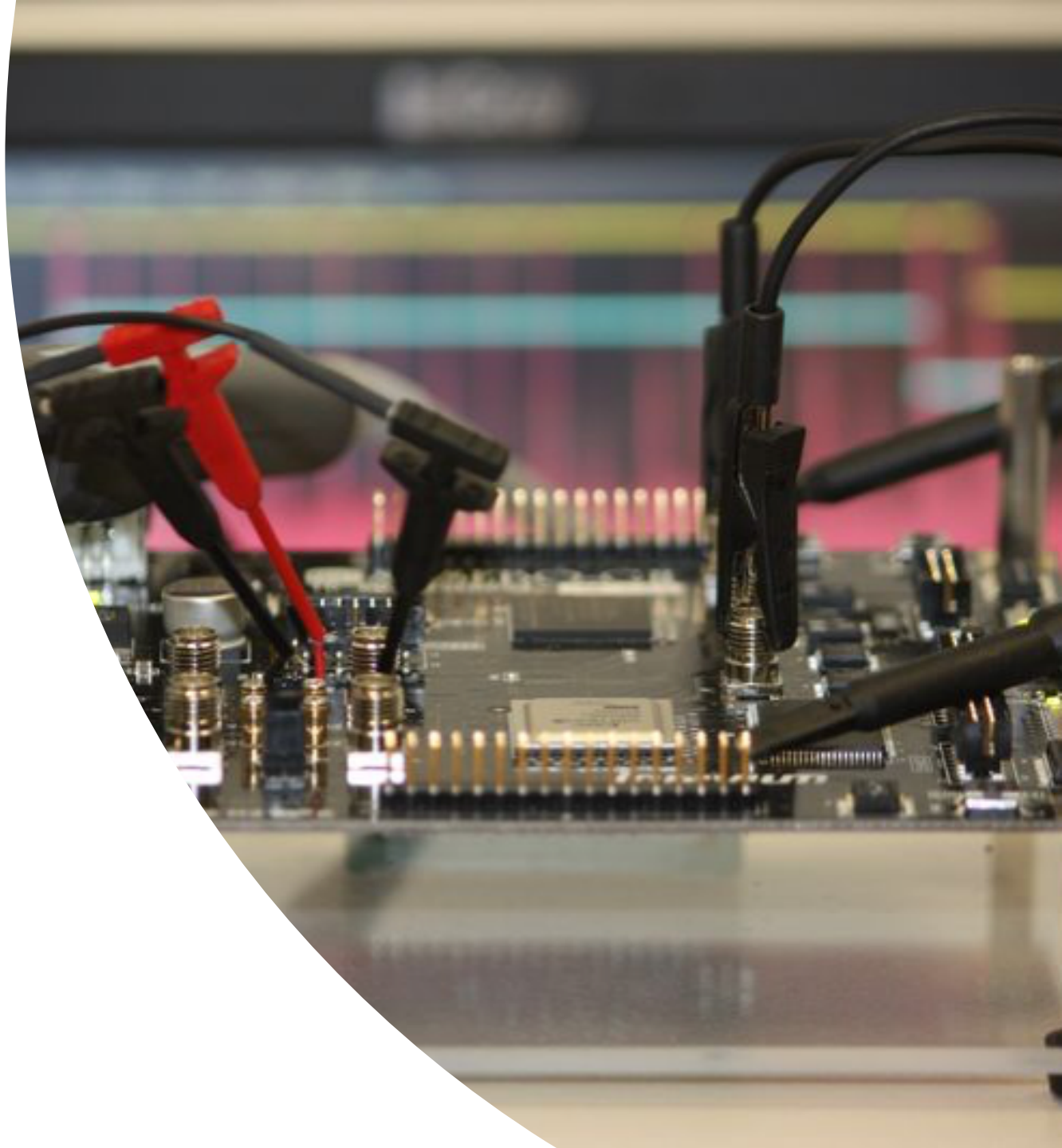
Side-Channel Attacks against EMV Cards

Main Idea

Source: National Geographic

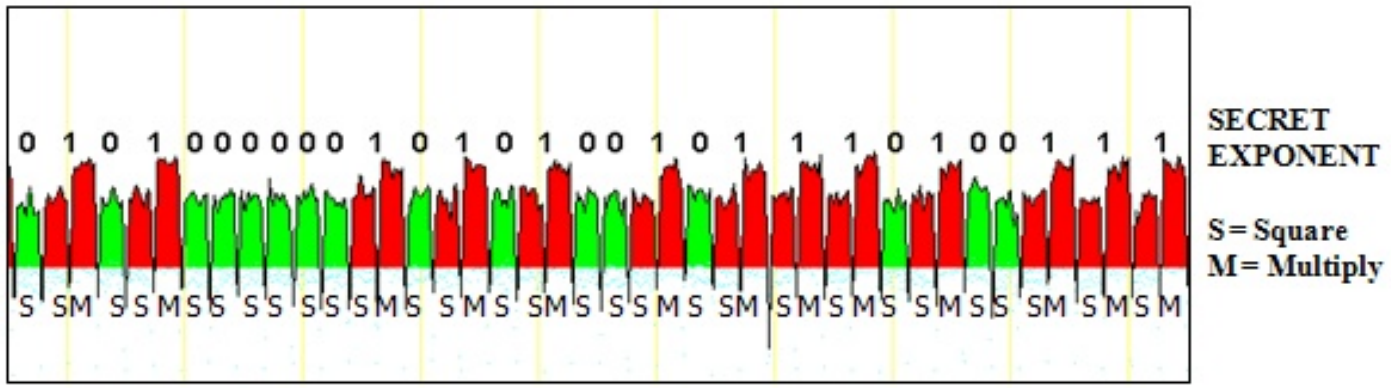
Side-Channel Attacks

- Observe physical characteristics of a device during the encryption
- Focus on implementation rather than algorithm
- Various methods to get the secret information:
  - Timing analysis
  - Power analysis
  - Electromagnetic analysis
  - Acoustic analysis
  - Cache analysis



Simple Side-Channel Attacks

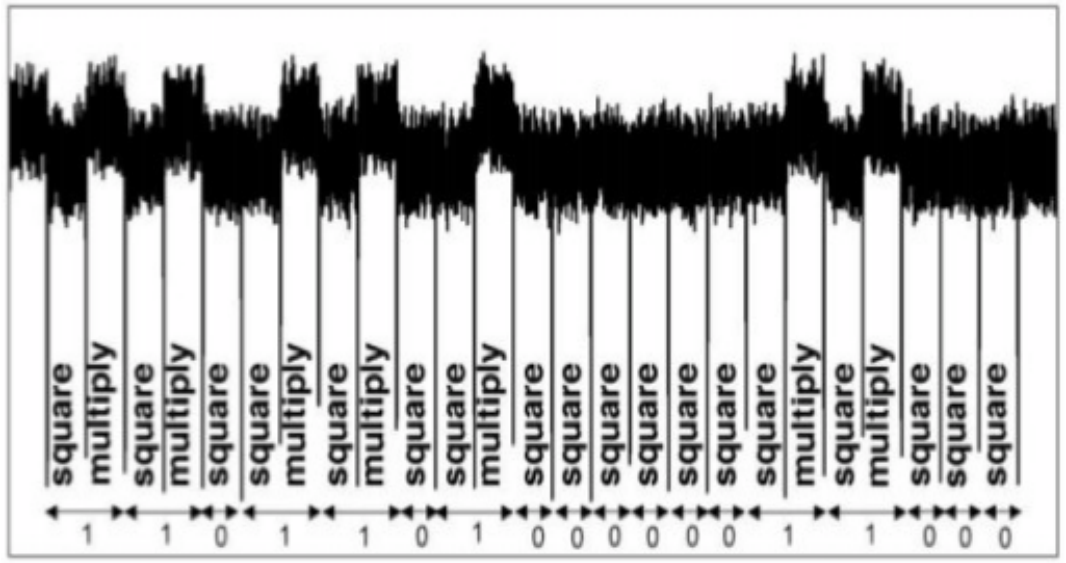
- Attacker uses information from one measurement to determine parts of the secret key
- Exploit relationship between the executed *operations* and the side-channel information



Source: Gilbert Goodwill, Cryptography Research, Inc.

Simple Power (EM) Analysis of RSA

- Secret exponent *e* is a large binary number, while *x* is the message (x^e)
- Square and multiply algorithm is applied:
  - If we encounter a 0, we square *x*.
  - If we encounter a 1, we square *x*, then multiply by *x*.



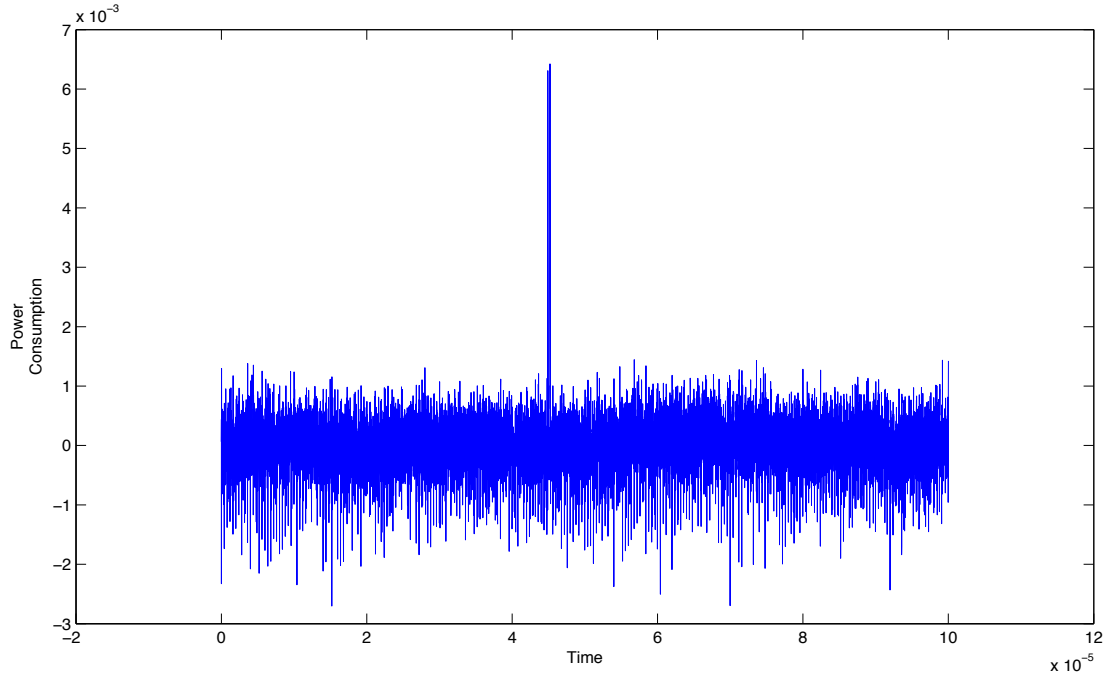
Source: David Oswald, Ruhr University Bochum, Germany

Protecting RSA

- Adding dummy operations:
  - Multiply-Always algorithm is a form of hiding countermeasure
  - Attacker will see a chain of identical operations
- Message blinding:
  - Instead of calculating x^e, we calculate $(xr)^e$, where r is a random integer between 1 and N, relatively prime to N
  - This method also protects against timing leakage
- Random operations:
  - Cryptoprocessor can be set in a way that random operations are executed at random times
- The best way is combination of several methods

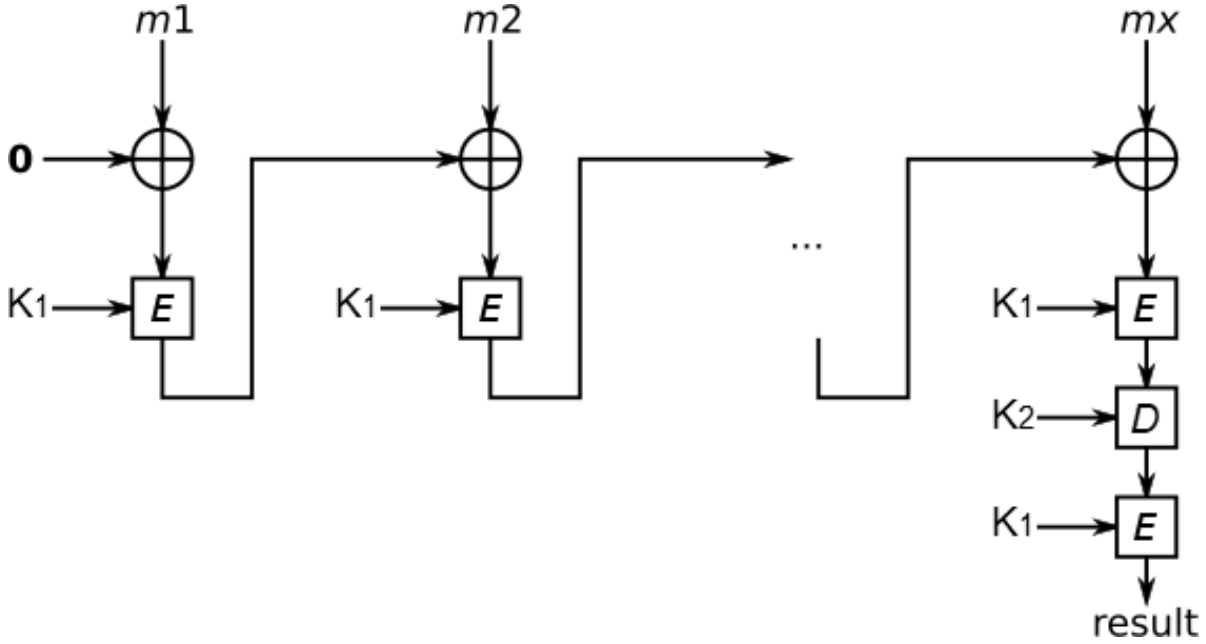
Differential Side-Channel Attacks

- Attacker uses multiple measurements to filter out the noise
- Exploit relationship between the processed *data* and the side-channel information



MAC Algorithm 3

- Message Authentication Code method according to ISO/IEC 9797-1 standard
- Used for generating Application Cryptogram in the card
- Uses DES and TDES-EDE
- Based on CBC MAC

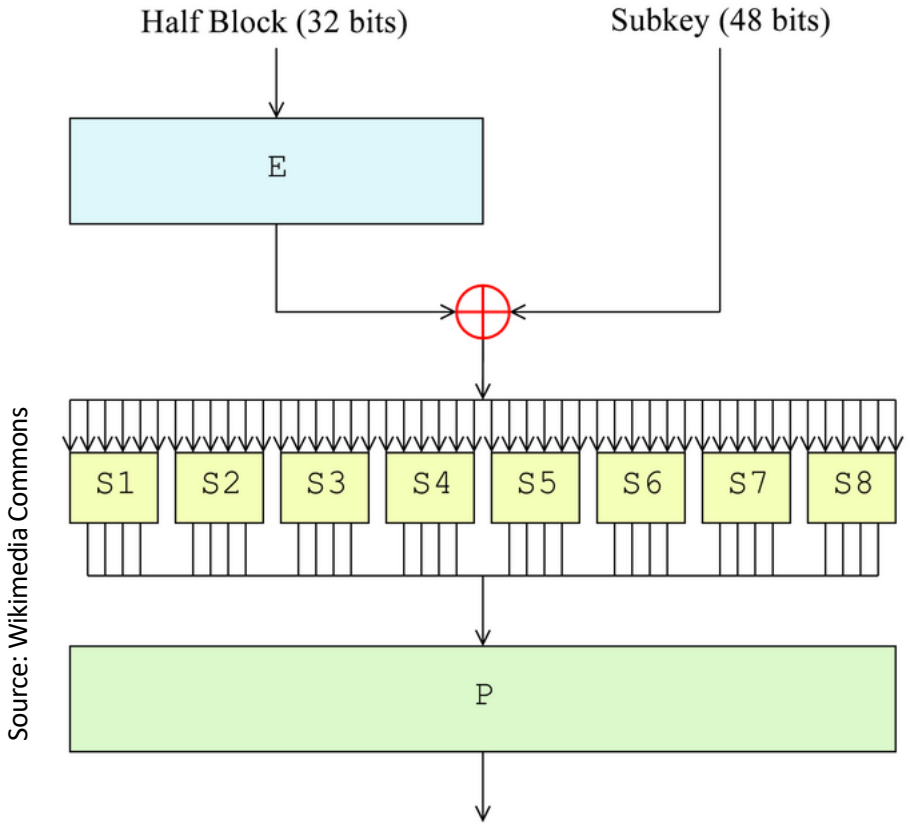


Source: fgrieu, Cryptography Stack Exchange

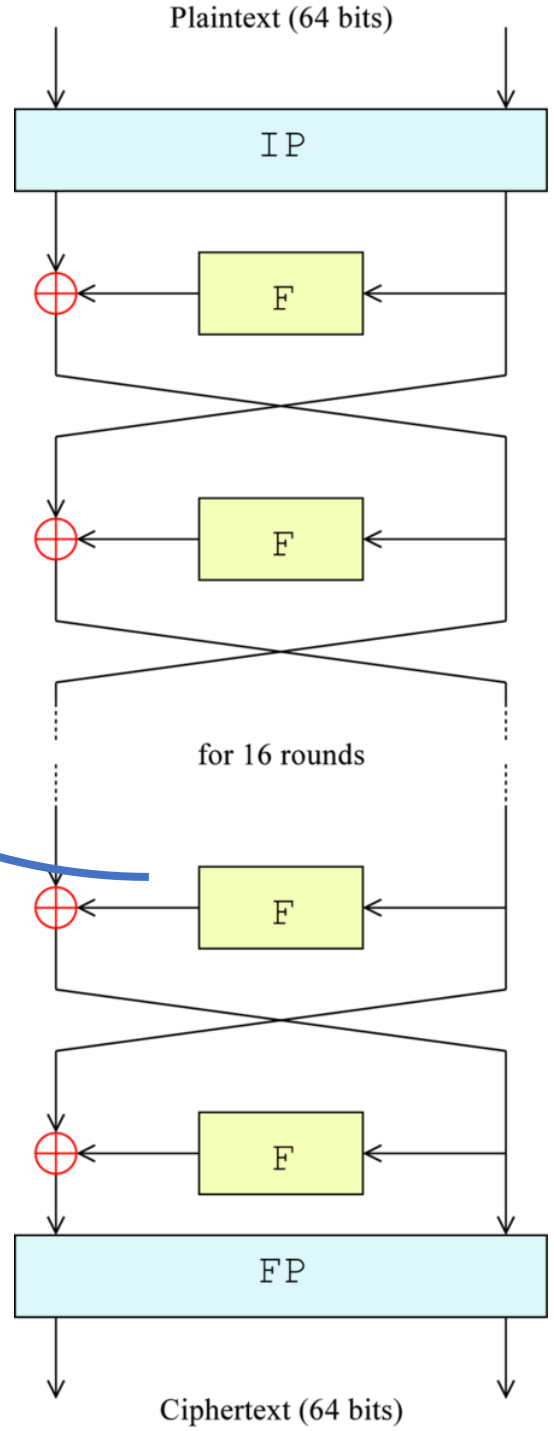
Data Encryption Standard (DES)

- Developed in early 70's at IBM by Horst Feistel
- Official US FIPS standard issued in 1977
- Fully broken in 1999 by Electronic Frontier Foundation in 22 hours
- Superseded by Advanced Encryption Standard (AES) in 2001
- Main characteristics:
  - 56-bit key size
  - Feistel structure with function *F* realizing confusion and diffusion
  - 16 rounds
  - 6x4 Sboxes (8 different Sboxes per round)

Data Encryption Standard (DES)



Source: Wikimedia Commons



Source: Wikimedia Commons

Triple DES (3DES or TDES)

- Effort to make DES resistant to brute-force attacks
- Several variants:
  - 1/2/3 keys – 1 key variant is weak, 3 key variant is vulnerable to meet-in-the middle attacks and only provides 2^{112} security instead of 2^{168}
  - Encrypt-Decrypt-Encrypt (EDE)
  - Encrypt-Encrypt-Encrypt (EEE)
- MAC Algorithm 3 uses TDES-EDE option with 2 keys
- According to NIST SP 800-57 rev.4, 2-key variants of TDES are depreciated for use in federal systems

Breaking DES – crack.sh

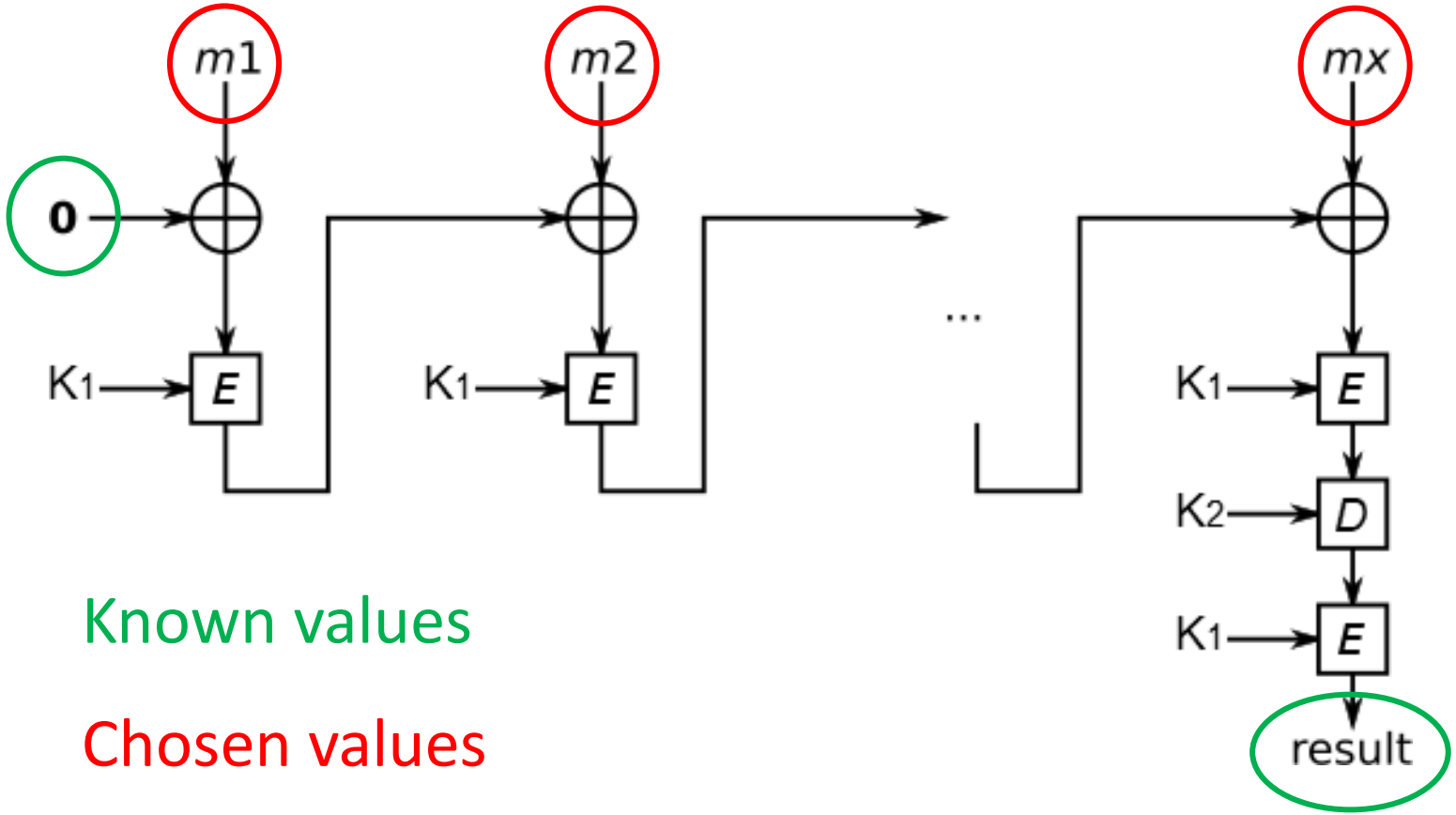
- Average time to break is 26 hours, worst time 3.5 days

TOKEN FORMAT	TYPE	NOR-MAL PRICE	ASAP PRICE	DESCRIPTION
(LM|NT)HASH:[0-9a-fA-F]{48}	NET(NT)LM	FREE	N/A	NET(NT)LM hashes captured with the 1122334455667788 challenge (like with SMB Capture or Responder)
$NET(NT)?LM$[0-9a-fA-F]{16}$[0-9a-fA-F]{48}	NET(NT)LM	$20	$200	NET(NT)LM hashes captured with a random challenge
99[a-zA-Z0-9\+/]{35}=	chapcrack	$20	$200	PPTP VPN and WPA-Enterprise MSCHAPv2 authentication cap-tures
$9[78]$[a-zA-Z0-9\+/]{32}	des_kpt	$30	$300	Custom Known-Plaintext DES Cracking or Kerberos5
[0-9a-zA-Z/\.]{13}	des_crypt()	$100	$1000	/etc/passwd 25-round DES hashes full keyspace search

Breaking MAC Algorithm 3

- If implemented properly, NOT easy.
- Depending on many factors:
  - Are the chip manufacturer's guidelines obeyed? – are the sensitive operations computed in a secure manner?
  - If there is masking, is the mask sufficiently protected?
  - Is there hiding which adds too much noise?
- Requires a combination of side-channel and brute-force attack.
- Master key size is 112b:
  - Intermediate secrets can be recovered by differential power/EM analysis.
  - Both portions of the key can later be recovered by a brute-force attack.

Attack Steps – Preconditions

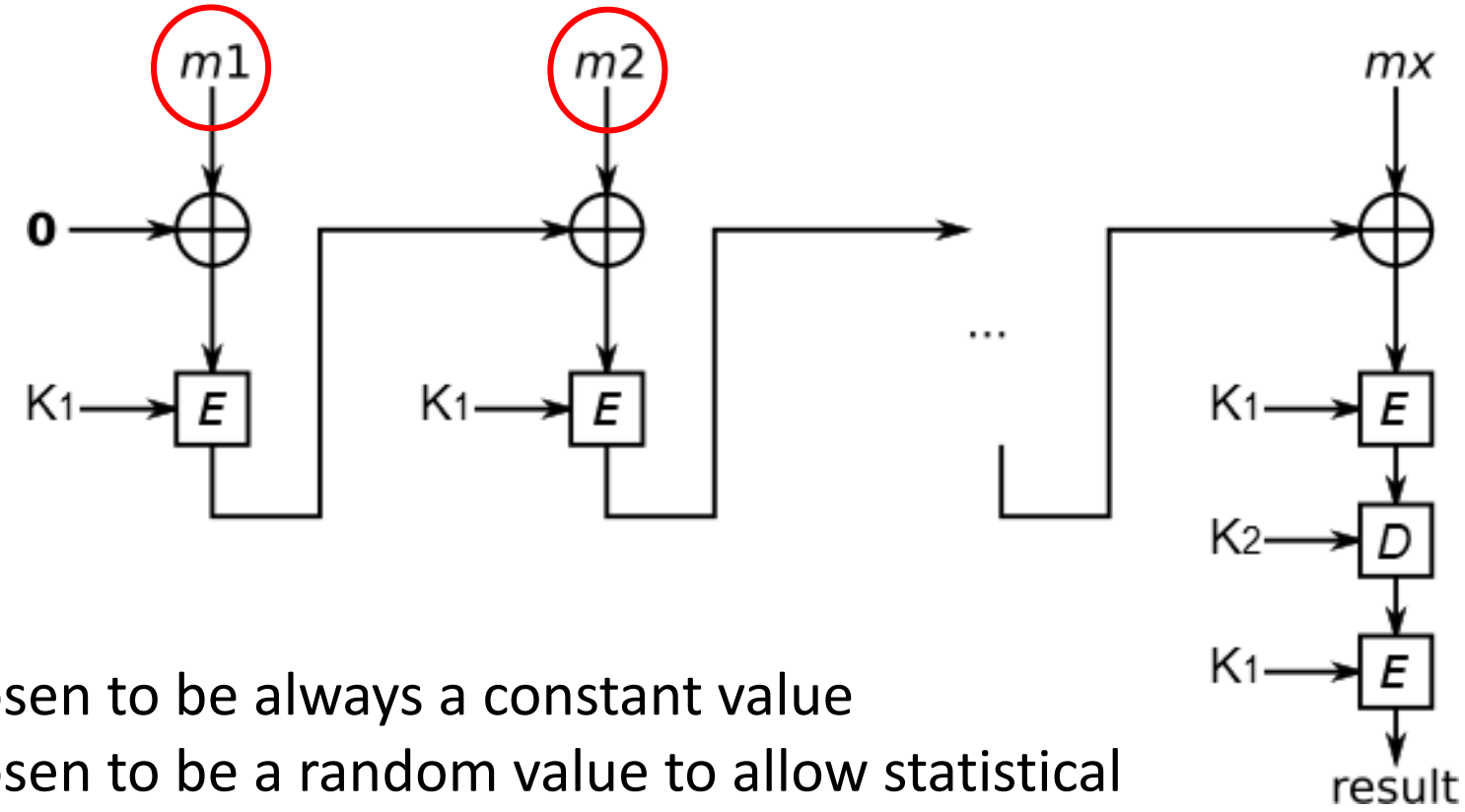


Known values

Chosen values

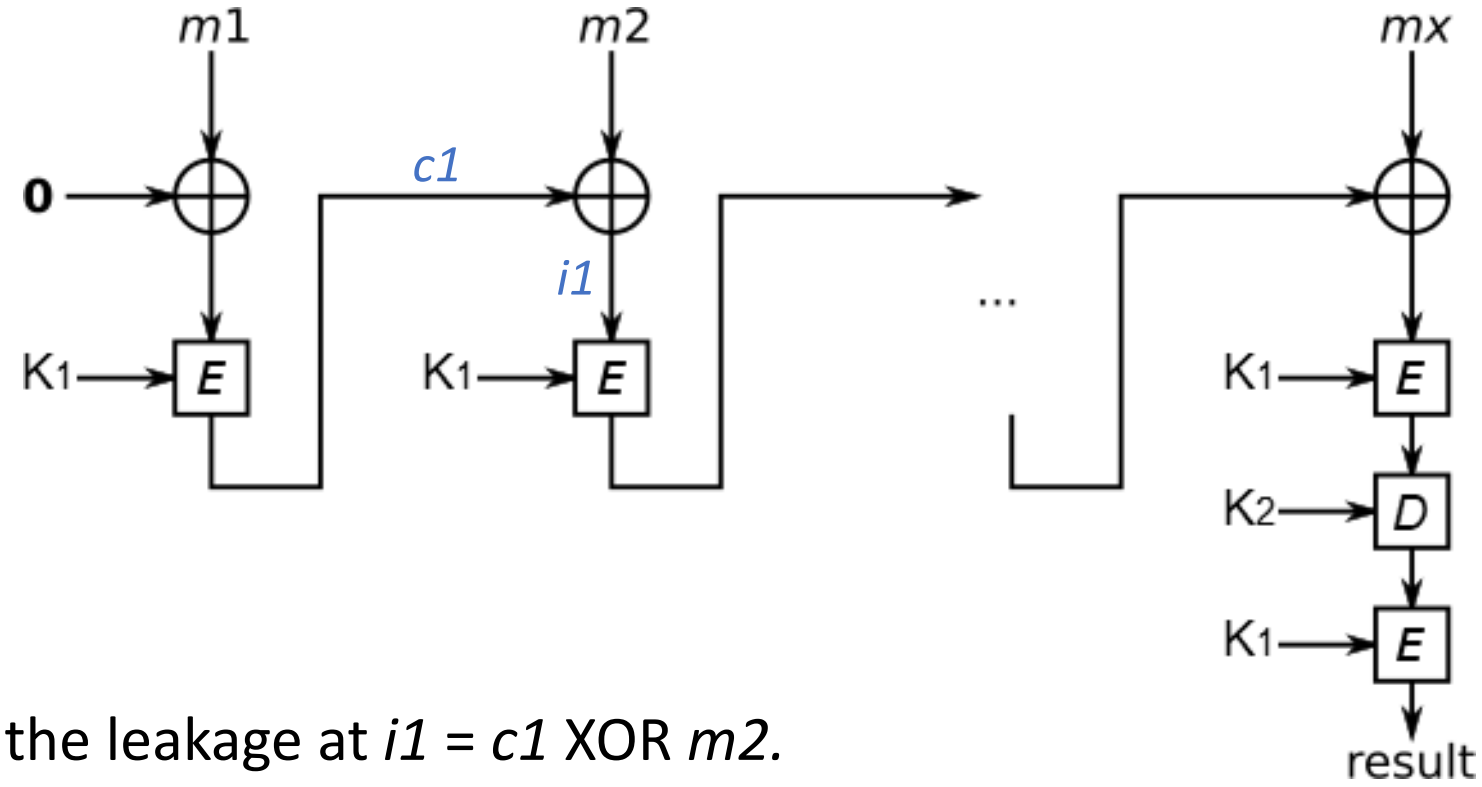
- The attacker must be able to control the message

Attack Steps – Choosing Values



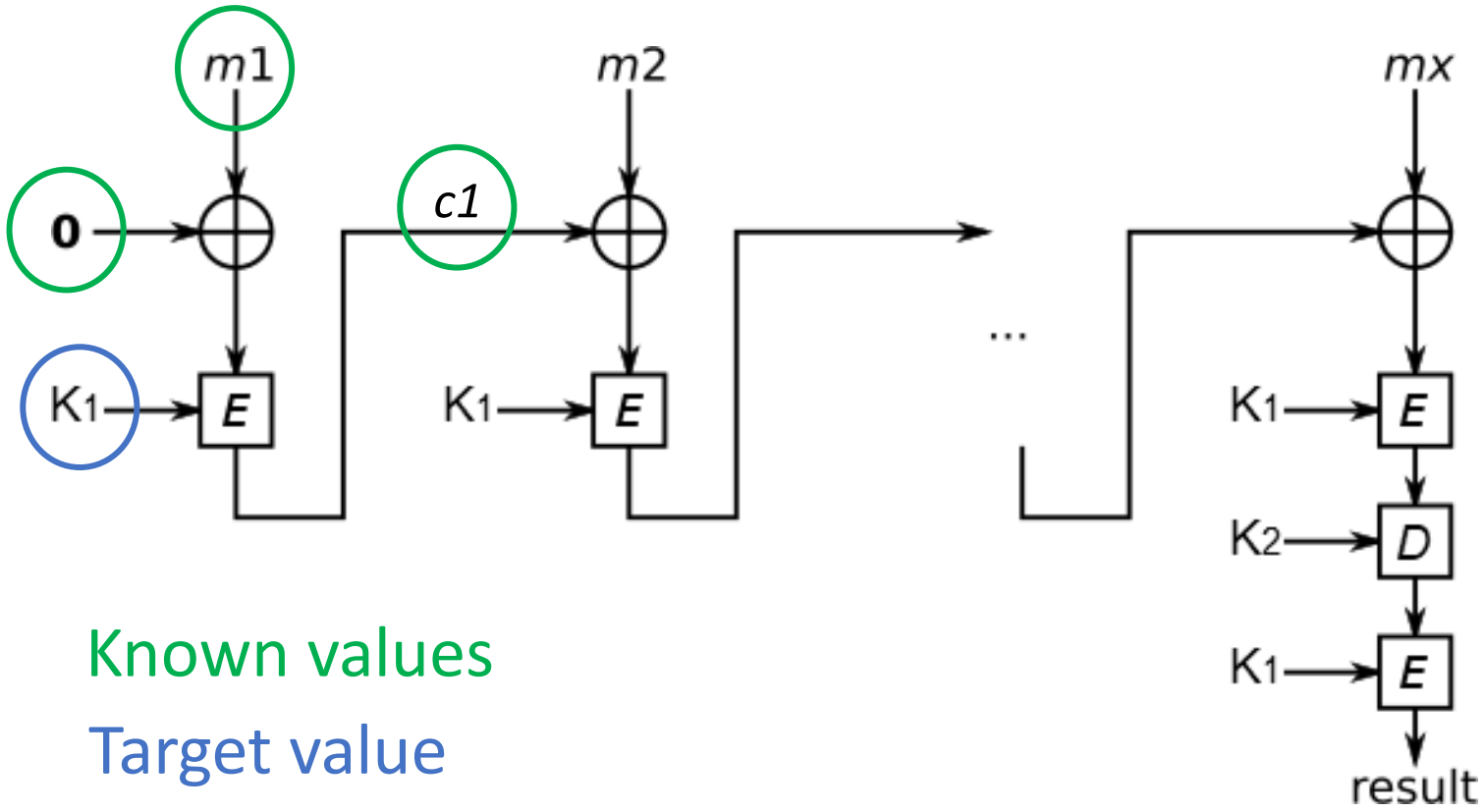
- *m1* is chosen to be always a constant value
- *m2* is chosen to be a random value to allow statistical attack

Attack Steps – Observing SCA Leakage



- Measure the leakage at *i1* = *c1* XOR *m2.*
- Recover *c1* by side-channel analysis.

Attack Steps – Brute-Force Attack 1

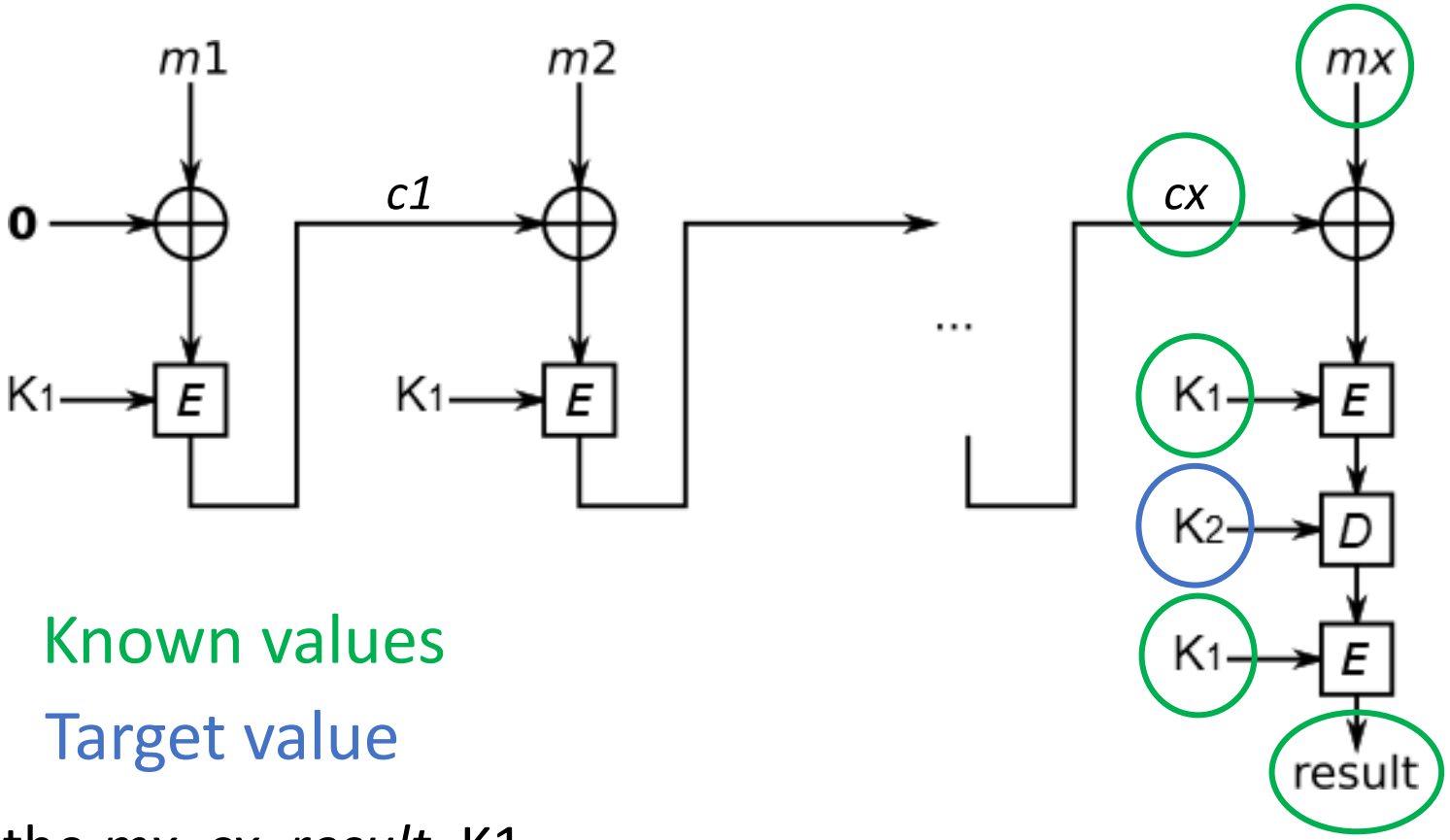


Known values

Target value

- We know the *IV, m1, c1*.
- Brute-force attack can be applied to recover K1.

Attack Steps – Brute-Force Attack 2



Known values

Target value

- We know the *mx, cx, result,* K1.
- Second brute-force attack can be applied to recover K2.

Side-Channel Attacks – Summary

- The main weakness is the short key length of DES.
- Schemes are slowly moving to AES, eliminating this type of attack.
- With proper usage of masking and hiding, SCA can be avoided.
- Current chip manufacturers are well-aware of SCA/FIA, expert security teams lead the design of countermeasures.
- Risk management is the right approach:
  - It requires expertise and equipment to recover the key by SCA.
  - Number of transactions on the card is limited, and the attacker normally does not have knowledge what chip is used and what countermeasures.
  - If the card is reported as stolen, secrets become useless.

Conclusions

Payment Card Security Summary

- Security of payment cards has gone a long way.
- Current EMVCo evaluation processes are well-defined.
- Attack vectors are thoroughly monitored for new threats published in literature.
- Payment systems are moving from physical cards to virtual cards on mobile phones.
- New companies are entering the payment market based on completely different methods – WeChat, AliPay.
- Shift from insurance protection to enhanced security is visible.

Additional Reading

[1] B. Feix and H. Thiebeauld: Defeating ISO9797-1 MAC Algo 3 by Combining Side-Channel and Brute Force Techniques, 2014. ePrint: https://eprint.iacr.org/2014/702.pdf

[2] EMVCo: A Guide to EMV Chip Technology, v.2 Nov 2014. Online: https://www.emvco.com/wp-content/uploads/2017/05/A_Guide_to_EMV_Chip_Technology_v2.0_20141120122132753.pdf

[3] EMVCo: EMVCo Security Evaluation Process, v.5.1 Jun 2016. Online: https://www.emvco.com/wp-content/uploads/2017/04/EMVCo-SEWG-14-P02-V5-1_EMVCo_Security_Evaluation_Process_20160725082101992.pdf

[4] Joint Interpretation Library: Application Attack Potential to Smartcards and Similar Devices, v3 Apr 2019. Online: https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3-0.pdf

Thank you! Any Questions?

Jakub Breier (jbreier@ntu.edu.sg)
https://jbreier.com