Securitatea Informatica

Curs 5. E-Banking Security

Elena Simona Apostol
elena.apostol@upb.ro

E-Banking: Glossary of Terms

Introduction

- ✓ **Electronic banking (e-Banking)**: service that lets the customer perform a collection of banking services through electronic means

- ✓ Popular Types of E-banking:
  - ✓ **Internet Banking**: It is the type of electronic banking service which enables customers to perform several financial and non-financial transactions via the internet
  - ✓ **Mobile Banking**: This electronic banking system enables customers to perform financial and non-financial transactions via mobile devices
  - ✓ **ATM**: Automated Teller Machines allows customers to withdraw funds, deposit money, change Debit Card PIN, and other banking services.

Special Features of Internet Banking

- ✓ Provides access to financial as well as non-financial banking services
- ✓ Facility to check bank balance any time
- ✓ Make bill payments and fund transfer to other accounts
- ✓ Keep a check on mortgages, loans, savings a/c linked to the bank account
- ✓ Safe and secure mode of banking
- ✓ Customers can apply for the issuance of a chequebook
- ✓ Buy general insurance
- ✓ Set-up or cancel automatic recurring payments and standing orders
- ✓ Keep a check on investments linked to the bank account

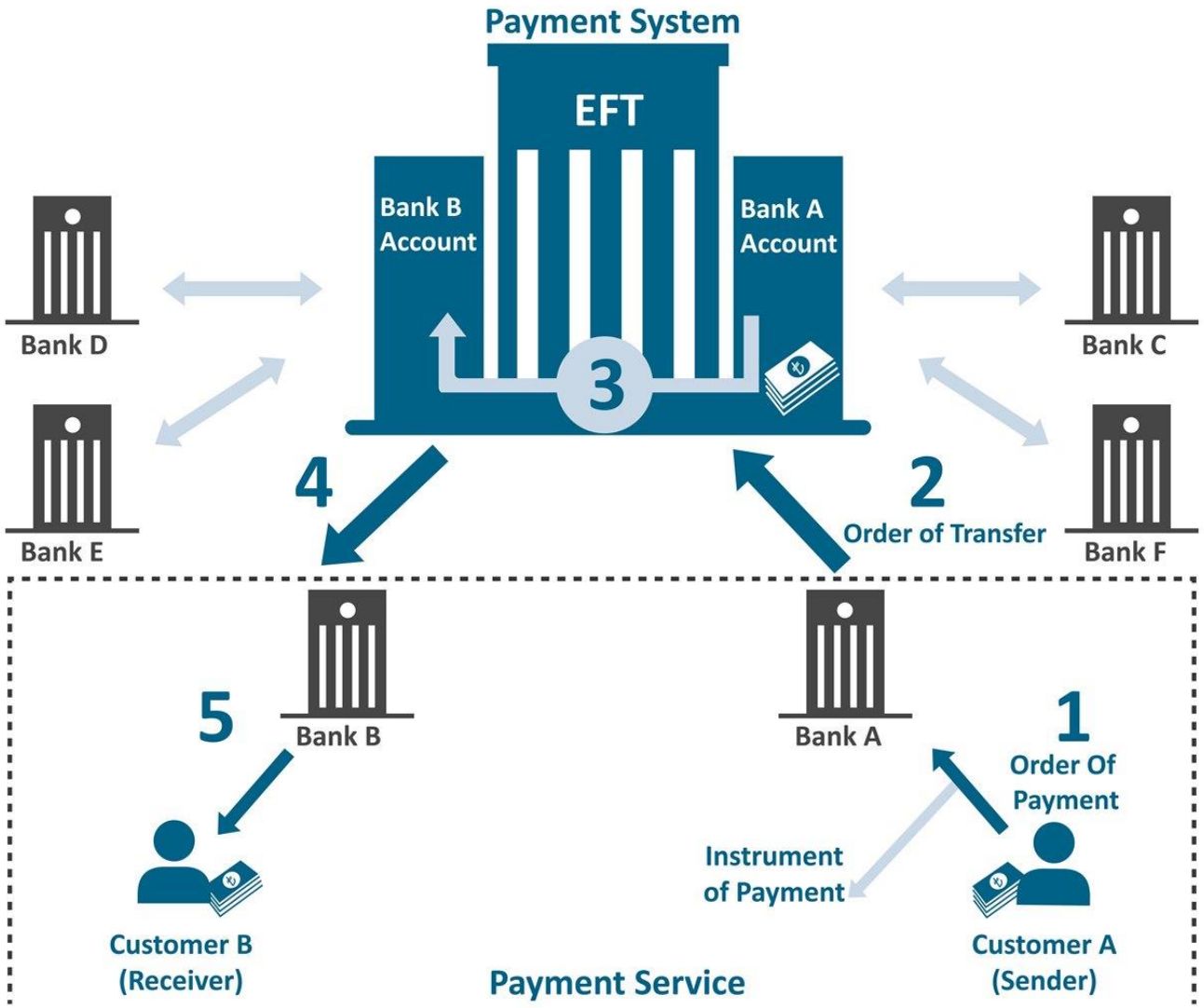
Electronic Funds Transfer (EFT)

- ✓ An electronic funds transfer (EFT) is a transaction that takes place over a computerized network

- ✓ EFTs include:
  - ✓ direct-debit transactions,
  - ✓ wire transfers,
  - ✓ ATM withdrawals and
  - ✓ online bill pay services

- ✓ EFTs also known as *online or PIN-based transactions* offer an alternative to signature debit transactions (Visa, MasterCard)

Electronic Funds Transfer (EFT)



https://www.tcmb.gov.tr/wps/wcm/connect/EN/TCMB+EN/Main+Menu/Core+Functions/Payment+Systems/Key+Issues/Payment+Service+and+Payment+System/

Security in EFT

- ✓ protection of the integrity of electronic funds transfer (EFT) systems
- ✓ protection of the EFT information

EFT vulnerabilities (compared with paper-based payment systems):

- ✓ EFT systems have many points of access where transactions can be affected in unauthorized ways
- ✓ Funds can be removed almost instantly without review of individual transactions by officials
- ✓ It is possible, in theory, for large banks of data to be destroyed by remote agents
- ✓ EFT crime is often difficult to detect because funds/data can be removed or manipulated by instructions hidden in complex computer software

E-Commerce: Exchanges

- The main types of markets:
  - Dealers (Over-the-counter)
  - Exchanges
  - Brokers

- **Exchange:** warehouse in which people buy and sell stocks
  - the exchange is the most automated

- **Broker**: buys and sells stocks through an exchange, charging a commission in this way

- **Foreign exchanges (FX)** : traders buy and sell currencies

E-Commerce: Portals

- ✓ Corporate treasurers regularly need to exchange currencies

- ✓ Foreign exchange (FX) portals:
  - ✓ Internet-enabled trading systems (corporates/users log on to buy and sell currencies)
  - ✓ The systems are integrated with other banking systems or the corporates' own systems

- ✓ 2 types of portals:
  - ✓ Banks: provide FX portals on which corporates/users can trade on this platform through that bank
  - ✓ Multi-bank portals: a wider range of banks to choose for trading

E-Commerce: Single-bank portals

- ✓ They offer straight currency transactions
- ✓ A corporate/user makes payments in any currencies without having to maintain local currency accounts
- ✓ An automatic and more detailed audit trail with potential for integration into TMS and ERP systems
  - ✓ **TMS - Transportation Management System**
  - ✓ **ERP - Enterprise Resource Planning** *(the integrated management of core business processes)*

E-Commerce: Multi-bank portals

- ✓ The portals offer corporate users the ability to trade FX with many banks through one online platform
- ✓ Huge numbers of currencies and currency pairs are available
- ✓ Clear audit trail
- ✓ Corporates seeking pre-trade anonymity can see constant streams of data from banks

Next-Generation Banking

Current Context

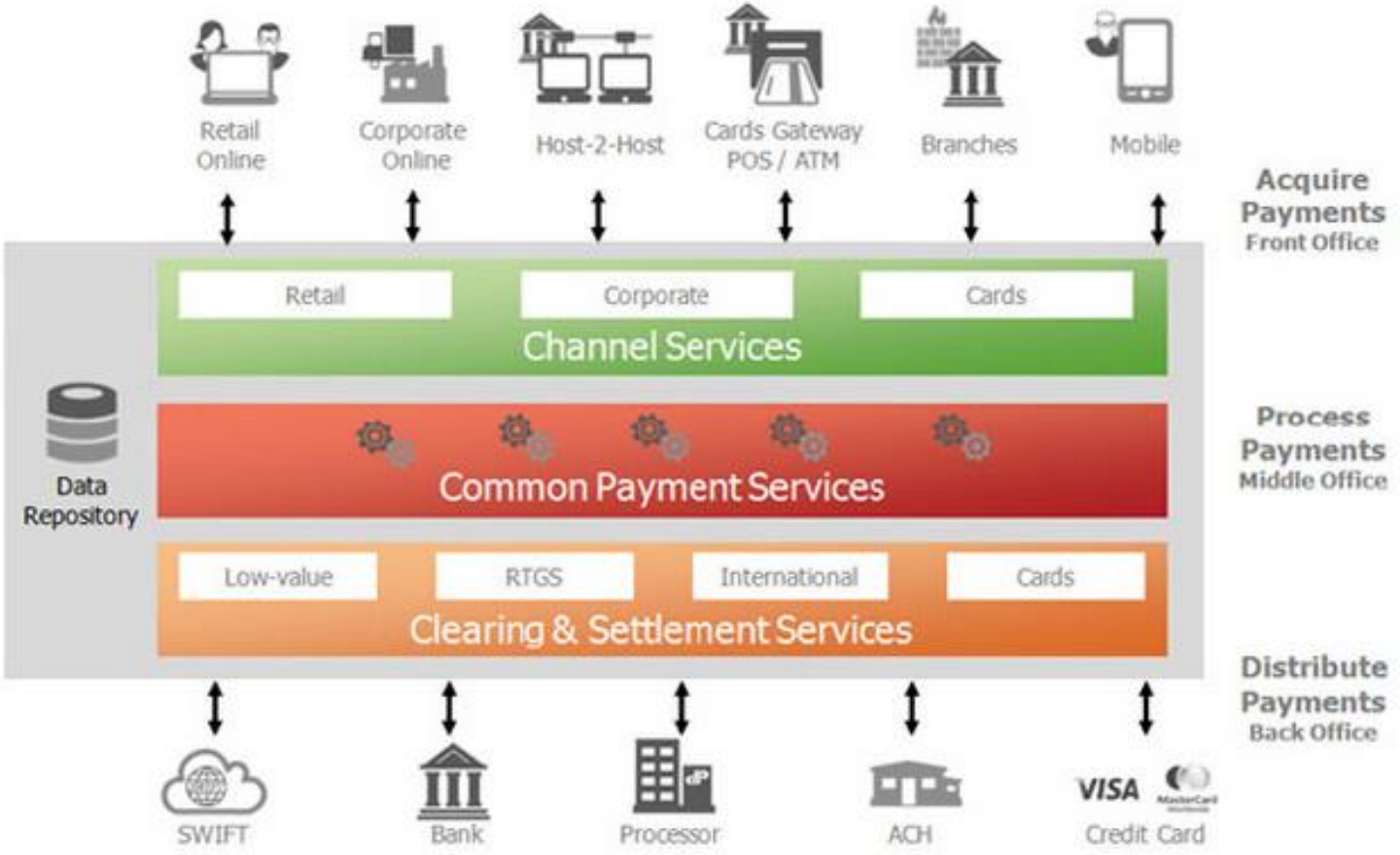
- ✓ Consumers want simple, seamless, efficient and low-cost experiences
- ✓ AI, ML, big data is becoming increasingly important to Consumer Banking

- ✓ Tech companies are in dominant positions with respect to having (a) Data, (b) Customer Access, etc.
- ✓ BigTechs are making inroads into the FinTech world, e.g., Amazon/Apple, Google Pay, Uber Bank

- ✓ Traditional banks will have to eventually partner with Big Tech companies to leverage on technology and access to the end customer

Banking Security Architecture

- ✓ **The <NEW> Open Payment Framework** – build as a SOA architecture
  - ✓ the biggest shift ever from traditional bank/customer transactional relationships
  - ✓ *'Open Banking Security Profile' - version 1 (14 July 2017)*



Banking Security Architecture

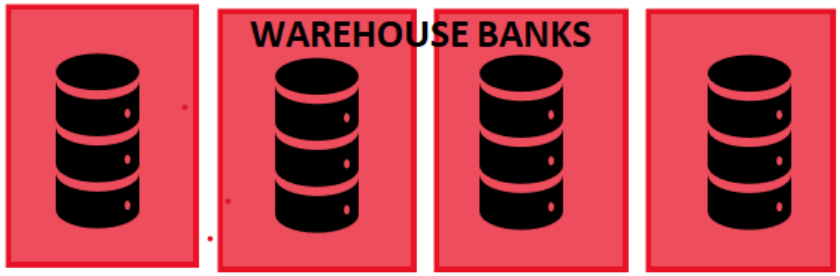
- ✓ **Traditionally banks** have **completely controlled** the sensitive customer information entrusted to them
  - ✓ Access has been restricted to strictly approved internal roles and entities that use corporate security measures, such as firewalls

- ✓ **Open banking**:
  - ✓ the banks' sensitive data perimeters → extend outside their premises
  - ✓ banks must now make their customers' personal or business current-account information accessible to external entities:
    - ✓ **account aggregators, challenger banks, start-ups, fintech**
  - ✓ banks may be exposed to **new threats** emanating from beyond their traditional areas of control

Potential Shape of Consumer Banking Ecosystem (1/2)

REGULATORY OVERSIGHT

WAREHOUSE OF CUSTOMER $

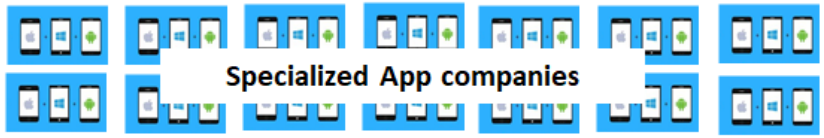


Ring Fenced from rest of the ecosytem
Customer Deposits (Liquidity)
Price loans (Risk)
"Too- Safe-To-Fail"
Low Risk - Low Stable Equity Returns
One customer can have multiple WB accounts

IDENTITY
SECURITY
KYC/CDD
DATA
CREDIT PROFILE

Important platform layer managing ID/KYC
Custodian of "Customer Data"
Provides Consent based open banking access
Integrates with Apps
Likely cross platform standards to allow portability
Use AI/ML to build credit profiles for customers

INTERACTION LAYER



Builds cutting edge specialized applications
Private Capital/relativly thinly capitalized
Assets are securitized to Warehouse Banks

CUSTOMERS

Profile and Data is kept at Platform Level
Transactions are made through apps
Money is 'Safely' kept with warehouse banks

Potential Shape of Consumer Banking Ecosystem (2/2)

- ✓ **Central Banks:** the primary regulatory body with regulatory oversight over the banking ecosystem
- ✓ **Warehouse Banks:** will only hold “Liquidity” and “Price Risk (Credit/Loans)
- ✓ **Platform Banks**: large platforms/marketplaces that will be the primary gateway for a customer to the banking system
- ✓ **Fintechs-App Banks:** the typical apps that will be connected to all other types of banks using APIs, connectors and so on

Payments Security

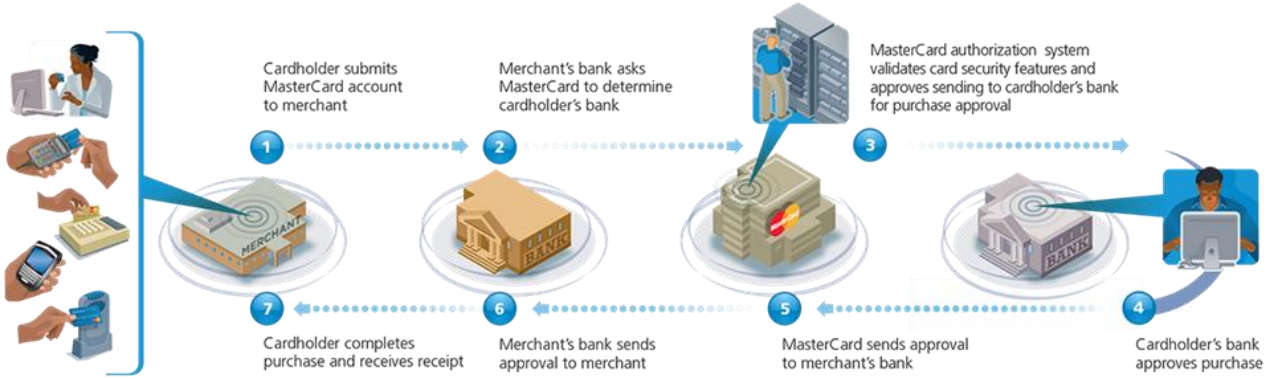
Modern Payments Security

- ✓ EMV (Europay, MasterCard, and Visa): standard for credit cards that uses **computer chips** to authenticate **chip-card** transactions

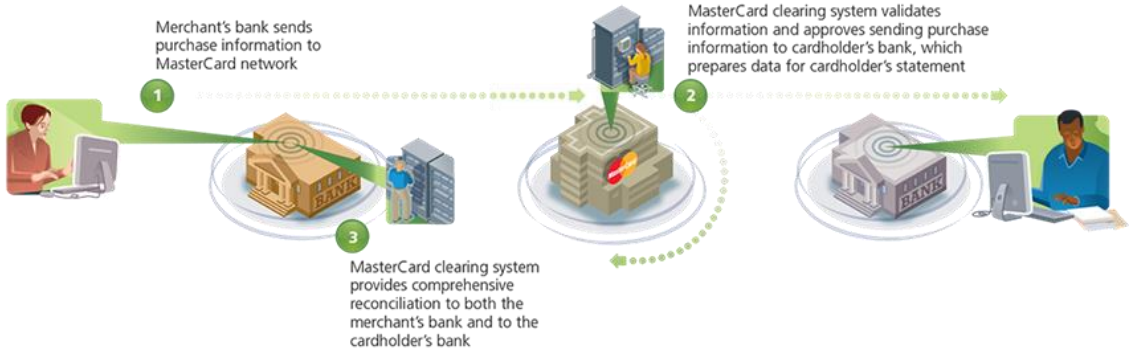
- ✓ Payment EMV cards
- ✓ The terminal reads card and talks to acquirer's host
- ✓ Transaction phases:
  - ✓ Authorization,
  - ✓ Clearing,
  - ✓ Settlement,
  - ✓ *Dispute resolution*

THE ANATOMY OF A TRANSACTION

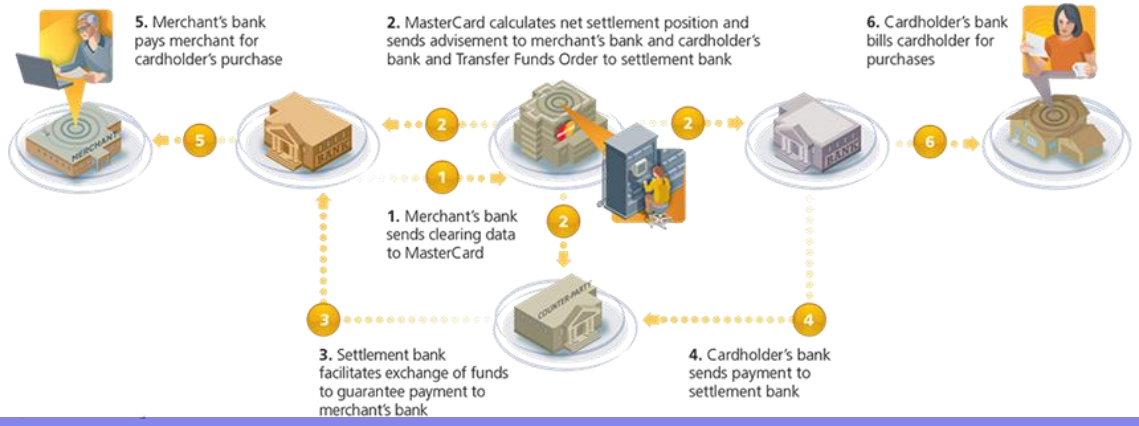
AUTHORIZATION
TIME OF PURCHASE FOR DUAL AND SINGLE MESSAGE TRANSACTIONS



CLEARING
USUALLY WITHIN ONE DAY FOR DUAL MESSAGE TRANSACTIONS; TIME OF PURCHASE FOR SINGLE MESSAGE TRANSACTIONS

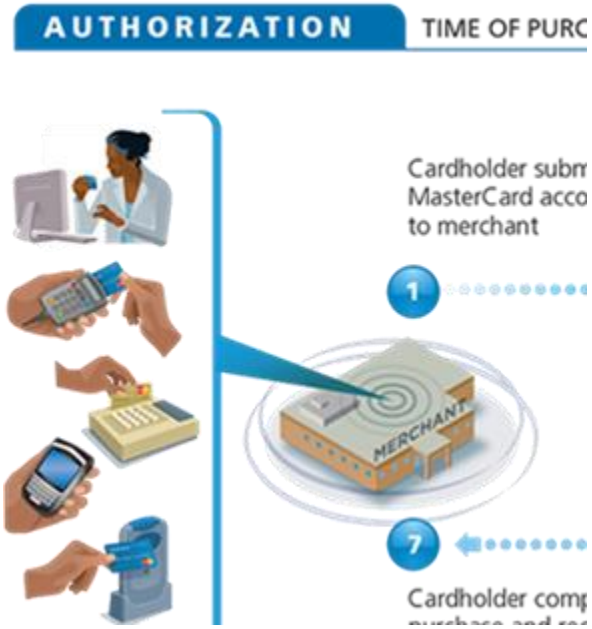


SETTLEMENT
USUALLY WITHIN TWO DAYS FOR DUAL MESSAGE TRANSACTIONS; TIME OF PURCHASE FOR SINGLE MESSAGE TRANSACTIONS



Secure Transaction

- **PIN**: personal identification number
- **PED**: pin entry device (e.g., **POS**: Point Of Sale, **ATM**: Automated Teller Machine)

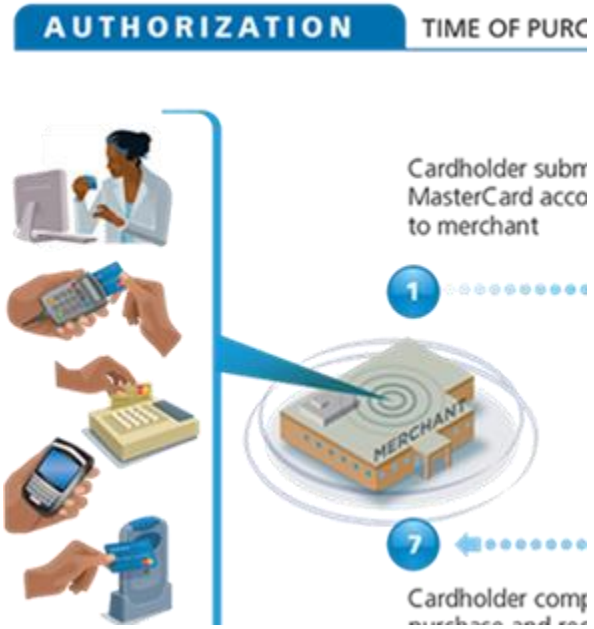


- **Acquirer**: bank or payment institution which accept card payment
- **Issuer**: bank or payment institution which manage the cardholder account

- **PAN**: Primary account number

Secure Transaction

- A **PED** has:
  - **TMK** [terminal master key] injected into PED and hardly changed
  - **TPK** [terminal PIN key] which is derived from TMK



- **Create PINBlock:** PIN and the card PAN

- **Encrypt the PINBlock:**
  - Create session key: **TPK** [terminal PIN key]

Chip Authentication Program (CAP)

- ✓ It uses the deployed "Chip & PIN" smart card infrastructure

- ✓ CAP operates in 3 modes: identity, respond, sign

- ✓ CAP implementation is based on the EMV* smart card protocol:
  1. Reader requests a list of all the data records stored by a card
  2. PIN verification
  3. Cryptogram generation

Chip Secrets – Attacks Methods

- ✓ **Non-invasive** attacks *(no physical harm to the chip)*
  - ✓ *low-cost*
  - ✓ *time consuming and not always successful*
  - ✓ *Ex.* side-channel attacks (such as Simple Power Analysis)

- ✓ **Invasive** attacks *(extracting information and understanding chip functionality)*
  - ✓ *expensive (requires a very sophisticated equipment and knowledge);*
  - ✓ *less time consuming and straightforward for many devices*
  - ✓ *Ex. partial reverse engineering followed by microprobing*

- ✓ **Semi-invasive** attacks *(direct access to the chip's surface)*
  - ✓ *moderate cost (some equipment can be easily built)*
  - ✓ *higher success rate compared to non-invasive attacks*
  - ✓ *some are easily repeatable and relatively quick to set up*
  - ✓ *Ex. optical fault injection attack*

Chip Secrets – Attacks Methods

- ✓ Security improvement:
  - ✓ Turn some ROM areas into reprogrammable Flash areas
    - ✓ Flash memory usually stores IP, sensitive data, passwords and encryption keys
    - ✓ Flash known vulnerabilities:
      - ✓ power glitching influence on data read from memory
      - ✓ laser scanning techniques reveal memory contents
  - ✓ Reprogram low-level features

Biometrics

- ✓ Recently, the cards have been easily cloned and used without user's knowledge
- ✓ Fingerprints problems:
  - ✓ Authentication fails if the user has a band aid on his finger
  - ✓ The fingerprint remains even the user is dead or unconscious
- ✓ Solution: authentication in two phases:
  - ✓ Iris recognition – identity
  - ✓ Palm vein technology - authentication

E-Commerce and Mobile Banking

E-Commerce Payment Systems

- ✓ Users can pay for online transactions using electronic payment
- ✓ A percentage of Internet users do not shop online because of a perceived risk of fraud
- ✓ Card verification number on credit cards transactions decreases the occurrence of frauds

Types of e-Commerce Payment Systems

- Credit Cards
  - Credit card number + date of expiry
  - Credit verification number (CVN) – to increase security
- Digital Wallets
  - Store personal information and payment
  - Are located on user's PC

- E-Cash
  - The money is exchanged electronically (PayPal)
- Mobile Payment
  - User sends payment request via text message

Mobile Payment (1)

- ✓ Mobile payments technology include:
  - ✓ NFC (Near Field Communications),
  - ✓ SE (Security Element), and
  - ✓ TSM (Trusted Service Manager)

- ✓ NFC does not offer native encryption → mobile payments need a SE (cryptographic module in the mobile device)

- ✓ Insecurity influences the adoption of mobile banking technology

Mobile Payment (2)

- ✓ Good points for mobile devices regarding security:
  - ✓ Are more protected against loss or theft
  - ✓ Users use them in a personal and confidential way

- ✓ Risks for mobile devices:
  - ✓ Malware
  - ✓ Malicious applications
  - ✓ Payments infrastructure/ecosystem
  - ✓ SMS vulnerabilities

E-Commerce Payment Systems - Comparison -

Payment systems	Properties	Costs	Advantages	Disadvantages
Electronic cash e.g., PayPal	– 31% of US population do not have credit cards – micropayments (< $10) – Independent – Portable – Divisible	– Internet cash transfer: no fixed cost of hardware – No distance costs – Small processing fee to banks	– Efficient – Less costly	– Money laundering – Forgery – Low acceptance – Multiple standards
Electronic wallets e.g., Passport	– Stores shipping & billing information – Encrypted digital certificate	– Lengthy download for client-side wallets	– Enter information into checkout forms automatically	– Client-side wallets are not portable – Privacy issue for server-side wallets
Smart cards e.g., Blue	– Embedded microchip storing encrypted personal information	– Time value of money	– Convenience	– Need a card reader – Card theft – Low acceptance
Credit cards e.g., VeriSign	– Line of credit – Purchase dispute protection – Secure Electronic Transaction (SET) Protocol	– Unpaid balance charge – $50 limit on frauds – Processing fee	– Most popular – Worldwide acceptance	– Costly

Protection for E-Commerce Bank and Credit Card Systems

- ✓ Existing cryptographic protection mechanisms: the PINs used at ATMs, the CVVs - are largely ineffective online
- ✓ Solution: Secure Sockets Layer Protocols (SSL) used with most Web browsers
- ✓ Risks: card transaction repudiation

Online-Banking Security

Authentication in Online Banking

Two-factor authentication using hardware devices (1)

- ✓ Due to low security of password verification → fraud problems for e-Banking and e-Commerce *(single-factor authentication not enough)*
- ✓ Comparison of hdw. auth. devices:

Method	Method of OTP Generation	Type of 2-Factor Solution
Push-Button Token (A)	User presses button on the device and a 6-digit access code is displayed	Know (Password) + Possess (Device)
Card-Activated Token (B)	User inserts their Bankcard into the card reader, presses button and a 6-digit access code is displayed	Know (Password) + Possess (Device) + Possess (Bankcard)
Chip and PIN-Secured Token (C)	User inserts their Bankcard into the card reader, enters card PIN and a 6-digit access code is displayed	Know (Password) + Possess (Device) + Possess (Bankcard) + Know (Card PIN)

Two-factor authentication using hardware devices (2)

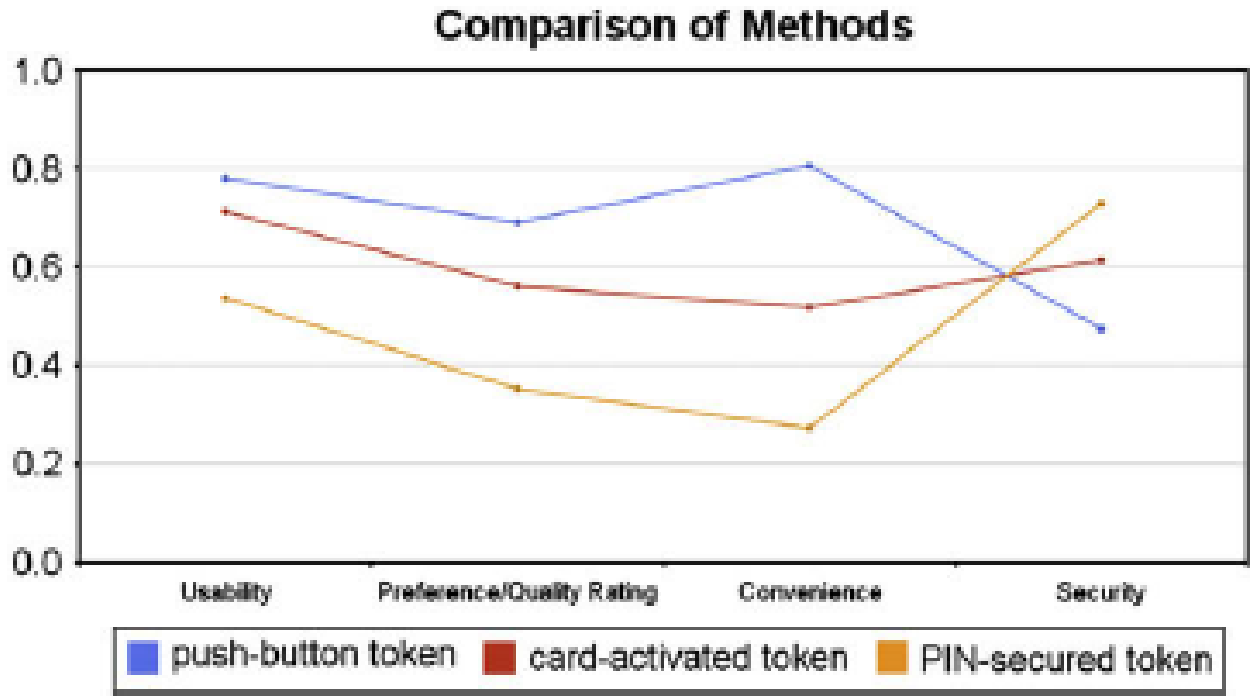


Fig. 5 – Usability, preference, convenience, security ratings for the three devices.

Two-factor authentication that does not use chips (1)

- ✓ Hardware devices (OTP) or software solution?
- ✓ Token-based devices presents weaknesses:
  - ✓ Easy to lost
  - ✓ Difficult to use
  - ✓ Requires middleware downloads and support
- ✓ Solution: two-factor authentication using 100% software solution

Two-factor authentication that does not use chips (2)

- ✓ **First factor**: A familiar, simple username/password interface
  - ✓ It provides the strength and protection of **PKI security**
  - ✓ It integrates with existing PKI-based applications and infrastructure (Identity Management/Single Sign On platforms)
- ✓ **Second factor**: A unique, software-only identity token that sits transparently in a user's device (e.g., laptop)

Two-factor authentication that does not use chips (3)

- ✓ Identity token:
  - ✓ Software equivalent of hardware smart card
  - ✓ Provides a PIN-protected software container for the user's credentials: a **digital certificate** (X.590v3) and an encryption **private key**
- ✓ Digital certificate - stored in container
- ✓ Private key - protected by a cryptographic camouflage

Two-factor authentication that does not use chips (4)

- ✓ Strong points of software-only identity systems:
  - ✓ Protection against attacks as: brute force attacks, man-in-the-middle *(OTP cannot do)*, phishing and key logging
  - ✓ Secure client that fraud-proofs the login process:
    - ✓ No expensive hardware
    - ✓ Rapidly scales to million of users
    - ✓ Runs on a variety of mobile platforms
  - ✓ Boost bank customers or employees confidence regarding data protection (familiar interface for the logging process)

Authorization in Online Banking

Authorization methods in Online-Banking (1)

- ✓ Code Card:
  - ✓ Plastic card with a set of fixed authorization codes
  - ✓ Good solution for private account holders
- ✓ Digipass GO3:
  - ✓ Small device that generates unique one-time password for transaction authorization with one push on the button (valid for 1 min)
  - ✓ Good choice for customers who are planning operations with high security level
- ✓ MobileSCAN
  - ✓ Online banking on mobile using MobileSCAN PIN code
  - ✓ No extra authorization tools needed

Authorization methods in Online-Banking (2)

- ✓ One Time Password (OTP): used as an additional factor in multi-factor authentication/authorization (usually sent by SMS)
  - ✓ The OTP is checked by the server and the transaction proceeds if valid
- ✓ Transaction Authentication Number (TAN) list for online transactions:
  - ✓ Indexed TAN list,
  - ✓ Indexed TAN with Captcha,
  - ✓ Mobile TAN,
  - ✓ TAN Generators (small HHT that generates a TAN)

Encryption in E-Banking

Encryption (1)

- ✓ Types of cryptographic algorithms:
  - ✓ **Secret Key Cryptography (SKC):** same key for encryption and decryption
  - ✓ **Public Key Cryptography (PKC):** one key for encryption, another for decryption
- ✓ Transaction security and privacy during e-banking depends on the **password** and **PIN code**

Encryption (2)

- ✓ Security goals: privacy, authenticity and repudiation can be achieved via digital signatures (it uses a secret and a public key) using RSA

- ✓ For SMS based secure mobile (Mobile banking): symmetric cryptographic techniques (common secret key)

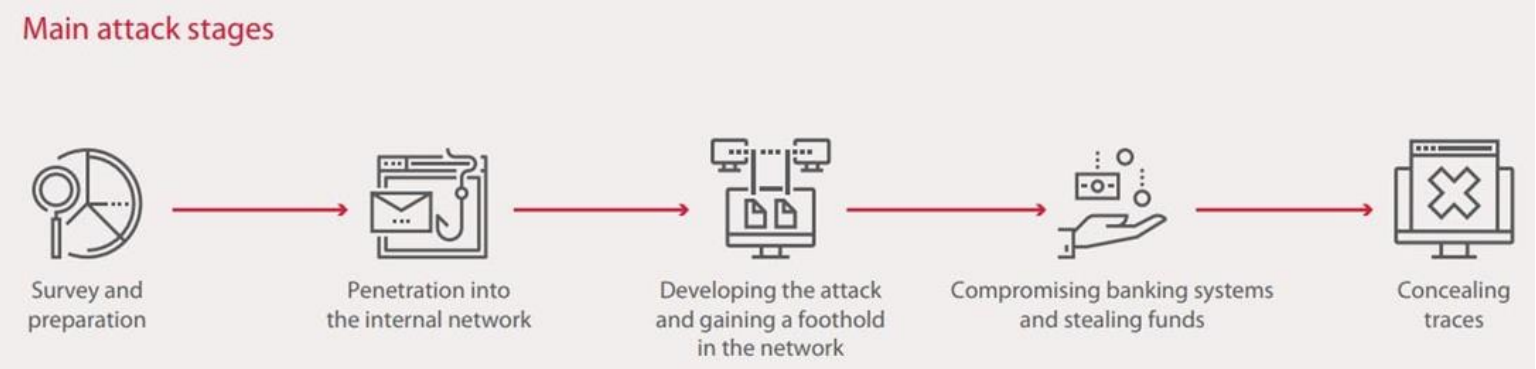
- ✓ Some ATMs: smart cards which enable the use of public key cryptography

Digital Signature Certificate

- ✓ Used to authenticate both the users and the banking systems itself
- ✓ Depends on the existence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA) who signs the certificates attesting their viability
- ✓ Provides an additional level of security safety and security for online banking transactions

E-Banking Attacks

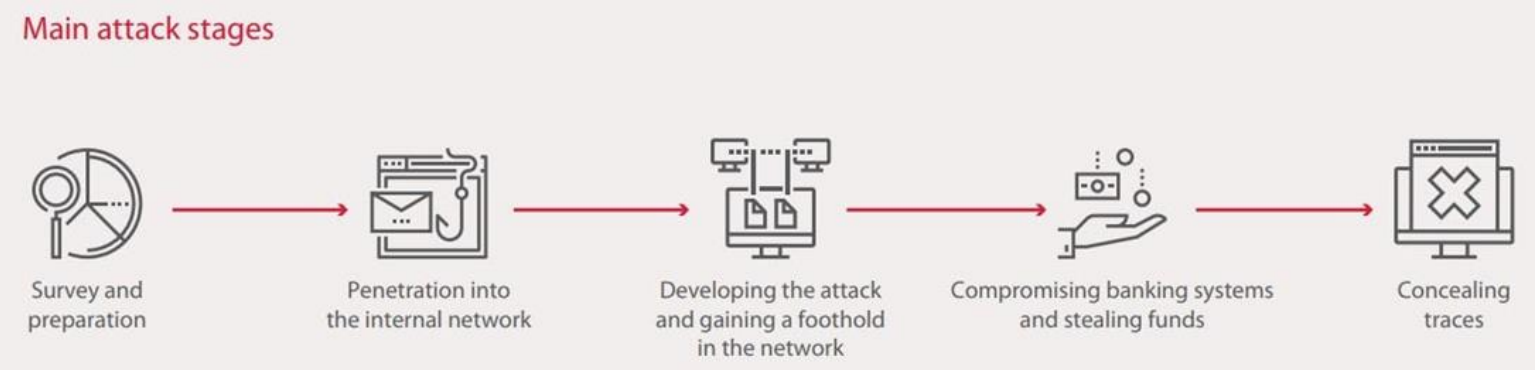
Typical attack scheme



Stage 1. Survey and preparation

- rather lengthy and time-consuming
- the task of gathering as much information about the bank as possible

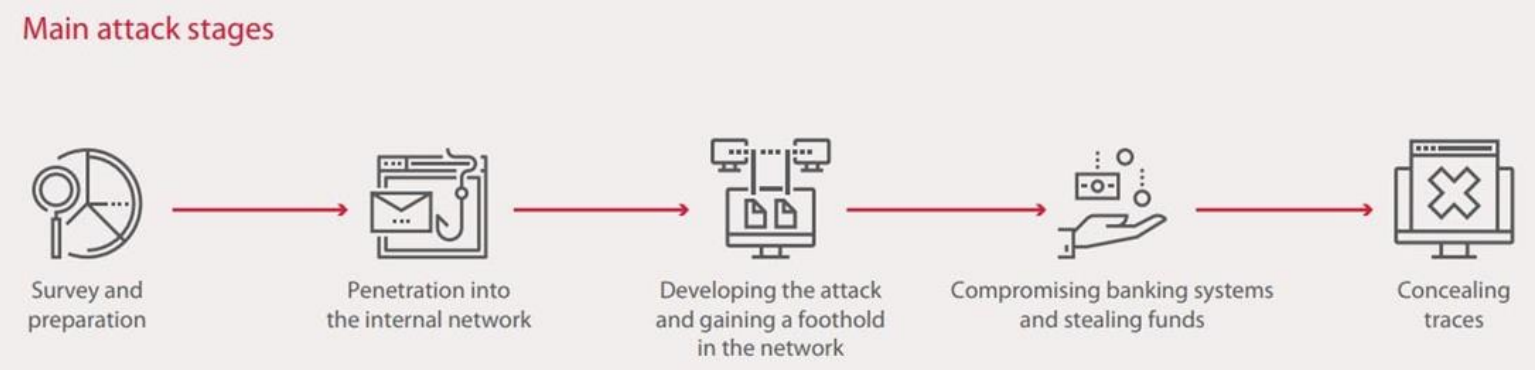
Typical attack scheme



Stage 1. Survey and preparation

- an attacker collects the following information about the bank:
  - Information about network perimeter systems and software
  - Employees Partners and contractors, as well as their systems and employees
  - Business processes

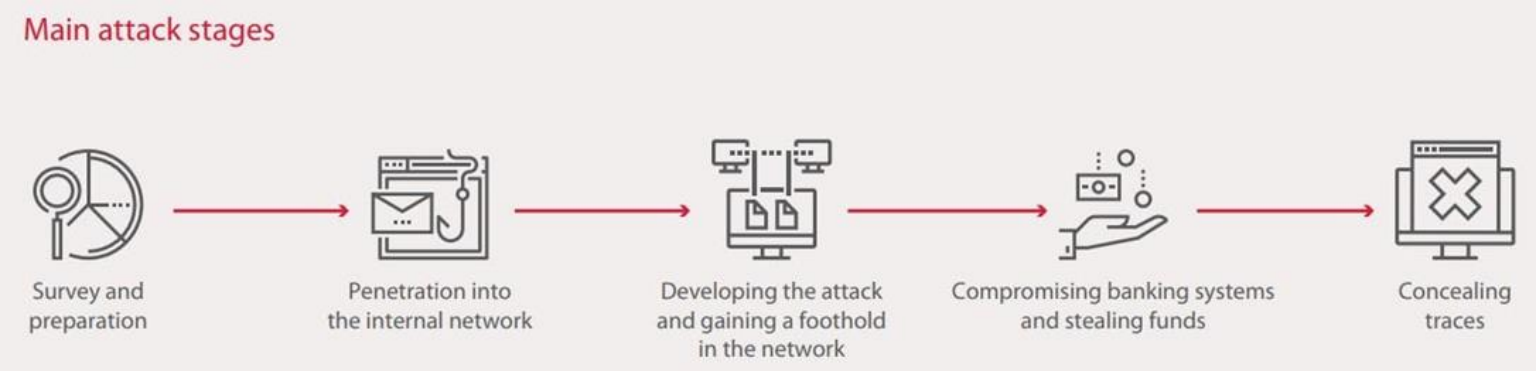
Typical attack scheme



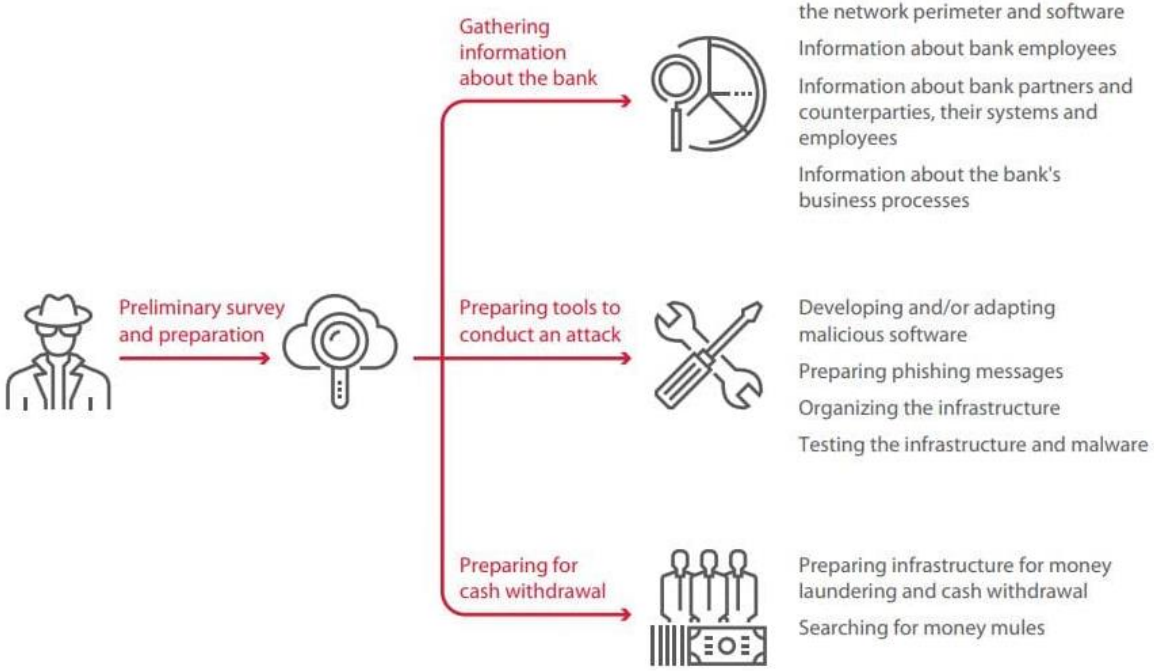
Stage 1. Survey and preparation

- examples of preparatory actions:
  - Developing or adapting malicious software
  - Preparing phishing emails
  - Testing the infrastructure and malicious software
  - MitM attack:
    - intercepts all traffic between the client and the server
    - Hides browser notifications about false web sites certificates

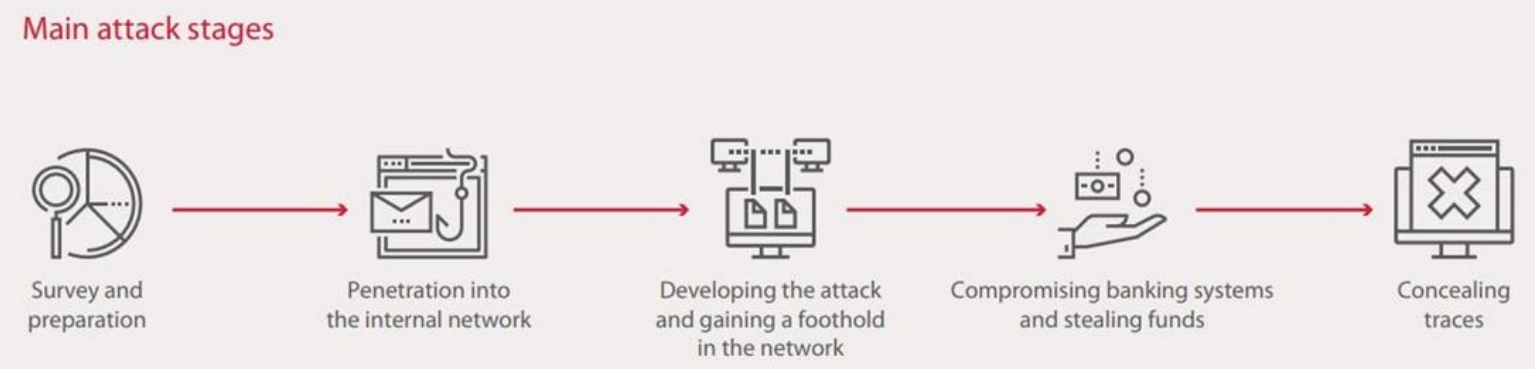
Typical attack scheme



Stage 1. Survey and preparation

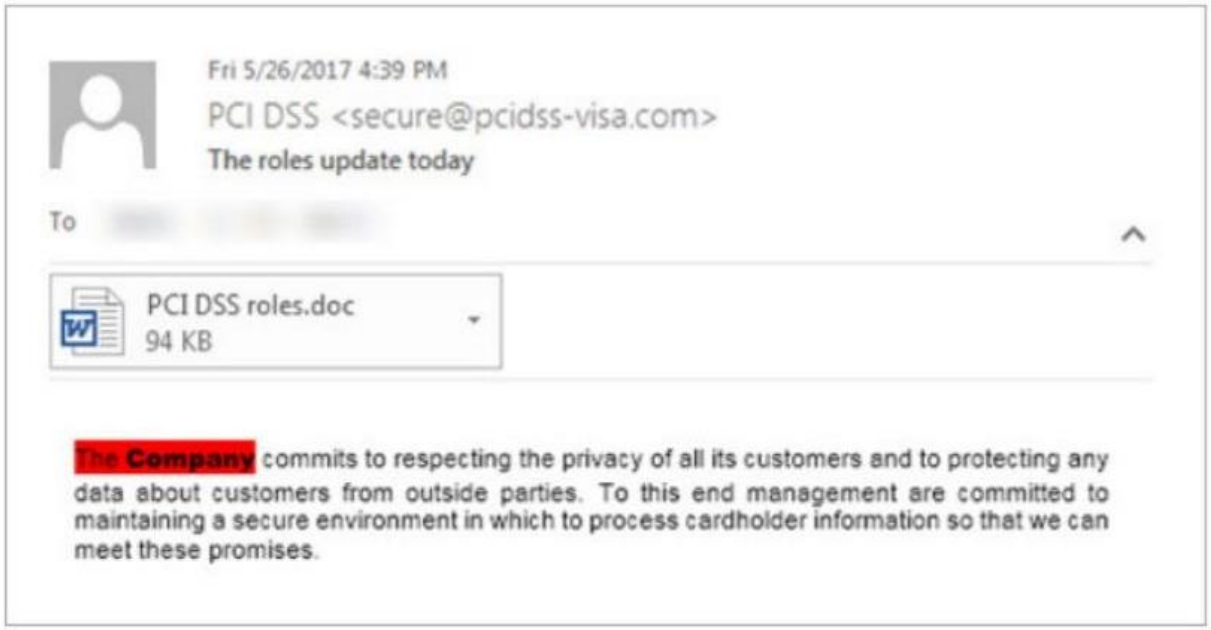


Typical attack scheme



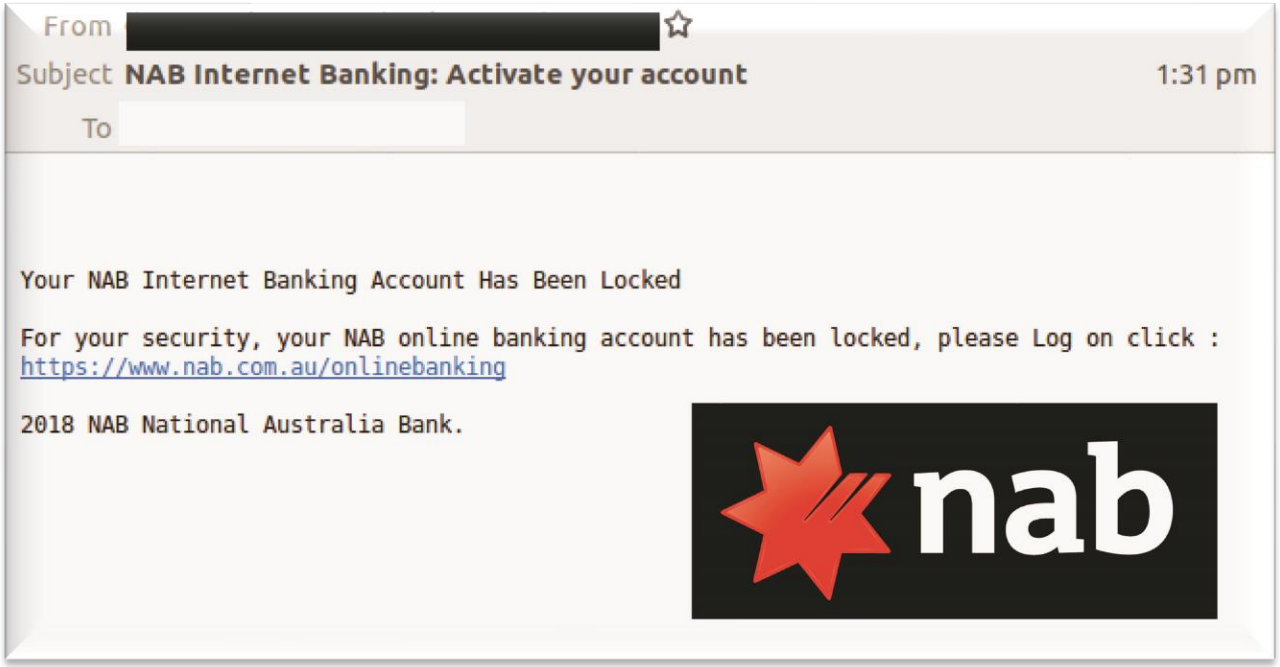
Stage 2. Penetrating the internal network

- Phishing:



Phishing

- ✓ A spoofed message that tries to trick the user to give its confidential information
- ✓ The number of phishing attacks are increasing:
  - ✓ ~482 million attempts in 2018 *(Kaspersky Lab)* [1] - 44 % of them in the banking financier system



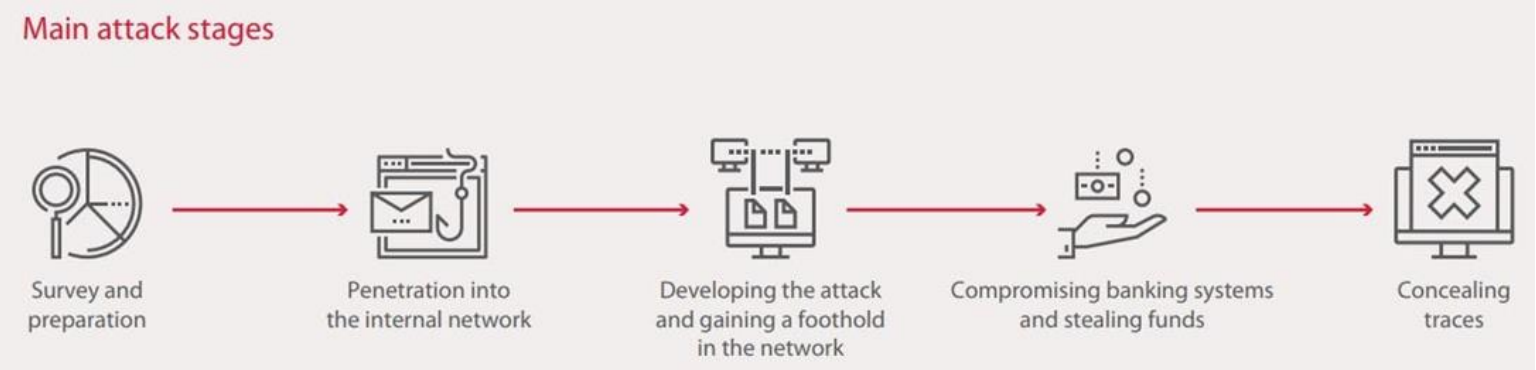
[1] https://www.itproportal.com/news/phishing-attacks-doubled-in-2018/

Phishing

- How?
  - *Traditional:* email links and attachments
  - social media feeds, search engines, browser extensions, pop-ups, chat bots, mobile apps, scareware, social engineering, malvertising*(the use of online advertising to spread malware)*

- Countermeasures:
  - E-mail and Web Page Personalization:
    - identifiable personal information could combat the risk of phishing attacks on bank users
  - Web Page Personalization
    - the bank users request a text or image to be used along with their passwords and usernames.
    - The users have to pass through two web pages when visiting their bank's website:
      - I. requires the user to provide a username. If the user name is valid →
      - II. personalized page for entering the password (personalized with the phrases or images that the user chose when he or she created the account)
  - Protection Software
  - Two-factor Authentication
  - Customer Awareness

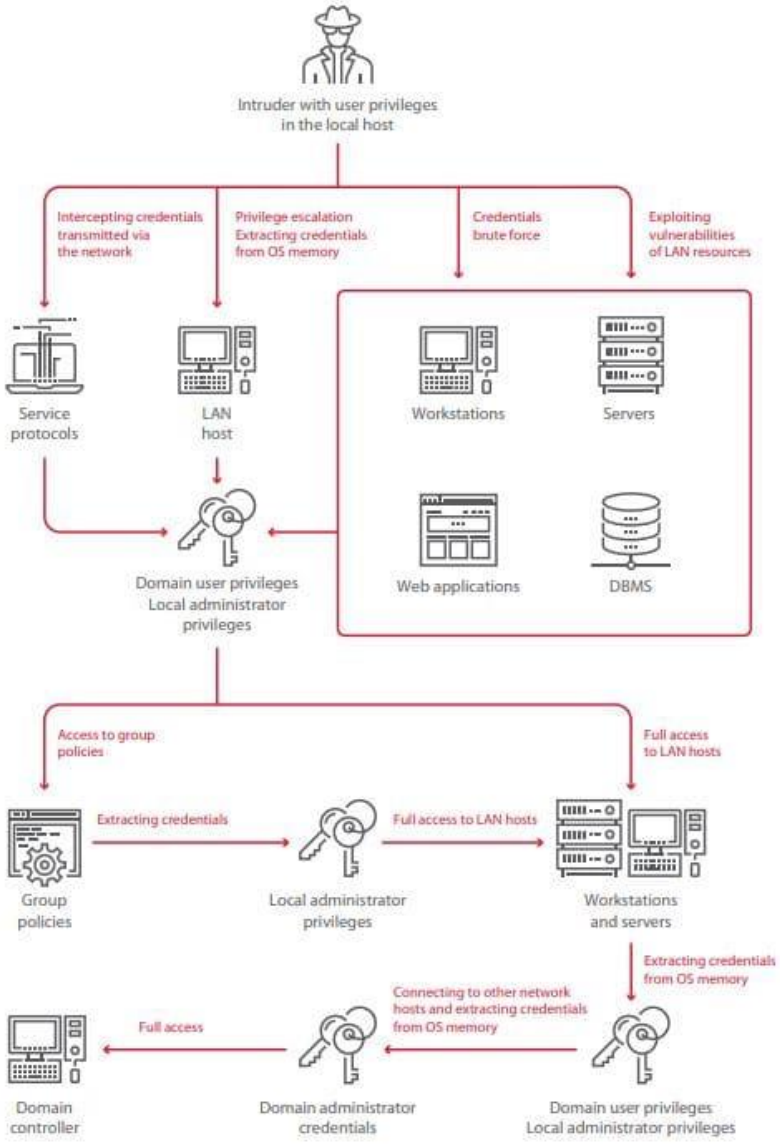
Typical attack scheme



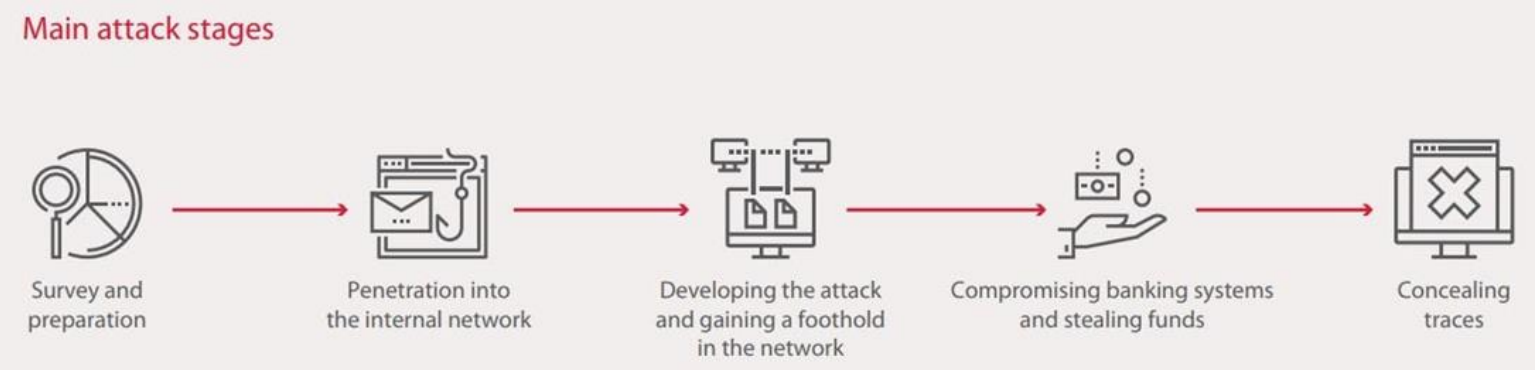
Stage 3. Developing the attack and gaining a foothold in the network

- Common vulnerabilities:
  - Use of outdated software versions and failure to install OS security updates
  - Configuration errors (including excessive user and software privileges, as well as setting local administrator passwords through group policies)
  - Use of dictionary passwords by privileged users
  - Absence of two-factor authentication for access to critical systems

Stage 3


Intruder with user privileges in the local host
Intercepting credentials transmitted via the network
Privilege escalation Extracting credentials from OS memory
Credentials brute force
Exploiting vulnerabilities of LAN resources
Service protocols
LAN host
Workstations
Servers
Web applications
DBMS
Domain user privileges Local administrator privileges
Access to group policies
Full access to LAN hosts
Extracting credentials
Full access to LAN hosts
Group policies
Local administrator privileges
Workstations and servers
Extracting credentials from OS memory
Connecting to other network hosts and extracting credentials from OS memory
Full access
Domain controller
Domain administrator credentials
Domain user privileges Local administrator privileges

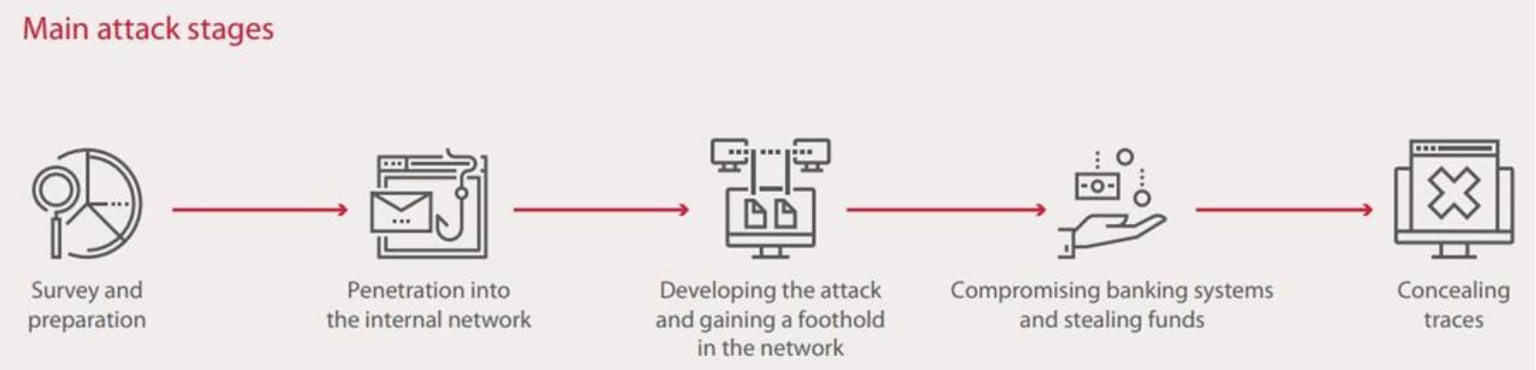
Typical attack scheme



Stage 4. Compromising banking systems and stealing funds

- The main methods of theft are:
  - Transferring funds to fictitious accounts through interbank payment systems
  - Transferring funds to cryptocurrency wallets
  - Controlling bank cards and accounts
  - Controlling ATM cash dispensing

Typical attack scheme



Stage 5. Concealing traces

- To impede investigation of incidents,
- Although many attackers use RAM-resident malware, signs of their presence in the system still remain: entries in event logs, changes in the registry, and other hooks.

- Possible approach: erase boot records and hard disk partition tables on network hosts, disabling them entirely

Common Malware

- **Spyware and Adware**
  - Spyware: type of software that secretively collects user information while on the Internet
  - Adware: type of spyware used to tack user's habits and interests for customizing future advertising material

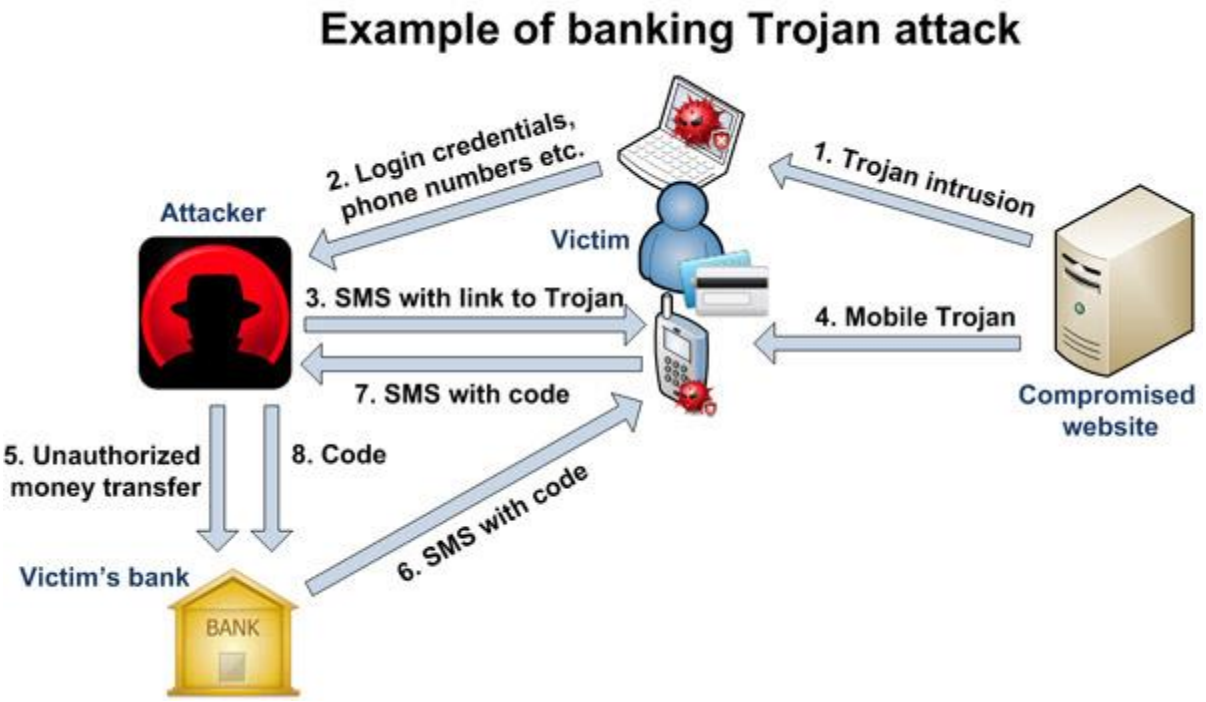
Common Malware

- **Viruses:** software that reproduce and attach itself to other programs
  - Countermeasures:
    - Anti-virus software
    - Not accepting attachments from emails of unknown sources

- **Keyloggers:** while accessing the Online Banking keylogger copies every keystroke typed on that PC

Common Malware

- ✓ **Trojans:** destructive program that poses as a harmless application



Q&A