DCIT

Internet Banking Attacks

Karel Miko, CISA
DCIT, a.s. (Prague, Czech Republic)
miko@dcit.cz

Contents

Agenda

- Internet banking today
- The most common attack vectors
- The possible countermeasures
- What protection is the best?
- The biggest threats – now & near future

Electronic banking today (1)

Internet banking systems

- Nowadays nearly every bank provides the clients with an access to their accounts over the internet

The other electronic channel

- Mobile banking (PDAs, mobile phones, …)
- Phone banking (old-style but still widely used)

Non-banking services (not in our scope)

- Stock (securities) trading online
- Long existing credit card payments

Electronic banking today (2)

All banks claims something like this:

- *We take internet security very seriously and use industry standard technology and practices to safeguard your account …*

Is the Internet Banking really safe?

How do we define Internet Banking

Internet banking does not mean only the bank side - you have to see it a complex

- Client side (=PC/browser)
- Network infrastructure (=Internet)
- Server side (=bank)

Every part can be subject of an attack:

- The hackers will choose the easiest way
- Generally the easiest seems to be attacking the user or his/her PC

Internet Banking hackers

DCIT

A hacker needs

- Knowledge (if not clever enough he/she can buy it)
- Motivation (in this case – money)

A hacker might not be a typical criminal

- Bank employees – no so often (they know better ways, how to commit a fraud)
- ISP (internet service provider) employees
- Mobile operator employees

Internet Banking frauds (1)

First you need an access to victim‘s bank account – but what next?

Trading the stolen credentials

- passwords, PINs, certificates etc.
- 10-1000 $ per account (compare to credit card: 0.5-20 $)

„Mule“ accounts

- Recruitment of genuine customers to receive the money from fraudulent transactions

Pump and dump transactions

- Dupe victim to unwittingly participate in unprofitable transaction – mostly used with stocks trading

Internet Banking frauds (2)

Comparing to credit card frauds

- Internet banking frauds – significantly lower volume
- Credit cards – more global
- Internet banking – local differences (not only USA vs. EU, also within EU)

It is not always about the money:

- Denial of Service Attacks = making the bank server unavailable to real clients
- Harming the bank image in other way

How do they break in?

The main „Attack Vectors“:

- Attacking server-side (=bank server)
- Credential stealing
- Phishing (social engineering)
- Pharming
- Man-in-the-middle
- Man-in-the-browser
- Generally – attacks utilising Trojan horses
- Cross-channel Attacks

Note: It is not a complete list – the area is dynamically evolving

Attacking server-side

The internet banking servers

- Mostly protected enough (more or less)
- Under full control of the bank (unlike the clients‘ PCs)

The successful attacks are nowadays quite rare but might happen

- It is more about stealing clients‘ personal data, transaction history etc. than fraudulent transactions

Denial of Service

- Hardly to protect against especially Distributed DoS
- Mostly thousands of computers involved (botnets)

Credential stealing (1)

The oldest and simplest attack

- Stealing user passwords, PIN, certificates or whatever is needed to access the bank account
- The success of this kind of attacks depends on authentication method used
- Vulnerable authentication: static PIN/password; certificate (in a file) + password

How does it work?

- Mostly via malicious SW (virus/trojan) at clients‘ PC (keylogger, browser eavesdropping, …)

Credential stealing (2)

The attack has two phases

- 1. Stealing the credential
- *(maybe trading the credentials)*
- 2. Abusing the credentials

Stealing vs. Abusing

- Different times,
- Different computers
- Different geographical locations
- Which makes it possible to detect and/or investigate

Phishing (1)

What is Phishing

- Phishing = phreaking + fishing
- **The goal:** to get a sensitive information from the genuine bank client (e.g. PINs, passwords, credit card numbers, etc.)
- Based on social engineering

How does it work?

- Luring the users into a fake website that looks very similarly to the real bank site
- Mostly via links in email messages

Phishing (2)

- Example (source: http://antiphishing.org)

Phishing (3)

DCIT

BROWSER

https://www.bigbank-secure.com/

Welcome to BigBank

Internet Banking Login:

ID:

Password:

PIN:

submit

FAKE SITE
- Usually different domain
- Mostly copy of frontpage
- Visually very similar
- After entering data an error ocures

BROWSER

https://www.bigbank.com/

Welcome to BigBank

Internet Banking Log

ID:

Password:

PIN:

submit

REAL SITE

The real bank cannot do much as it stays aside the attack

4. user credentials go to the hacker

URL leading to the fake server

3. the victim believes that he/she is talking to BIGBANK

E-MAIL MESSAGE received by VICTIM

From: faked.address@bigcompany.com
To: victim@otherdomain.com
Subject: You must look at this ...

Dear Sir,

You have immediately log into your internet banking, otherwise ...

http://www.bigbank-secure.com/login.asp.

hacker

H

victim

V

2. the victim opens the mail and cklicks on the URL

1. the hacker sends an e-mail with malicious URL

DCIT

Phishing (4)

Phishing variants

- **Basic**
  - Pure site copy
  - Mostly only login page
  - Fake site usually installed on more than one server
  - **This is what we can see nowadays**
- **Advanced**
  - Phishing proxy
  - Fake domain e.g. *www.bigbank.cn* + proxy "translating" all request to the original server *www.bigbank.com*
  - **This is what we will see in the future**

Pharming (1)

- After phishing started a “ph-fashion” another slightly advanced technique appears
- Pharming = phreaking + fishing
- **The goal:** the same as by phishing (stealing PINs, passwords, credit card numbers, etc.)

How does it work?

- Not Based on pure social engineering
- Some technical tricks involved (DNS reconfiguration)
- Mostly requires a trojan horse/virus on victims computer

Pharming (2)

What is the main trick?

- The attacker again needs to bring the user to the fake site (e.g. fake internet banking server)
- It is not done via e-mail + link
- The redirection is done by reconfiguration of some networks settings (on user PC, home internet router etc.) – for that an attacker needs a malicious SW.
- Apart from phishing in case of pharming user sees the correct URL in browser location bar

Man-in-the-middle (1)

Characteristics:

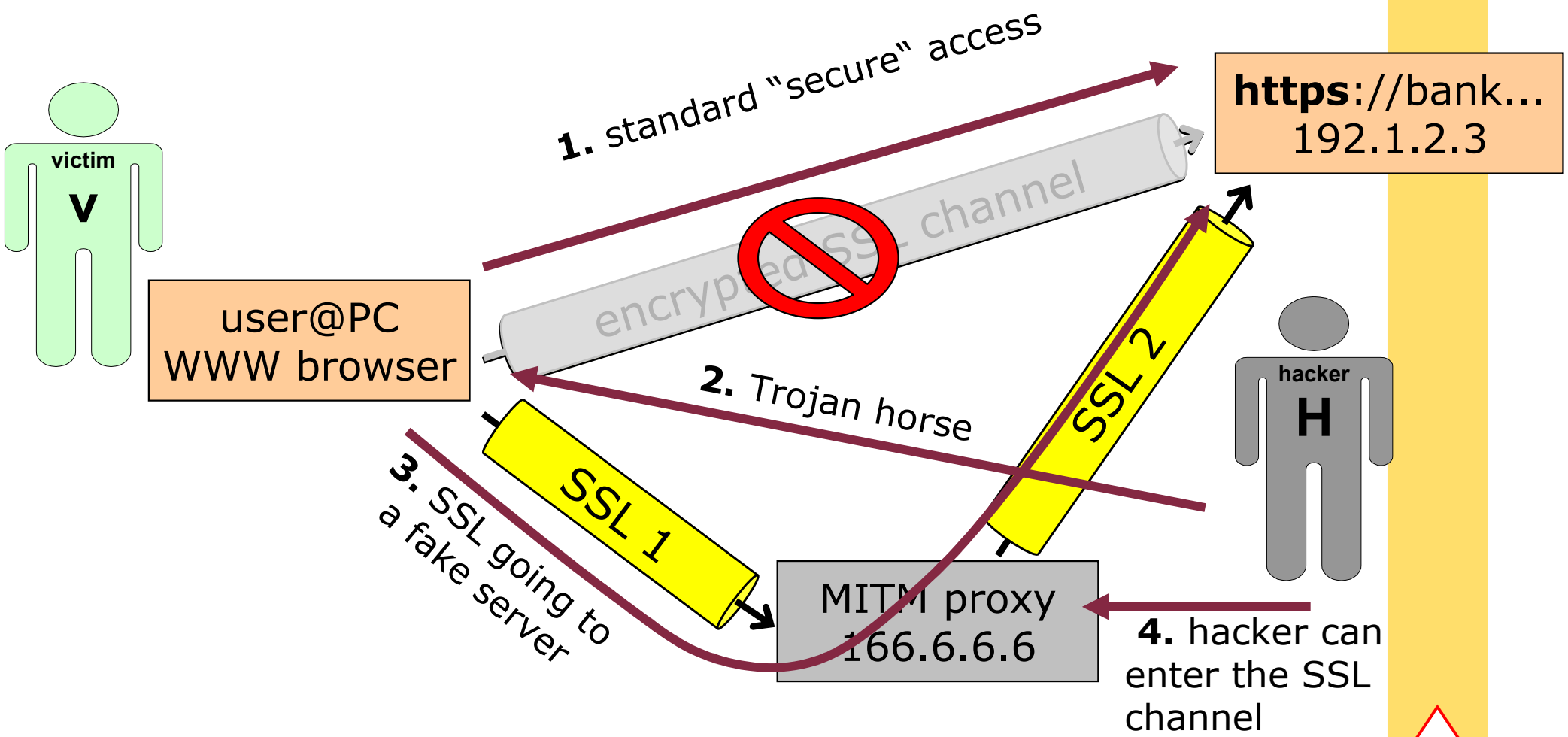
- Category of sophisticated attacks
- Encrypted SSL connection (https://…) was considered as proof to communication eavesdropping
- However there are scenarios that allows the hacker to see or even to modify (!) the communication between the client and the bank

The attacker needs to have a trojan horse on the victim computer

Man-in-the-middle (2)

DCIT

MITM Scenario:



DCIT

Man-in-the-browser (1)

Characteristics:

- Category of very sophisticated attacks
- Even some very advanced technologies are vulnerable to this attacks
  - HW generators of one-time-passwords
  - One-time-passwords sent by SMS
  - Pre-generated password tables (TAN codes)
  - Digital signatures via smartcards (most of them)
- Again needs a trojan on victim computer
- The protection is not easy
  - Either expensive or uncomfortable to the users

Man-in-the-browser (2)

MITB Frauds

- The fraudulent transaction is done from victim's computer
- It is made during the time the victim works with internet banking
- It is done "silently" without asking the victim for anything
- **Thus extremely hard to detect and/or investigate**

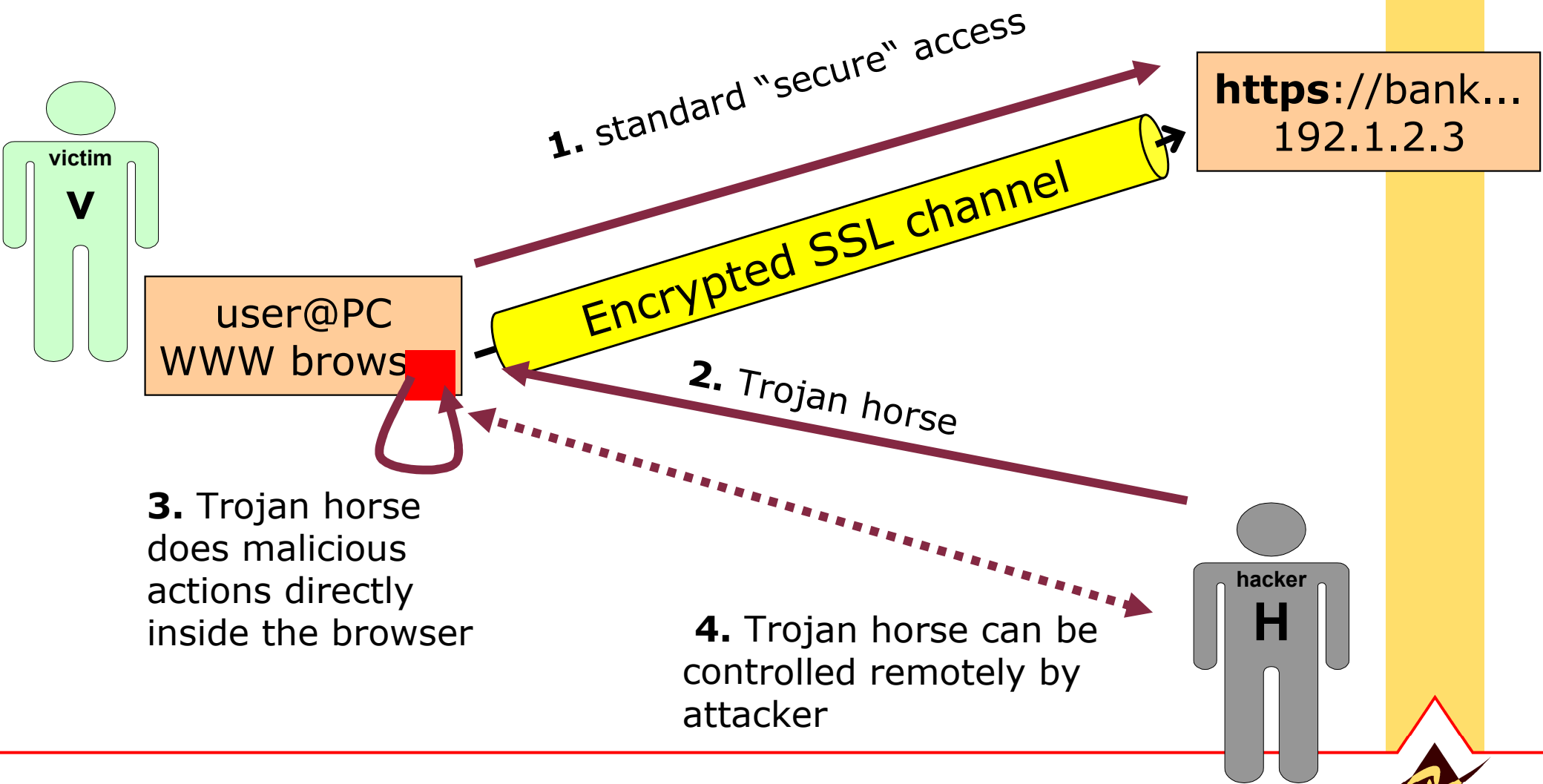
Not widely used (yet)

- As today there are still simpler ways

Man-in-the-browser (2)

DCIT

MITB Scenario:



DCIT

Attacks utilising Trojan horses (1)

Trojan Horse = The Ultimate Enemy No.1

- Today but also in the future

Attacks utilising Trojan horses (2)

Trojans (malicious SW)

- Simple (keyloggers, steal file/password)
- Sophisticated (remotely controlled, highly organised in botnets)

Trends

- Generic Trojan Horse Kits (make your own custom trojan)
- Remotely controlled Trojans (dynamically updating the malicious actions performed on victim computer)
- Rootkit variants – extremely hard to detect
- The old-fashioned antivirus approach (pattern matching) absolutely inefficient

Attacks utilising Trojan horses (3)

Infection of client computer

- The “old-school”
  - E-mail attachments
  - Email with link to malicious URLs
  - Links in social networks / instant messaging (ICQ, Skype)
  - Packed in popular free software.
  - CD-ROM/USB Stick
- The “new-age”
  - Drive-by malicious sites (just look at a webpage and you have a problem) – vulnerable browser/flash player/…
  - Hide from personal firewalls, antivirus/antispyware SW

Cross-channel Attacks

The most common scenario

- Stealing a payment card number + other info through internet banking (via phishing)
- Later abusing it for payment card fraud

Credit card → Internet banking

- Some internet banking systems use the payment cards for authentication (EMV CAP/DPA technology)
- If badly implemented the physically stolen card can open an access to Internet banking

How to protect? (1)

There are basically two main area the banks have to handle

- The user authentication
  = whether the user is who he/she claims to be
- The transaction authorisation
  = whether the user is allowed (authorized) to perform particular transaction

The protection of the client side

- Completely out of bank control
- The biggest issue – thus the primary attack target

How to protect? (2)

Generally good ideas

- Using trusted HW devices
  - = HW calculators, HW password generators, smart card readers, mobile phone
  - Assume that the computer is under attacker control (e.g. via Trojan Horse)
- Using alternate channel (OOB – out of band)
  - = SMS messages, phone calls, …
  - Assume that all the communication computer ↔ Internet is under attacker control

However even those Hi-Security technologies might not be enough

How to protect? (3)

DCIT

One-time-passwords (OTP)

- TAN codes, GRID cards, HW tokens, EMV chip OTP

	1	2	3	4	5	6	7	8
A	4650	8234	5098	9559	6794	8968	5395	7665
B	1441	8285	4239	9595	9338	5563	7488	6966
C	6565	7614	9155	9855	9261	9628	9874	4107
D	1775	5631	3231	8739	6358	1543	6231	5906
E	1518	6899	6965	1580	8982	4696	6258	6979
F	3476	9048	6221	7091	4770	8863	6681	2931
G	5633	6948	4199	9782	6075	8138	4135	6241
H	1339	6406	4105	5983	2880	8715	5204	8210

Serial No.: 0123456789

- Solves only credential stealing. The confirmations **codes are not linked with authorising transaction**
- **Totally vulnerable to MITM + MITB**

DCIT

How to protect? (4)

Challenge response technologies

- HW tokens (or SW calculators)

- If the challenge is meaningless number then it is **vulnerable to MITM + MITB**
- User has to enter the transaction details (account number, amount) into the calculator – uncomfortable

How to protect? (5)

SMS security codes

- If it is just pure code without additional information it is equivalent to OTP
- For authorization SMS has to contain transaction details, otherwise **vulnerable to MITM + MITB**

PKI technologies (certificates + signatures)

- Certificates in a file – **vulnerable to credential stealing (very easily)**
- Certificates on a smartcard – depends on the implementation (mostly **vulnerable to MITB**)

How to protect? (6)

A lot of new approaches – for example:

- visual transaction signing (visual cryptogram) http://www.cronto.com/

- IBM Zone Trusted Information Channel (ZTIC)

How to protect? (7)

There are many other technologies

- Mobile technologies (SIM toolkit)
- Optical keys
- Introduced some time ago – secure enough but not widely used

The main problem of internet banking security technologies

- Either expensive or uncomfortable for the user

How to protect? (8)

To Conclude: There is no “golden bullet”

- No technology brings the “final solution”
- The guys on the other side are very adaptive – we are aiming at moving target

If technology is not good enough

- If bank cannot prevent it at least detect it
- The importance of interne banking fraud detection systems will rise

Questions?