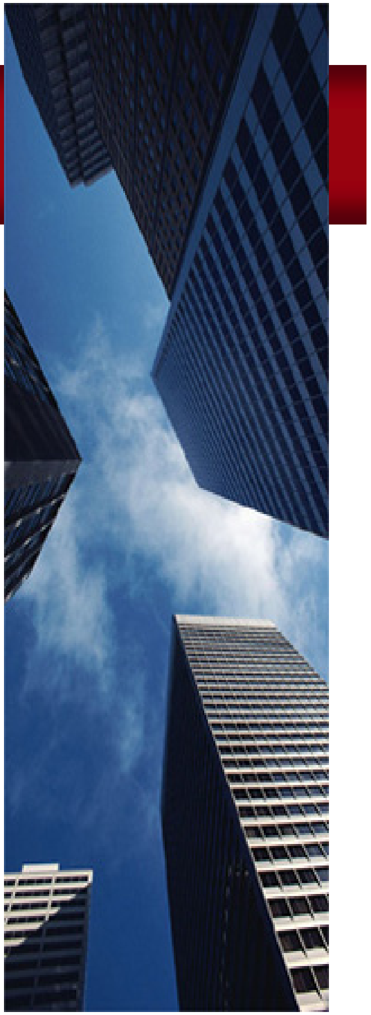
Authentication and Transaction Security in E-Business

AXSionics AG, BFH Spin-off Park, Seevorstadt 103b, CH-2501 Biel-Bienne

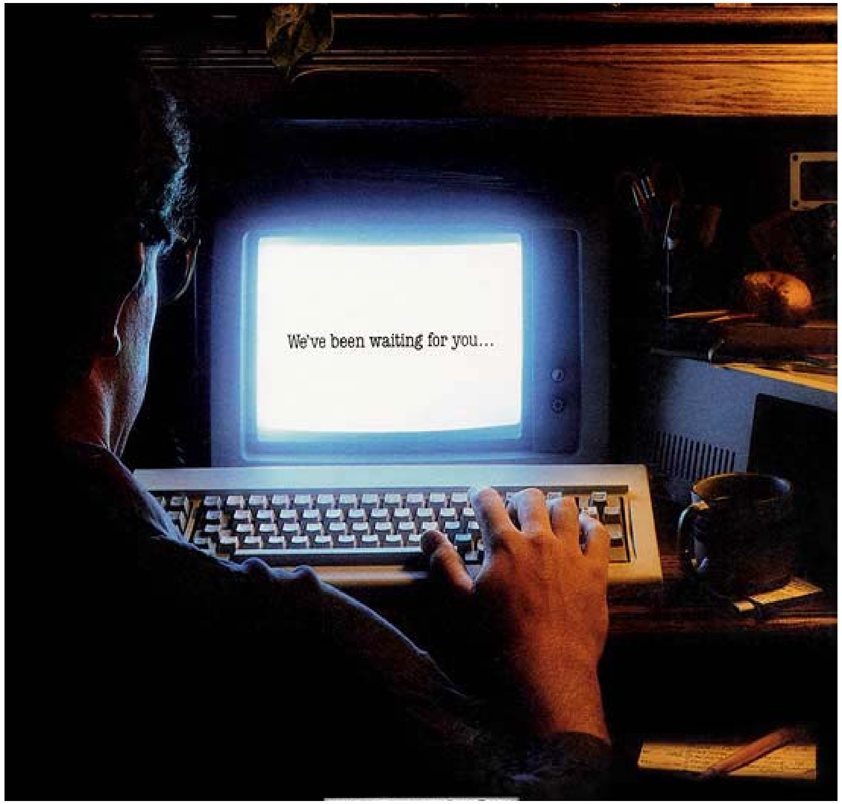
Lorenz Müller
Mobile: +41 79 341 03 26
Lorenz.mueller@axsionics.ch

Overview

- Phising – what it is, how it works…
- Malware – a landscape
- Role of authentication and transaction security
- Authentication with biometrics
- AXS Authentication System™



Bank robbery – what is your style?



Old goals – new methods

The goal of most crimes is to get money!

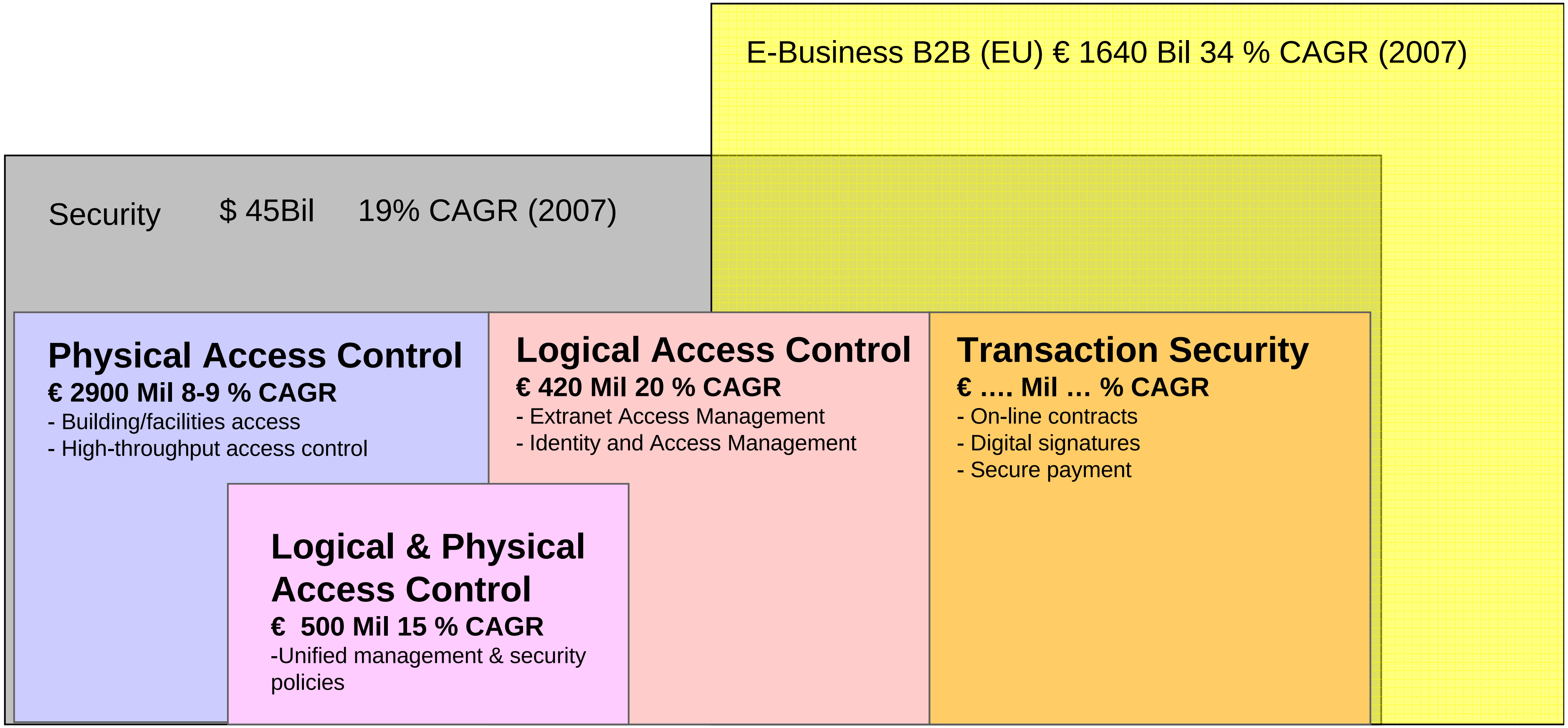
Classical attack

- Personal presence
- Hard work
- Single copy
- Limited action range
- High risk
- High success rate is critical

Cyber attack

- Remote attack
- Available tools
- Automated industrial copies
- Worldwide action range
- Low risk
- Low success rate is sufficient

Market perspectives and indicators



E-Business B2B (EU) € 1640 Bil 34 % CAGR (2007)

Security $ 45Bil 19% CAGR (2007)

Physical Access Control
€ 2900 Mil 8-9 % CAGR
- Building/facilities access
- High-throughput access control

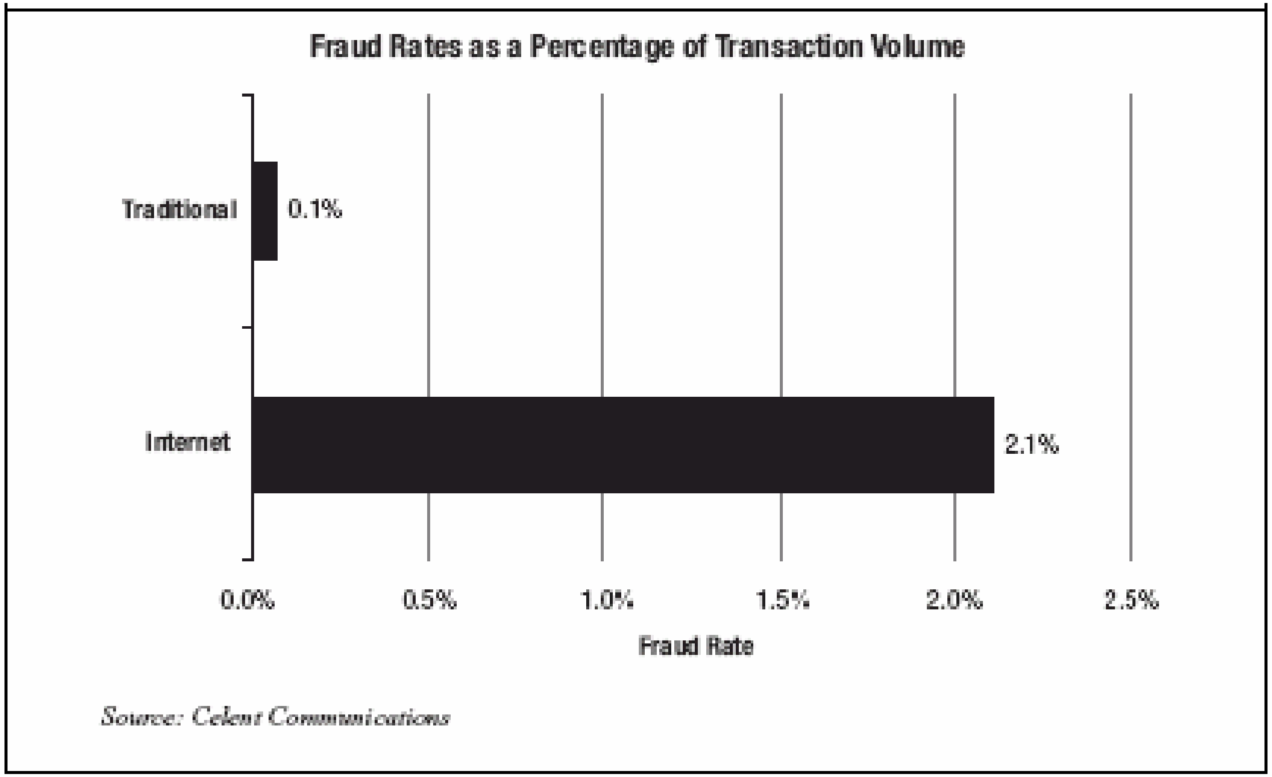
Logical Access Control
€ 420 Mil 20 % CAGR
- Extranet Access Management
- Identity and Access Management

Transaction Security
€ .... Mil ... % CAGR
- On-line contracts
- Digital signatures
- Secure payment

Logical & Physical Access Control
€ 500 Mil 15 % CAGR
-Unified management & security policies

Source: Gartner Group

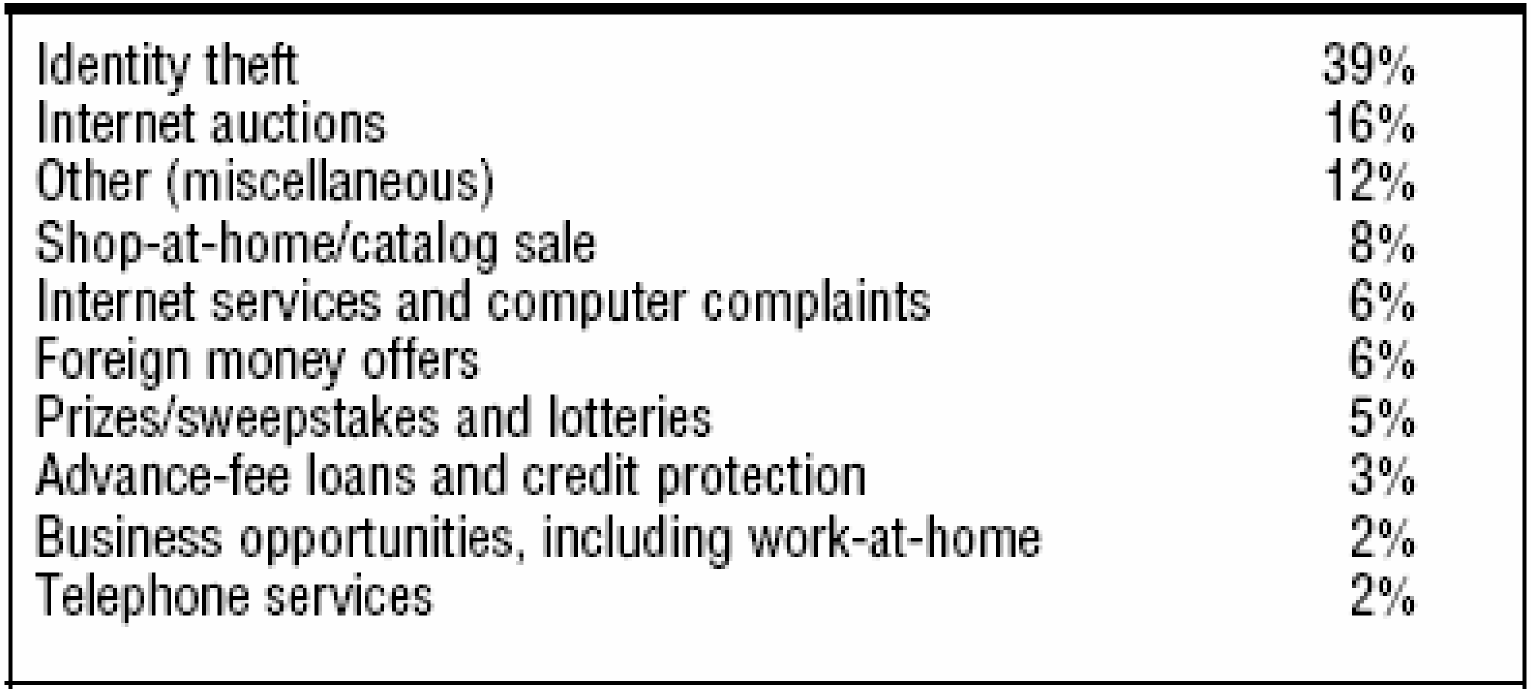
Fraud Rate in the Cyber Space



Source: Celent Communications

US credit card based transactions: 2004

Fraud Types in non-physical interactions



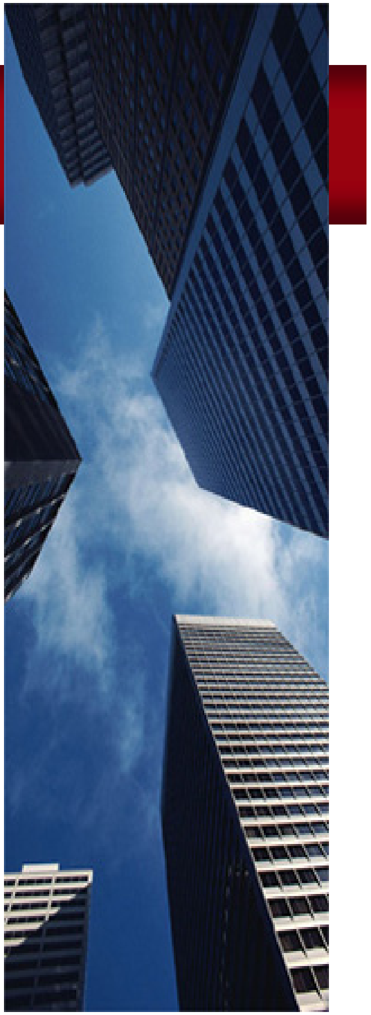
Identity theft	39%
Internet auctions	16%
Other (miscellaneous)	12%
Shop-at-home/catalog sale	8%
Internet services and computer complaints	6%
Foreign money offers	6%
Prizes/sweepstakes and lotteries	5%
Advance-fee loans and credit protection	3%
Business opportunities, including work-at-home	2%
Telephone services	2%

US Federal Trade Commission's:
Top Categories in 2004 for Consumer Fraud Complaints

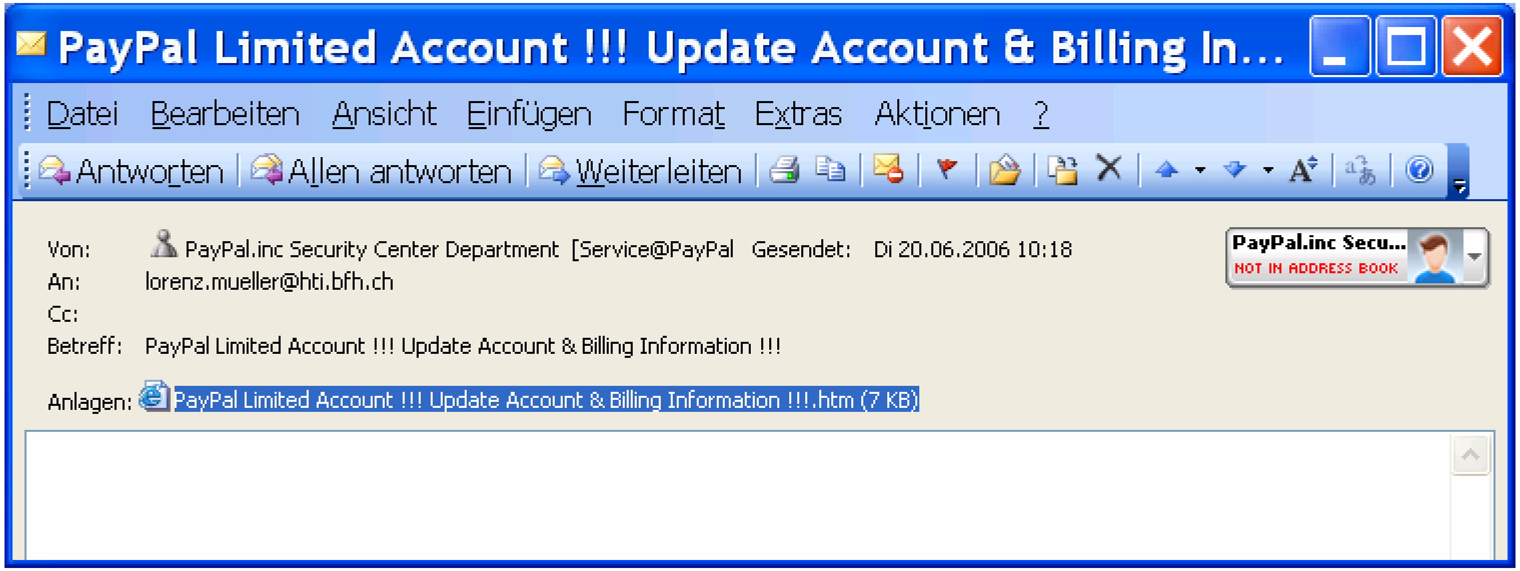
Source ISACA

Phising – what it is, how it works…

- **A few examples**
- **How to set-up a phising attack**
- **Facts and figures**
- **The business case**



Phising Mail PayPal



PayPal Limited Account !!! Update Account & Billing In...
Datei Bearbeiten Ansicht Einfügen Format Extras Aktionen ?
Antworten Allen antworten Weiterleiten
PayPal.inc Secu...
NOT IN ADDRESS BOOK

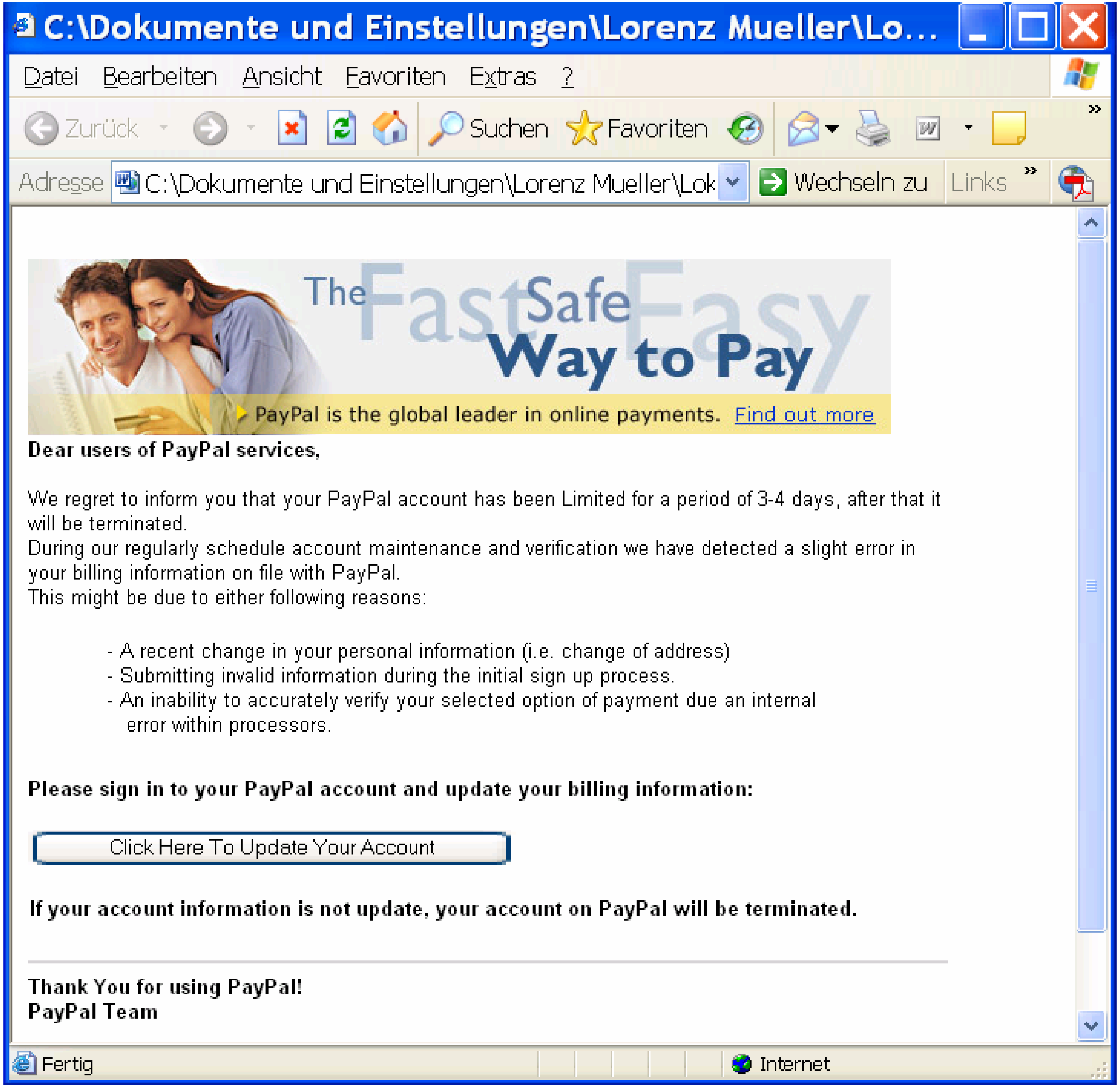
Von: PayPal.inc Security Center Department [Service@PayPal Gesendet: Di 20.06.2006 10:18

An: lorenz.mueller@hti.bfh.ch

Cc:

Betreff: PayPal Limited Account !!! Update Account & Billing Information !!!

Anlagen: PayPal Limited Account !!! Update Account & Billing Information !!!.htm (7 KB)



C:\Dokumente und Einstellungen\Lorenz Mueller\Lo...
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Adresse
C:\Dokumente und Einstellungen\Lorenz Mueller\Lok
Wechseln zu
Links
The Fast Safe Easy
Way to Pay
PayPal is the global leader in online payments. Find out more
Fertig
Internet

Dear users of PayPal services,

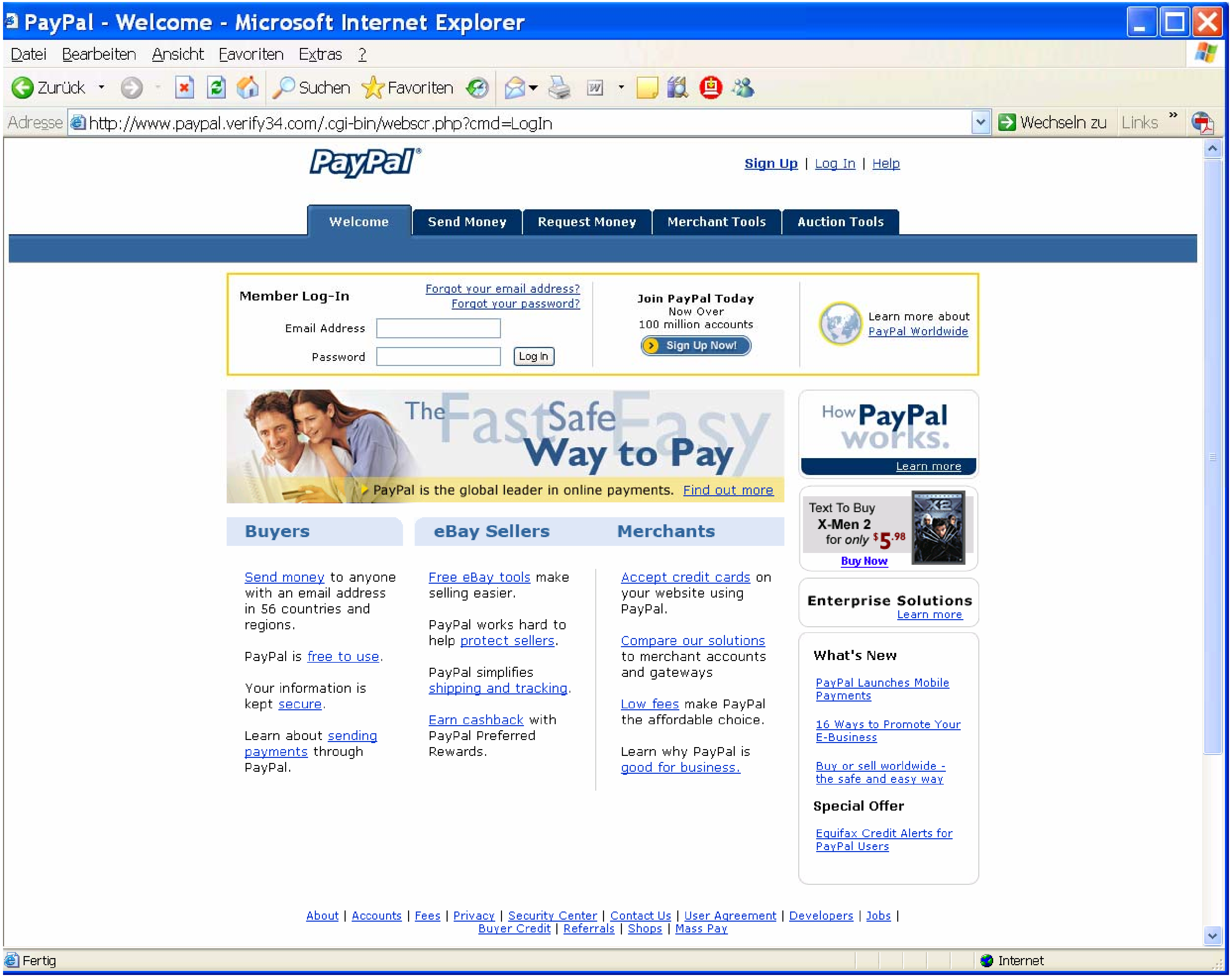
We regret to inform you that your PayPal account has been Limited for a period of 3-4 days, after that it will be terminated.
During our regularly schedule account maintenance and verification we have detected a slight error in your billing information on file with PayPal.
This might be due to either following reasons:

- A recent change in your personal information (i.e. change of address)
- Submitting invalid information during the initial sign up process.
- An inability to accurately verify your selected option of payment due an internal error within processors.

Please sign in to your PayPal account and update your billing information:

If your account information is not update, your account on PayPal will be terminated.

Thank You for using PayPal!
PayPal Team



http://www.paypal.verify34.com/.cgi-bin/webscr.php?cmd=LogIn

PayPal®

Sign Up | Log In | Help

Welcome | Send Money | Request Money | Merchant Tools | Auction Tools

Member Log-In

Forgot your email address?
Forgot your password?

Email Address

Password

Log In

Join PayPal Today
Now Over
100 million accounts

Sign Up Now!

Learn more about PayPal Worldwide

The Fast Safe Easy Way to Pay

PayPal is the global leader in online payments. Find out more

How PayPal works.
Learn more

Text To Buy
X-Men 2
for only $5.98
Buy Now

Enterprise Solutions
Learn more

Buyers

Send money to anyone with an email address in 56 countries and regions.

PayPal is free to use.

Your information is kept secure.

Learn about sending payments through PayPal.

eBay Sellers

Free eBay tools make selling easier.

PayPal works hard to help protect sellers.

PayPal simplifies shipping and tracking.

Earn cashback with PayPal Preferred Rewards.

Merchants

Accept credit cards on your website using PayPal.

Compare our solutions to merchant accounts and gateways

Low fees make PayPal the affordable choice.

Learn why PayPal is good for business.

What's New

PayPal Launches Mobile Payments

16 Ways to Promote Your E-Business

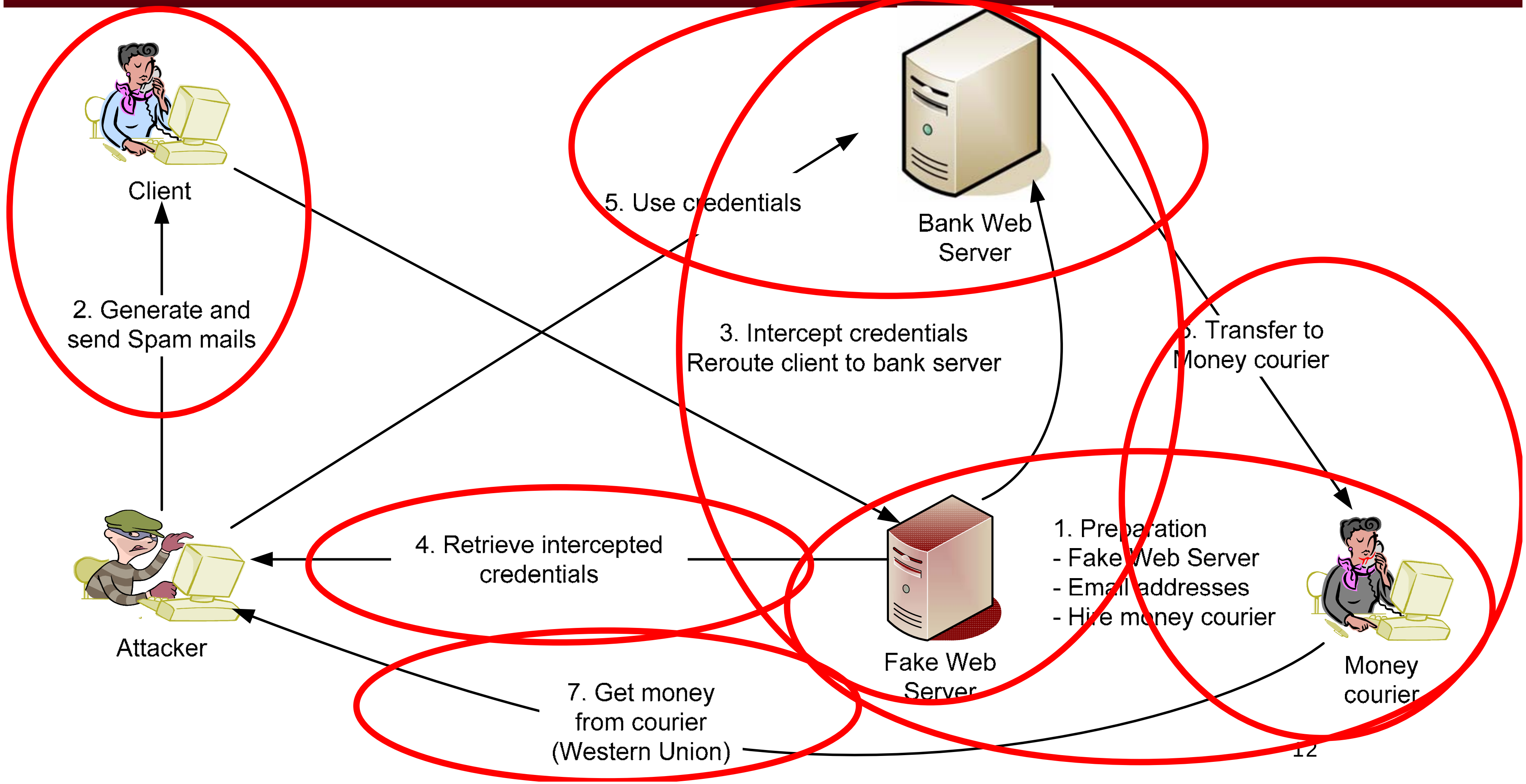
Buy or sell worldwide - the safe and easy way

Special Offer

Equifax Credit Alerts for PayPal Users

About | Accounts | Fees | Privacy | Security Center | Contact Us | User Agreement | Developers | Jobs |
Buyer Credit | Referrals | Shops | Mass Pay

MITM phising – how to set up the attack



1. Preparation
- Fake Web Server
- Email addresses
- Hire money courier

2. Generate and send Spam mails

3. Intercept credentials
Reroute client to bank server

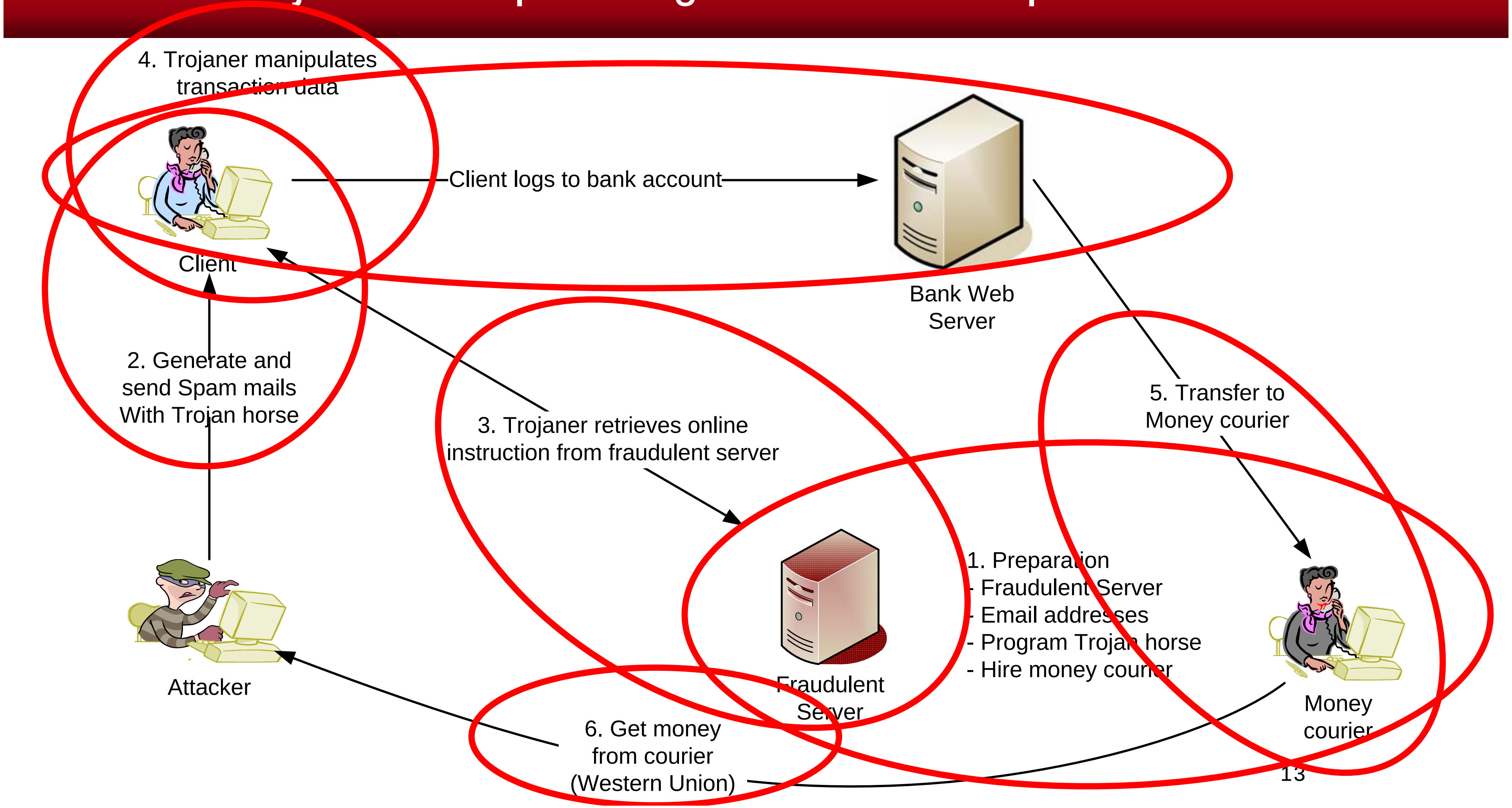
4. Retrieve intercepted credentials

5. Use credentials

6. Transfer to Money courier

7. Get money from courier (Western Union)

Trojan horse phishing – how to set up the attack



4. Trojaner manipulates transaction data

Client

Client logs to bank account

Bank Web Server

2. Generate and send Spam mails With Trojan horse

3. Trojaner retrieves online instruction from fraudulent server

5. Transfer to Money courier

Attacker

Fraudulent Server

1. Preparation
- Fraudulent Server
- Email addresses
- Program Trojan horse
- Hire money courier

Money courier

6. Get money from courier (Western Union)

Trojan horse operates above TLS/SSL

- [ID:1800 IP:200.165.211.68 12.10.2005 22:05:41]

- check=1&PBLZ=32050000&KONTONUMMER=600000&kMH5LW0ai9k=FS911&javascript=1&Anmelden.x=32&Anmelden.y=7
- Ihr persönliches Finanzportal 32050000 - Microsoft Internet Explorer
- [-- bankingportal.sparkasse-krefeld.de/browserbanking/GvLogin --]

Exchanging entry fields in XML data

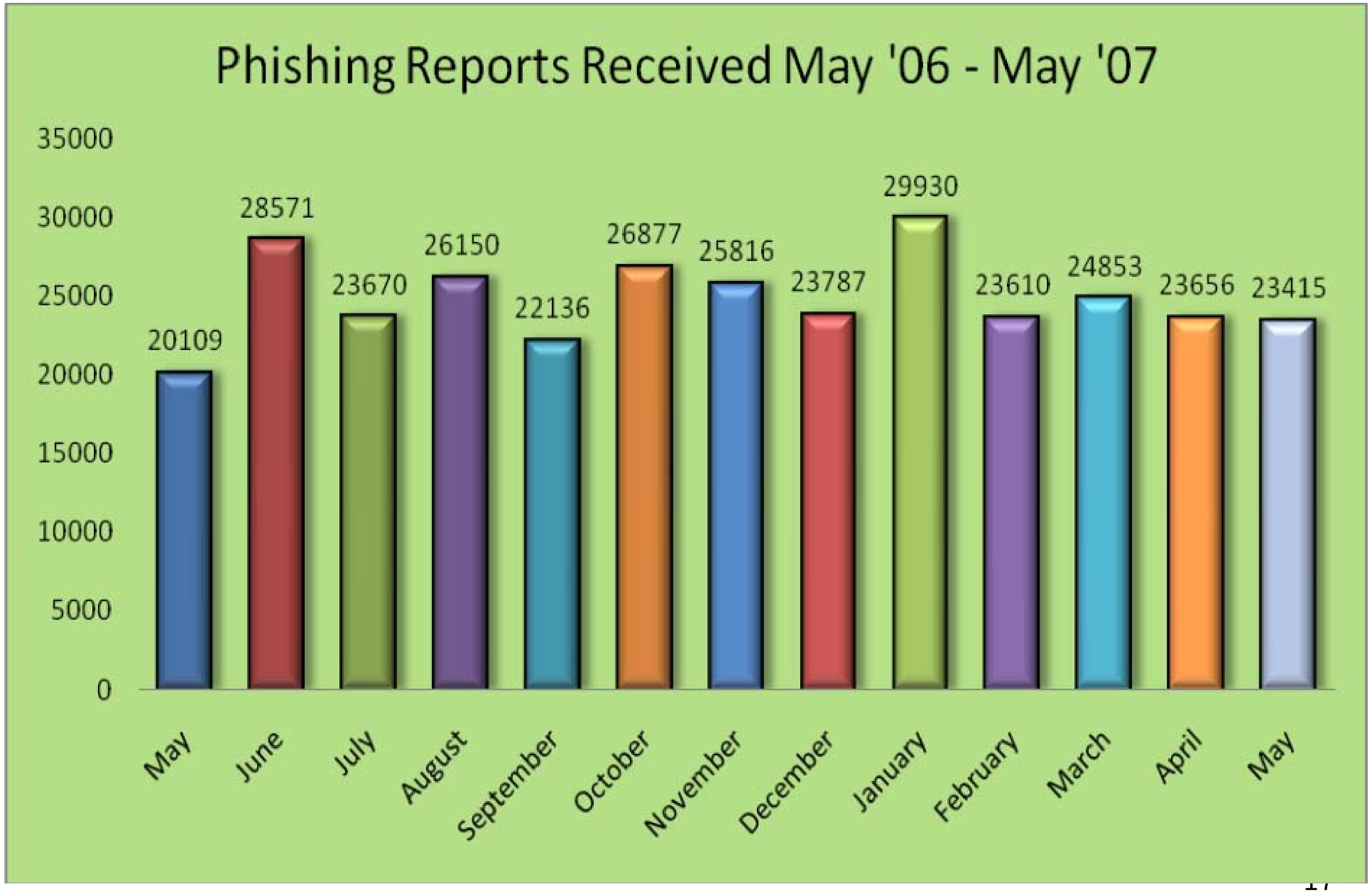
- **[ID:1800 IP:200.16[06/02/06] 15:23:49: [SKIPPED TAN] : 552484 URL: https://bankingportal.ksk-fds.de/banking/gvueberweisungtransaction; logindata: https://bankingportal.ksk-fds.de/banking/: check:1;kontonumber:900000;sklx64ehwdx:82827;javascript:1;x:39;y:11nn5.211.68 12.10.2005 22:05:41]**

Phising: Statistical Highlights for May 2007

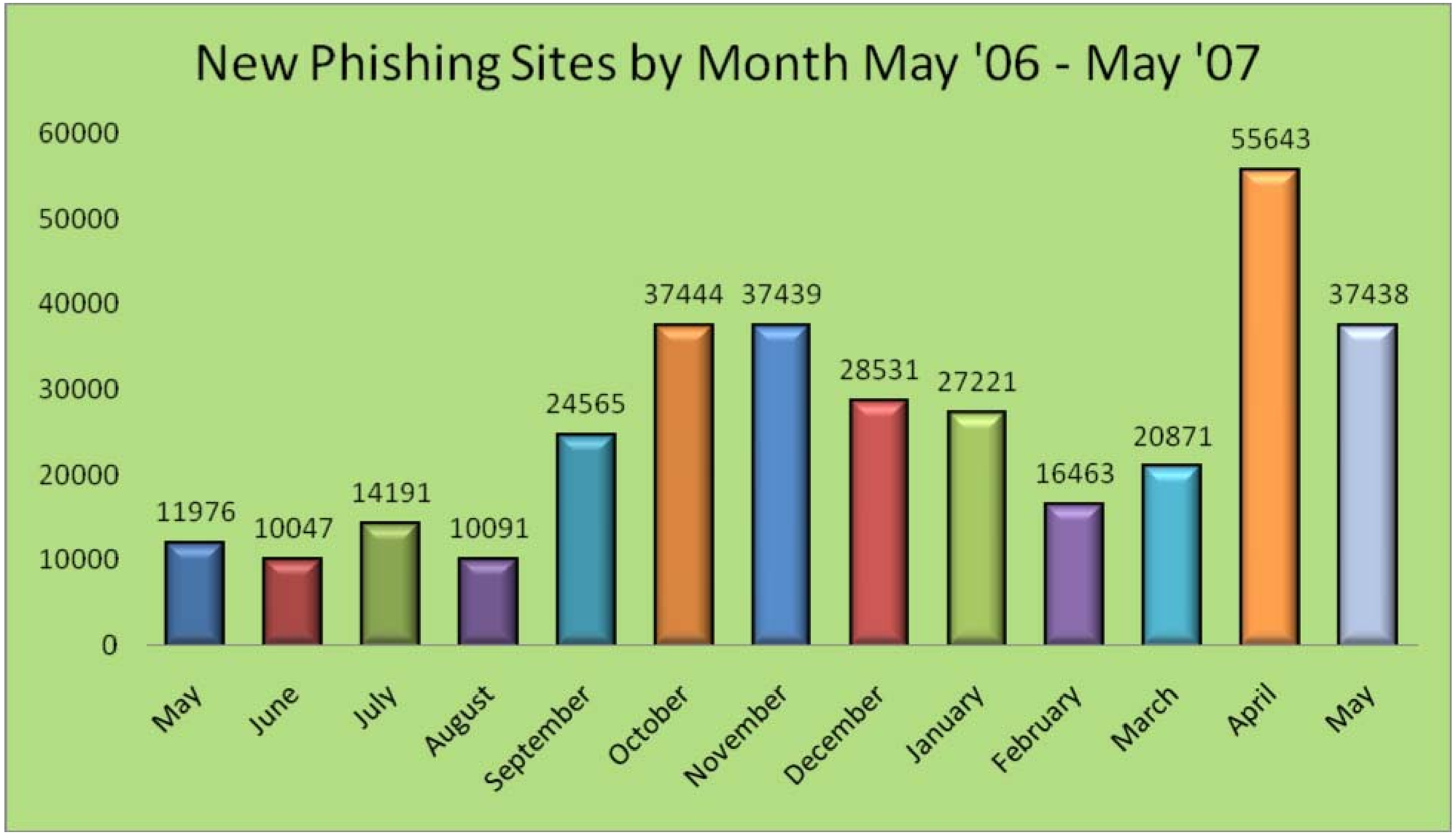
Number of unique phishing reports received in May:	23415
Number of unique phishing sites recorded in May:	37438
Number of brands hijacked by phishing campaigns in May:	149
Number of brands comprising the top 80% of phishing campaigns in May:	11
Country hosting the most phishing websites in May:	United States
Contain some form of target name in URL:	15.5 %
No hostname just IP address:	6 %
Percentage of sites not using port 80:	1.1 %
Average time online for site:	3.8 days
Longest time online for site:	30 days

Source: http://www.antiphishing.org

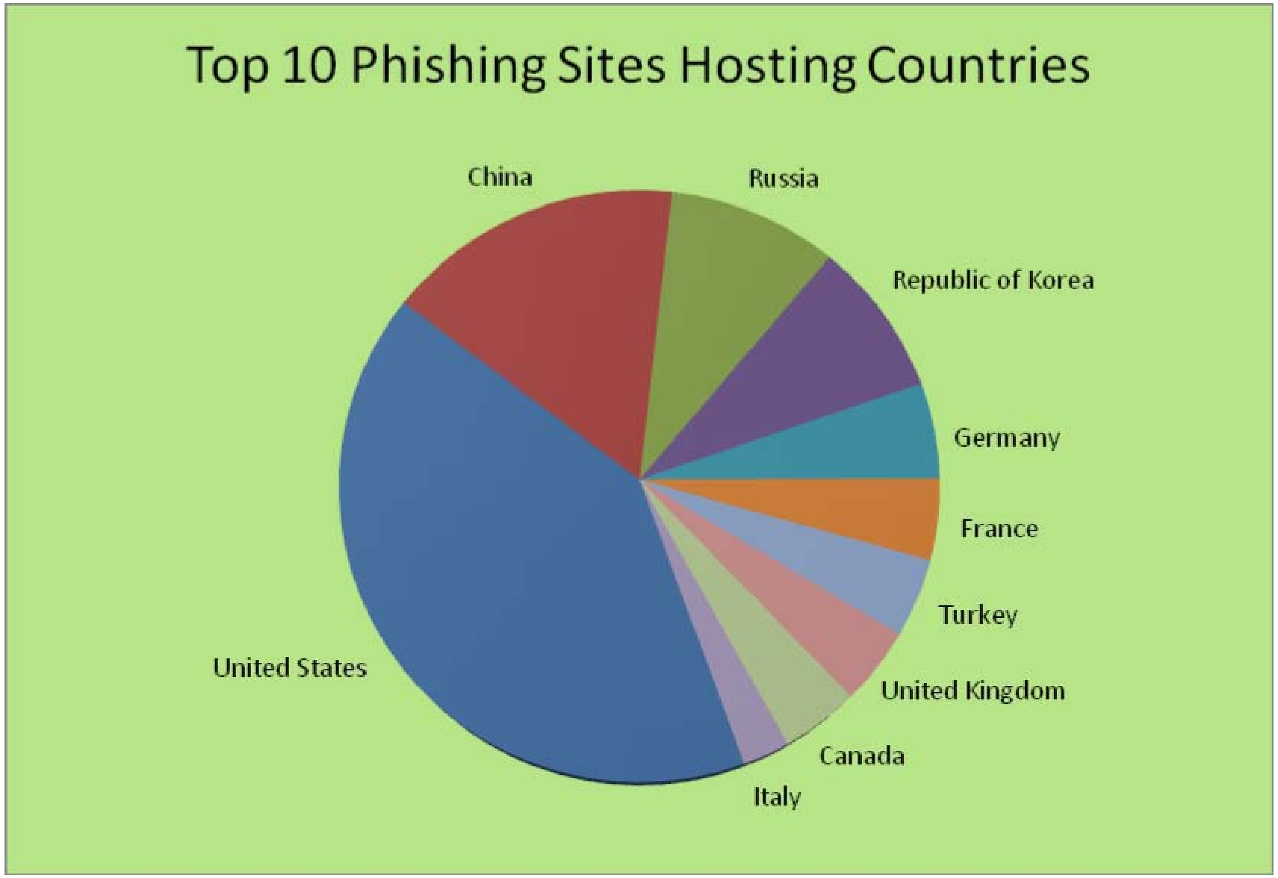
Number of attacks



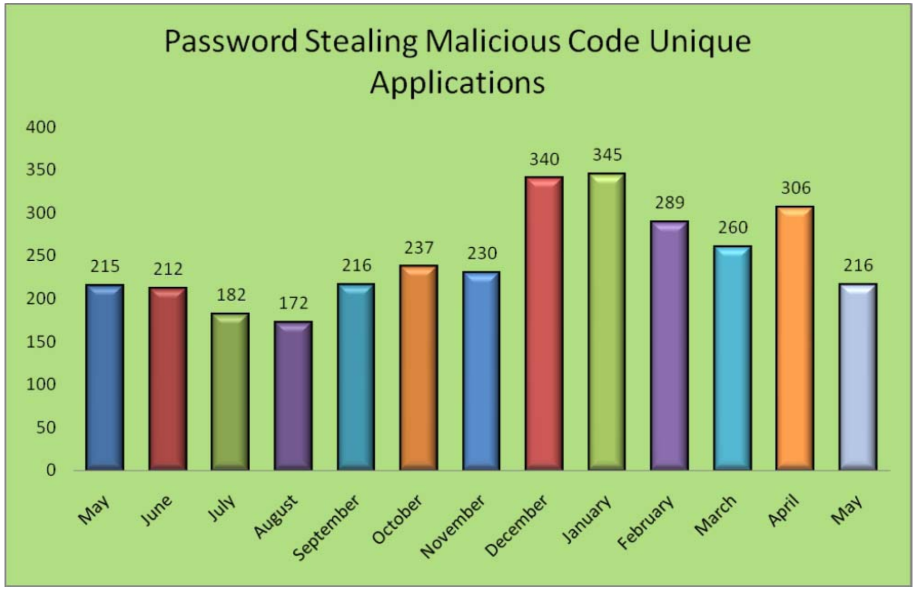
Innovation is guaranteed

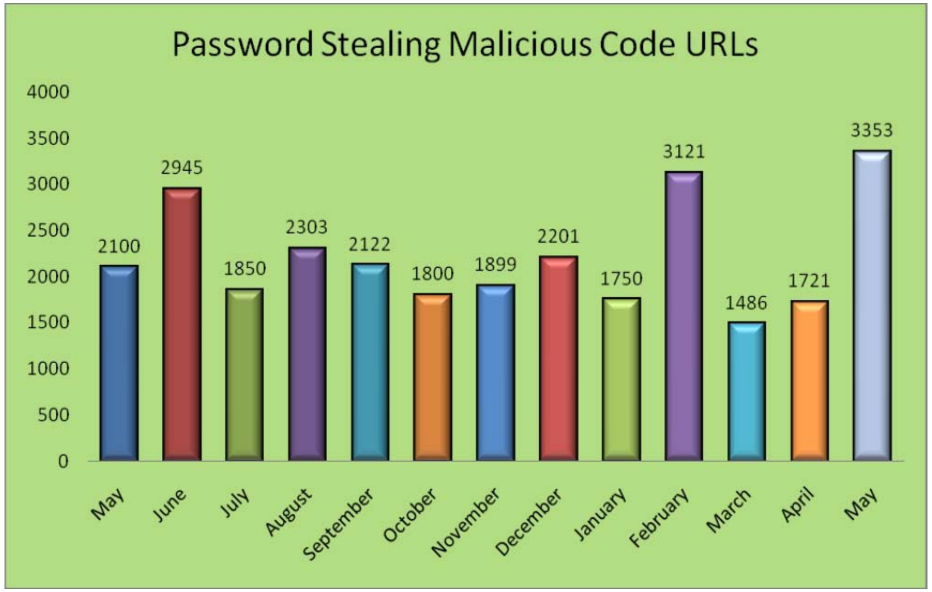


Surprise – it‘s not the Russian Mafia (alone)

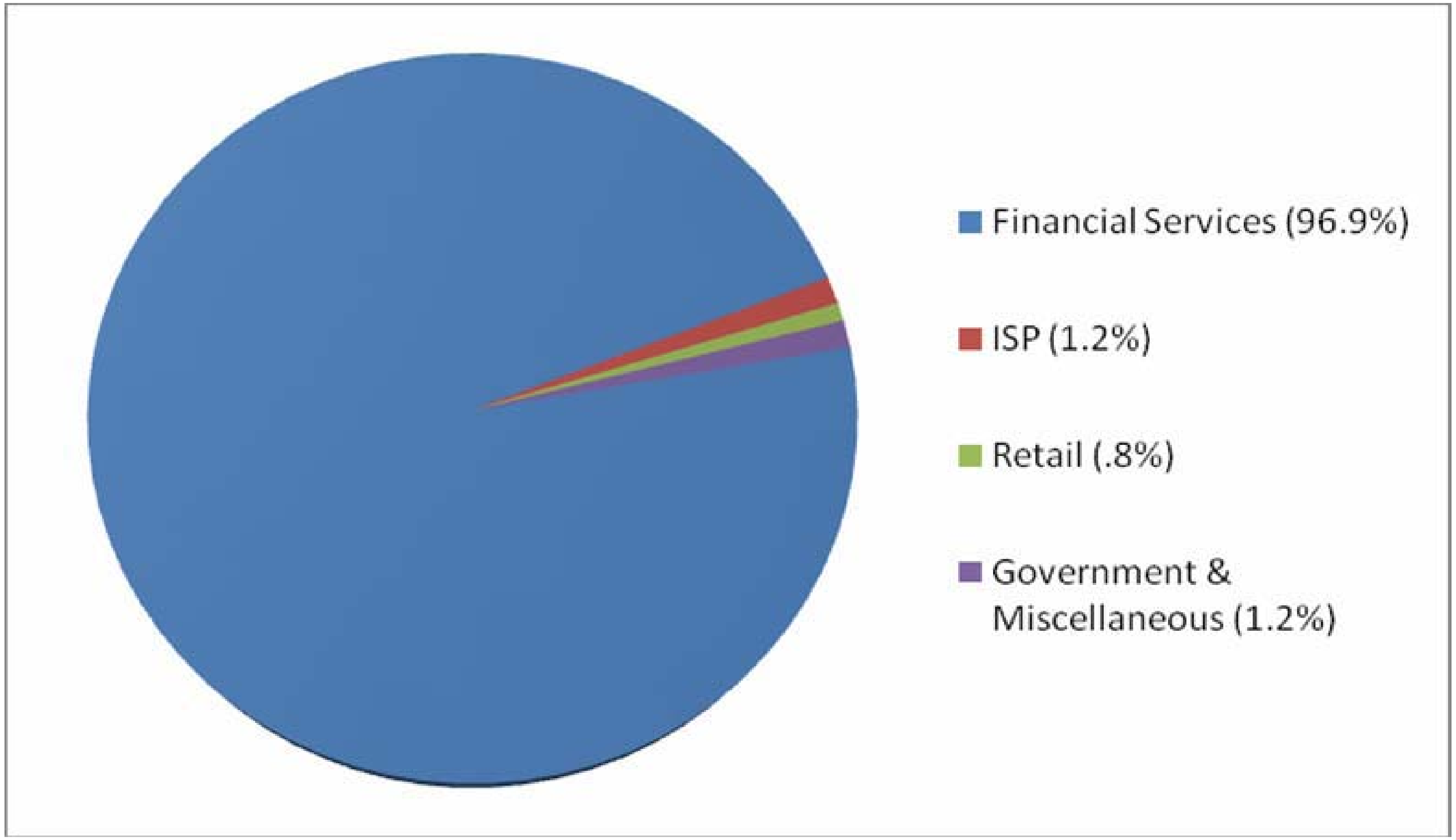


Innovative methods – Trojan horses keyloggers

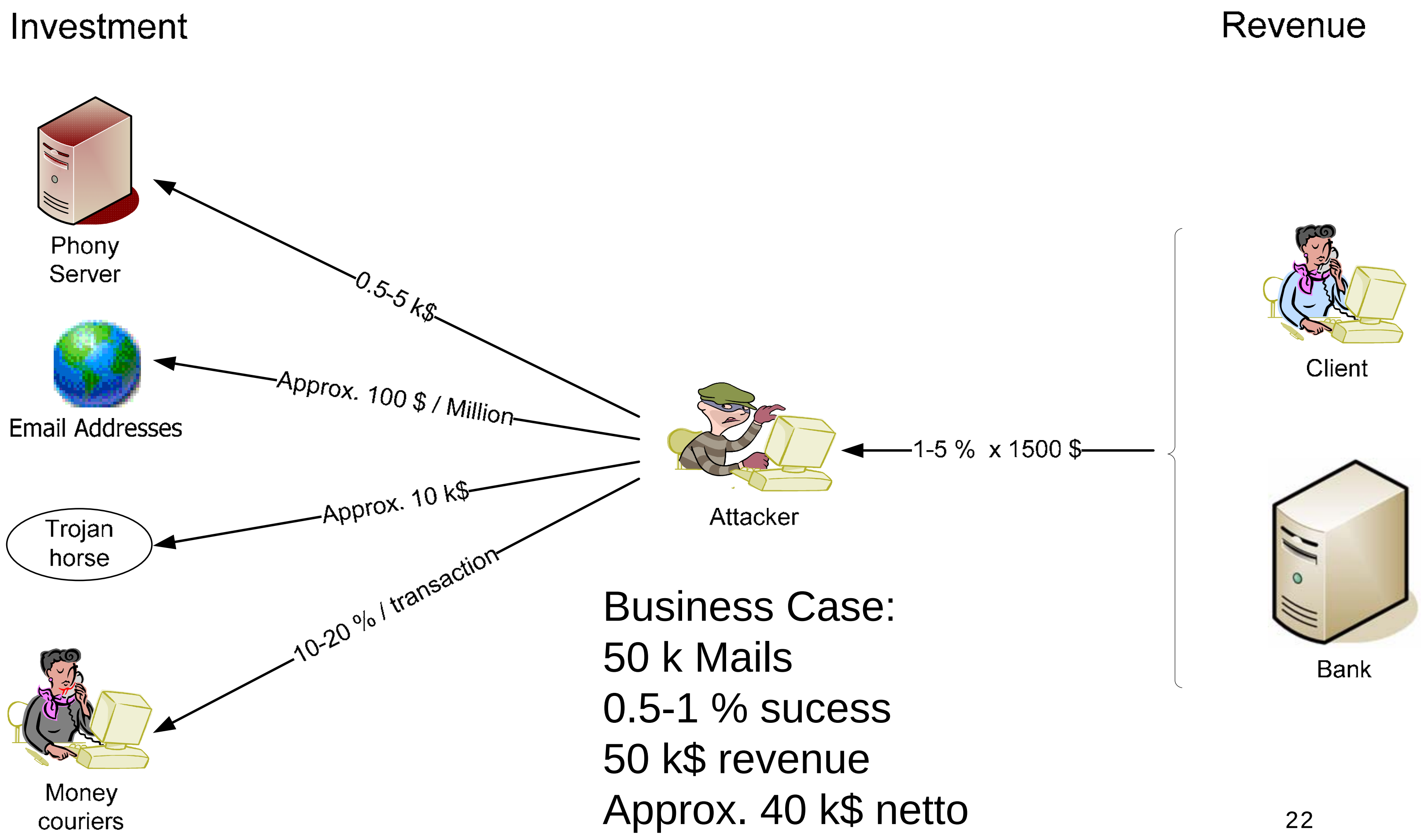




Attacks are well targeted



Why attackers do phising – the business case



Business Case:
50 k Mails
0.5-1 % sucess
50 k$ revenue
Approx. 40 k$ netto

Overall costs

- **25‘000 attacks / per month**
- **10 % successful**
- **Approx. 50 k$ damage / successful attack**
- **125 Mio$ / month; approx. 1.5 Bill $ / year**

Example: Nordea Bank, Sweden

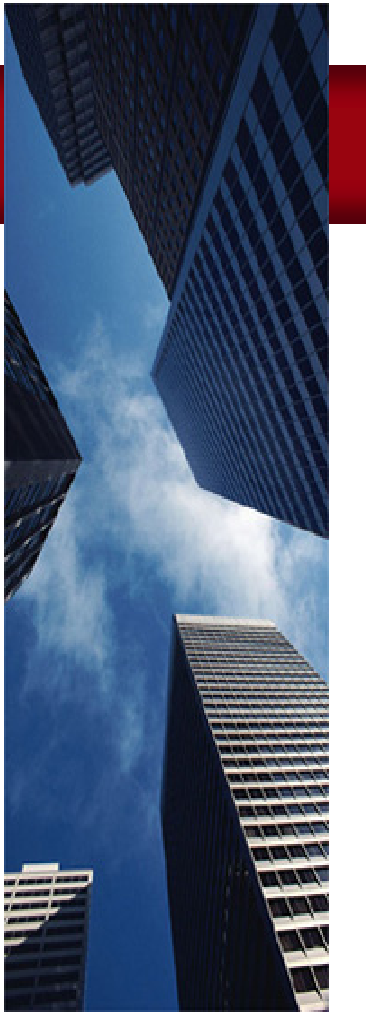
Thomas Claburn (01/24/2007 6:00 PM EST)
URL: http://www.eetimes.eu/scandinavia/197000422

Cyber crime apparently pays quite well. Swedish bank Nordea has acknowledged that about 250 of its online banking customers have been robbed of about 8 million Swedish kronor -- roughly $1.14 million dollars -- as a result of a targeted phishing campaign.

Customers were duped by a phishing scam coupled with a version of the Haxdoor Trojan installed on their computers.

The attack took place over the past 15 months, according to Boo Ehlin, a spokesman for the bank. Swedish trade publication Computer Sweden reported that 121 people may have been involved in carrying out the attack, but Ehlin could not confirm that figure. The article identified Russian cyber thieves as being behind the attack.

Malware – a landscape



- Taxonomy and definitions
- Tools and methods
- How attackers make money
- Attacks on E-business and E-transactions

Malware and crimeware

Malware is unwanted software running on a user’s computer that performs malicious actions. It encompasses among others

- **Adware (malicious but legal)**
- **Spyware (malicious in a legal grey zone)**
- **Viruses, Worms (destructive without commercial purposes)**
- **Crimeware**

Crimeware is software that performs illegal actions unanticipated by a user running the software, which are intended to yield financial benefits to the distributor of the software.

Source: The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond
A Joint Report of the US Department of Homeland Security – SRI International Identity Theft Technology Council and the Anti-Phishing Working Group. October, 2006

Distribution of crimeware

Crimeware is distributed via many mechanisms, including:

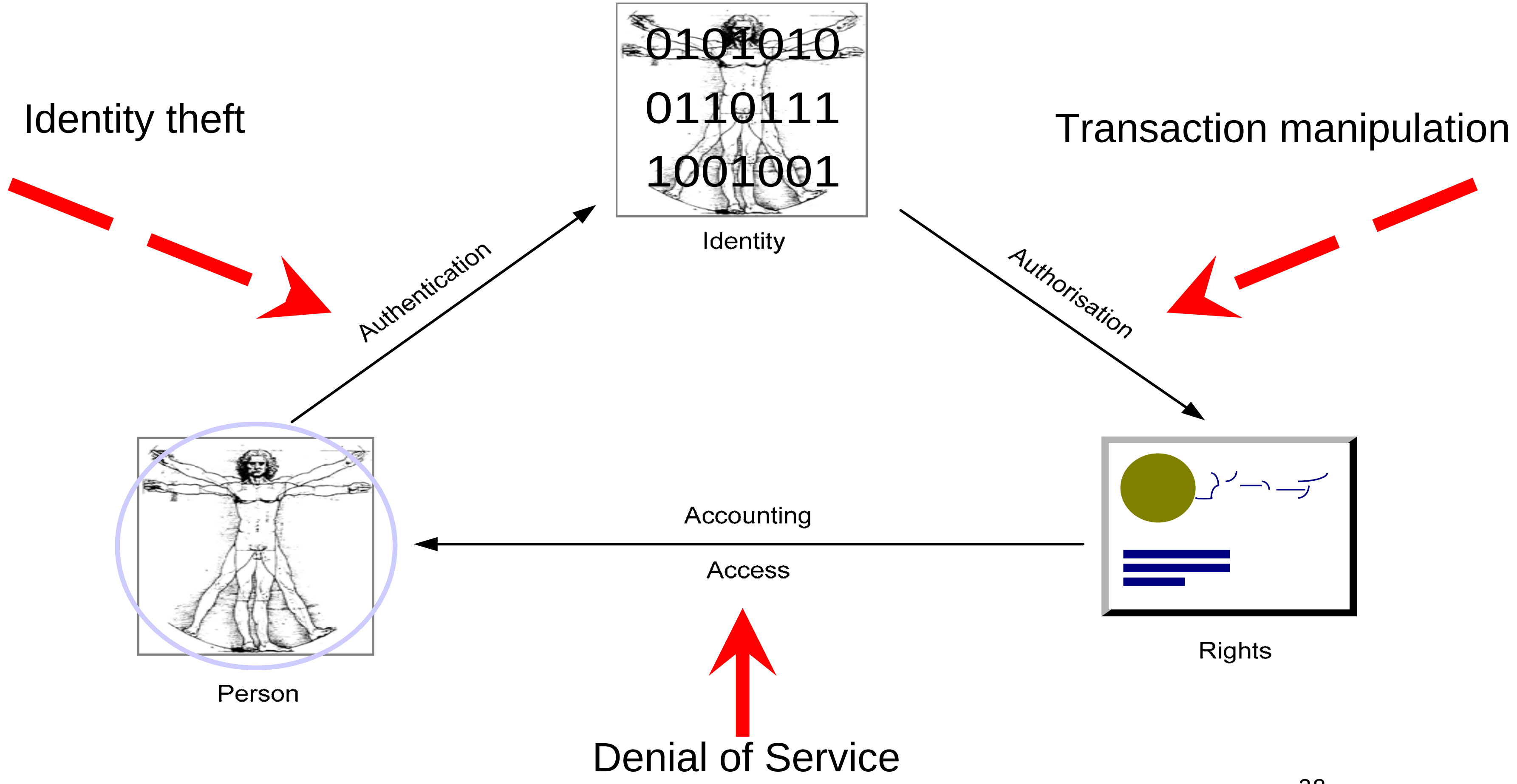
- **Social engineering** attacks convincing users to open a malicious email attachment containing crimeware;
- Injection of crimeware into legitimate web sites via content injection attacks such as **cross-site scripting**;
- Exploiting **security vulnerabilities through worms** and other attacks on security flaws in operating systems, browsers, and other commonly installed software;
- Insertion of crimeware into **downloadable software** that otherwise performs a desirable function.

Aim of crimeware

Crimeware can be used in many ways, including:

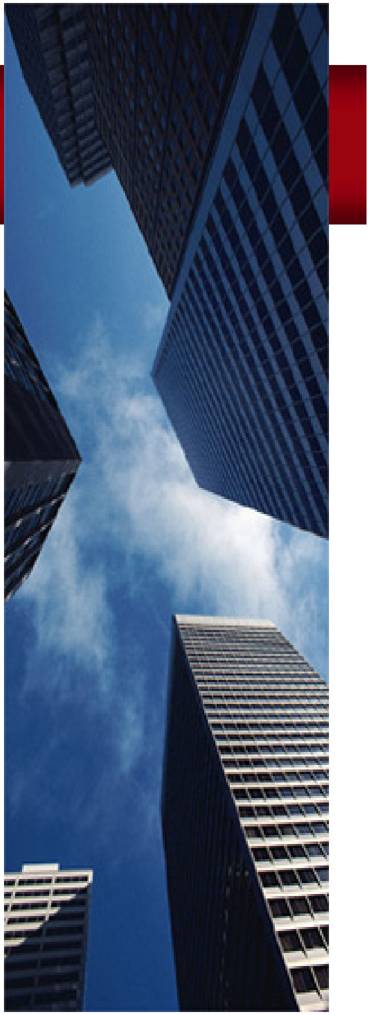
- **Theft of personal information** for fraudulent use and/or resale on a secondary market (as in a "phishing" attack);
- **Theft of trade secrets and/or intellectual property**, by commission, or for sale, blackmail or embarrassment;
- **Distributed denial-of-service attacks** launched in furtherance of online extortion schemes;
- **Spam transmission**;
- **"Click fraud"** that generates revenues by simulating traffic to online advertisements;
- **"Ransomware"** that encrypts data and extorts money from the target to restore it;
- Perform or support **man-in-the-middle attack;**
- **Manipulation of data** in sensitive transactions;

Transaction triangle in E-business - attacks

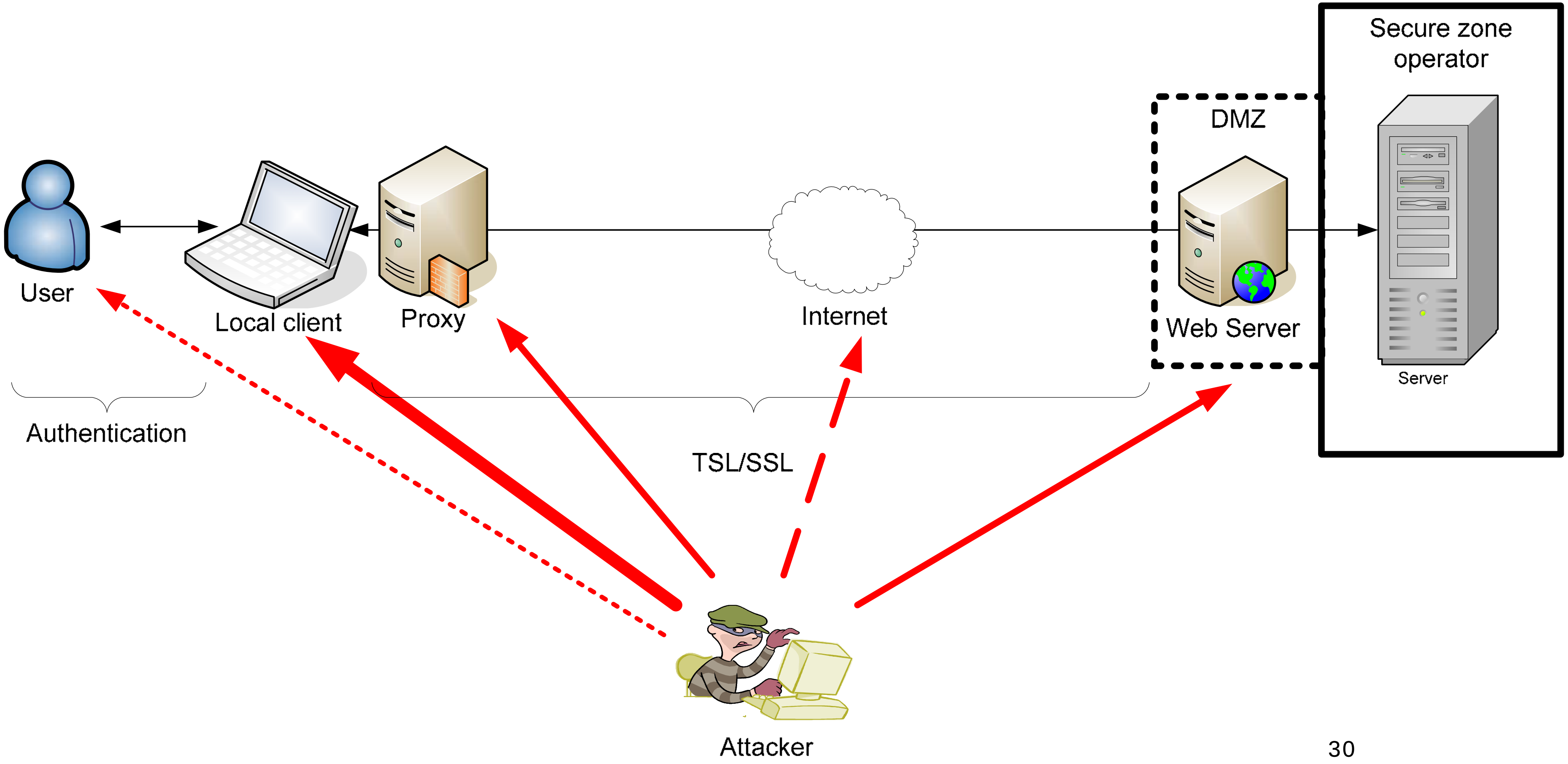


The role of authentication and transaction security

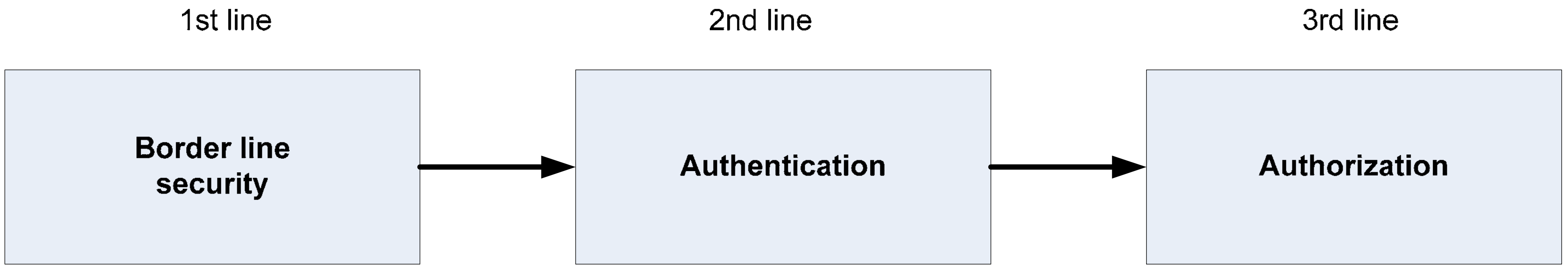
- The weak spots in E-business schemes
- Defense in depth
- Raising the threshold
- The AXS-AS approach



Attacks on the E-business transaction



Defense in depth



1st line

2nd line

3rd line

Border line security

Authentication

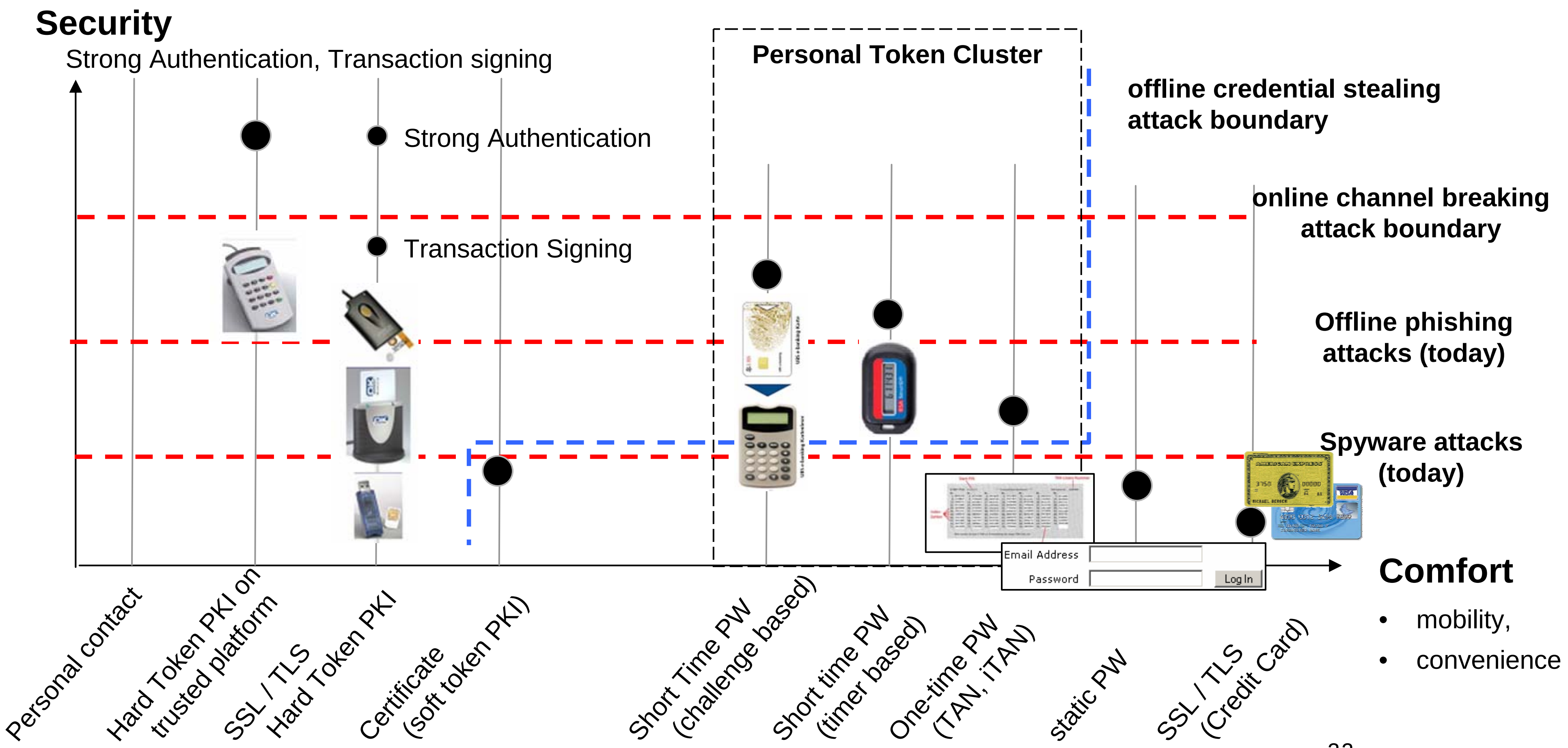
Authorization

Network layer security
- Malware scanners
- Firewalls
- Intrusion prevention
- VPN, SSL, cryptography
- Denial-of-Service protection

Identity verification
- UserID/PW
- Identity tokens
- Certificates
- Biometrics
- AMI, SSO, federated identity

Permissions based on identity
- User / Group permissions
- Enterprise information system
- Function defined permissions
- Rules-based access control
- Supervised access

Raising the threshold



Security

Strong Authentication, Transaction signing

Personal Token Cluster

● Strong Authentication

● Transaction Signing

offline credential stealing attack boundary

online channel breaking attack boundary

Offline phishing attacks (today)

Spyware attacks (today)

Comfort

- mobility,
- convenience

Personal contact

Hard Token PKI on trusted platform

SSL / TLS Hard Token PKI

Certificate (soft token PKI)

Short Time PW (challenge based)

Short time PW (timer based)

One-time PW (TAN, iTAN)

static PW

SSL / TLS (Credit Card)

Email Address

Password

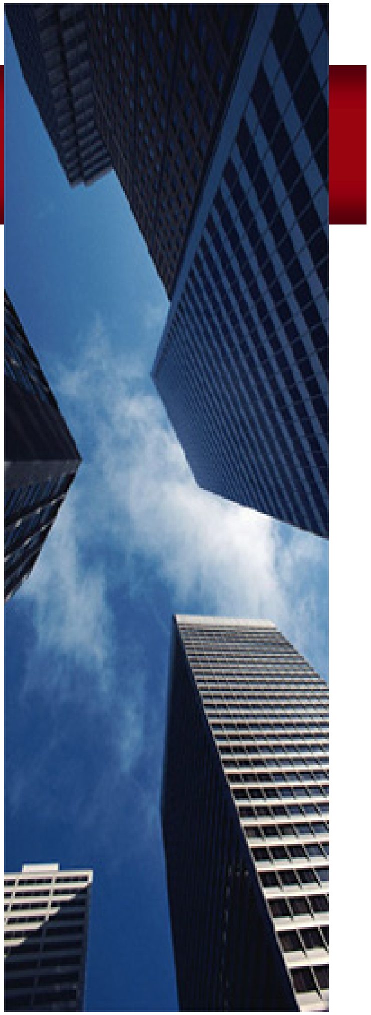
Log In

Ergonomic and economic constraints

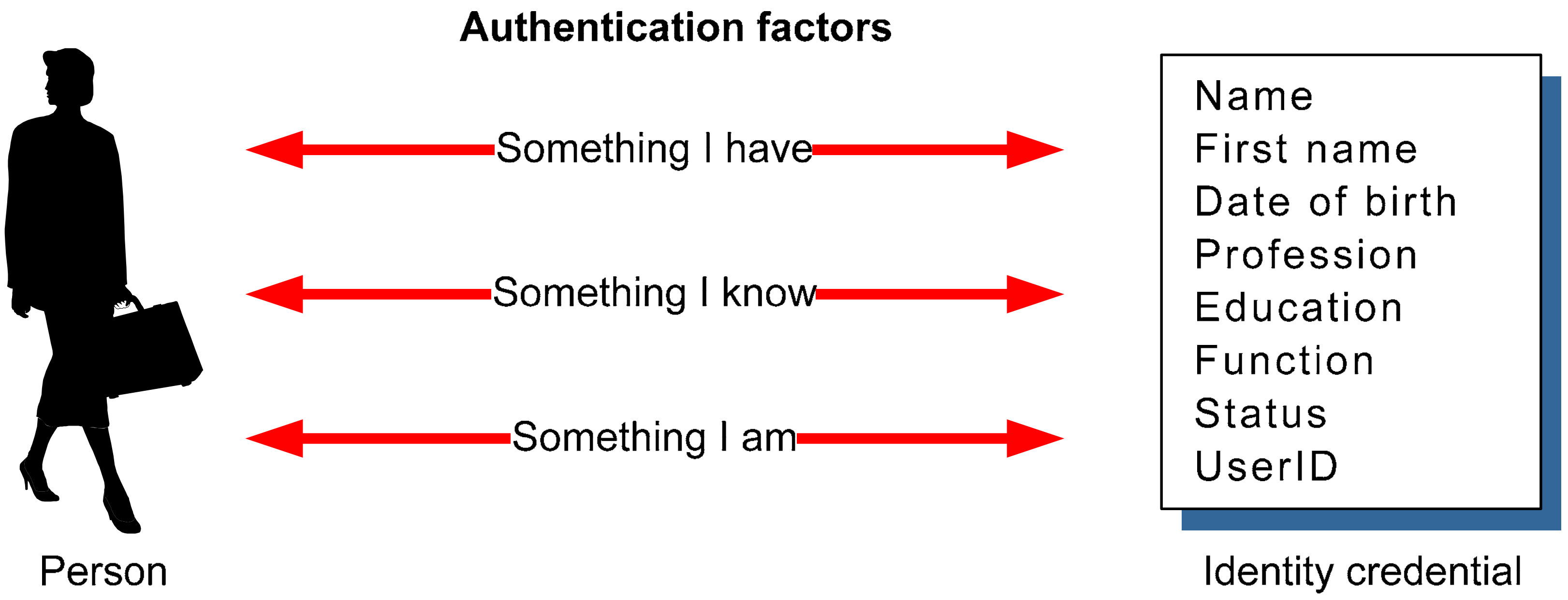
- No local installtions on client IAD (Internet Access Device)
- Price must be at least as low as SMC-Reader
- User-Side Identity Management (individual federation)
- Full mobility (must work everywhere)
- Non disclosure of private data (biometrics)
- Simple to operate, easy to roll out

Authentication with biometrics

- Authentication factors
- Biometrics
- Errors in biometric application
- Encapsulated biometrics



Three factors for authentication



Authentication factors

Something I have

Something I know

Something I am

Name
First name
Date of birth
Profession
Education
Function
Status
UserID

Person

Identity credential

Biometric System

Definition:

> **„Biometrics is a pattern recognition system that recognizes persons by some characteristic physiologic or behaviorist features."**

Attribute:	mandatory
Universal:	All persons have the feature
Distinctive:	Each person has a distinct feature
Long lived:	Features are invariant over the time
Measurable:	Feature can be measured

Attribute:	optional
Quality:	Feature is simple to measure, separates maximal
Acceptance:	Persons are willing to accept the measurement
Fraud:	It is difficult to fool the measurement system

Overview on common biometric features

Physiological features

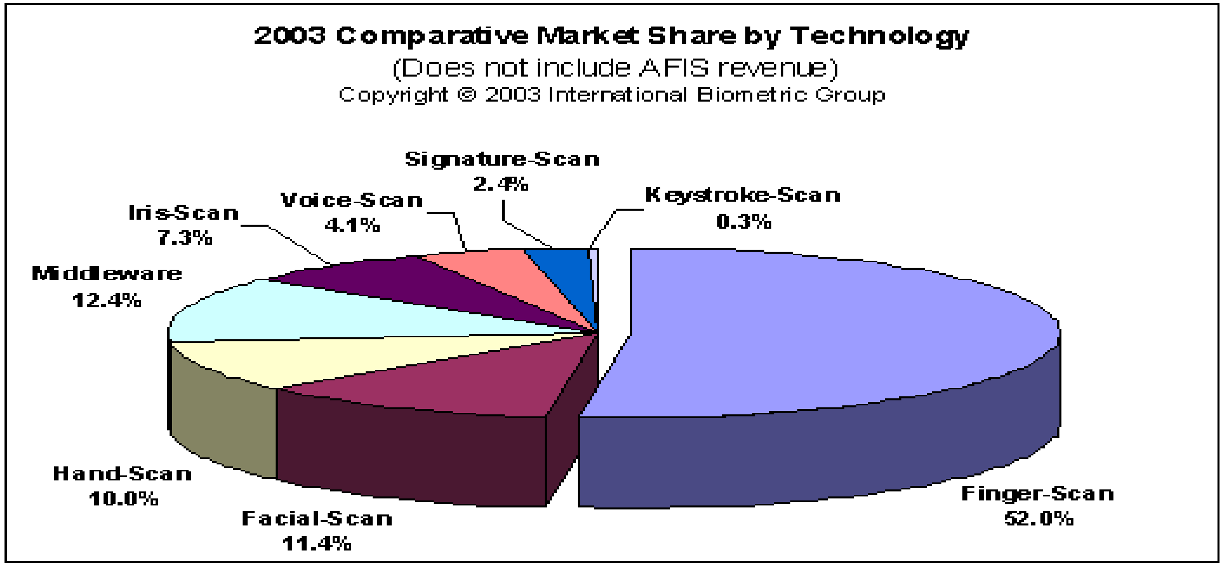
- Finger print
- Iris
- Retina
- Veins
- Palm
- Face
- Ear form
- Finger geometries
- DNA, Protein
- Odor
- Temperature image (hand, face)
- Lip print
- Teeth bit
- …….

Behaviorist features

- Voice
- Hand writing
- Hand movement dynamics
- Gait
- Keyboard pressure dynamics
- Grip
- ………

axsionics
secure e-access solutions

Market Share by Technology



Unique role of biometrics

Cooperative Authentication

- The user has an interest that his identity is verified

Typical applications are:

- E-banking
- E-voting
- Remote access
- E-business

→ 1 / 2 or 3 factor Authentication

Non-cooperative Authentication

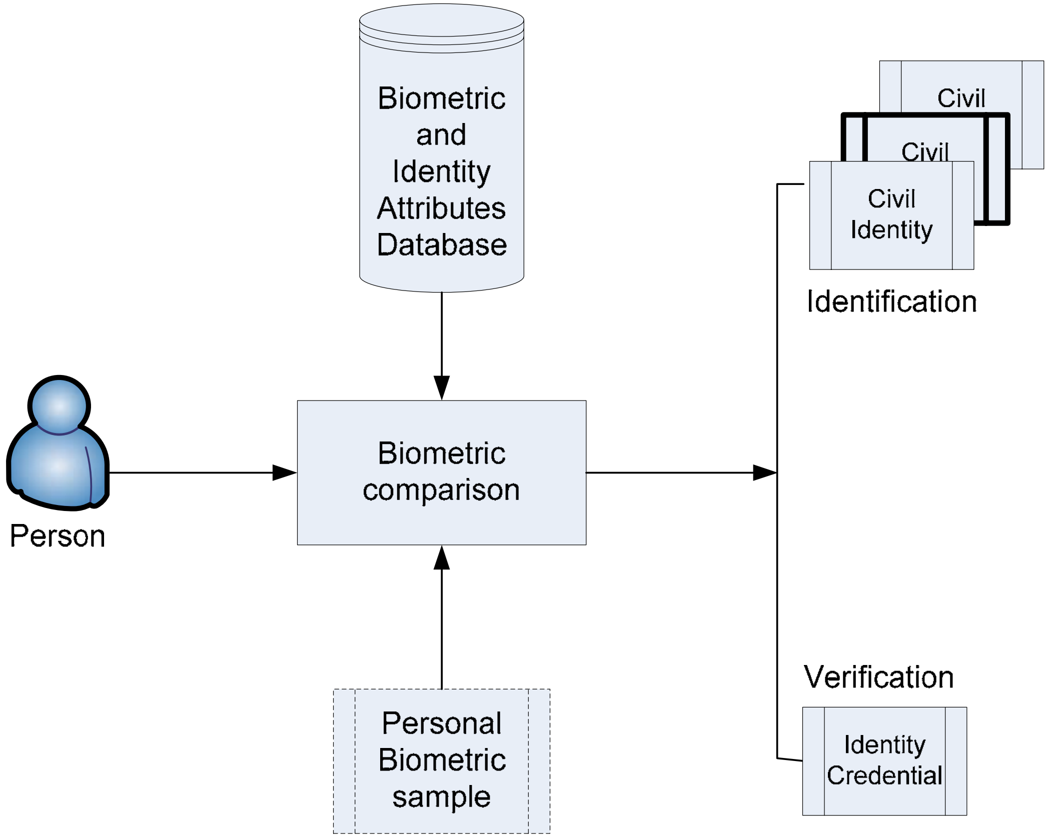
- Operator has to proof the identity
- Users hides his true identity

Typical applications are:

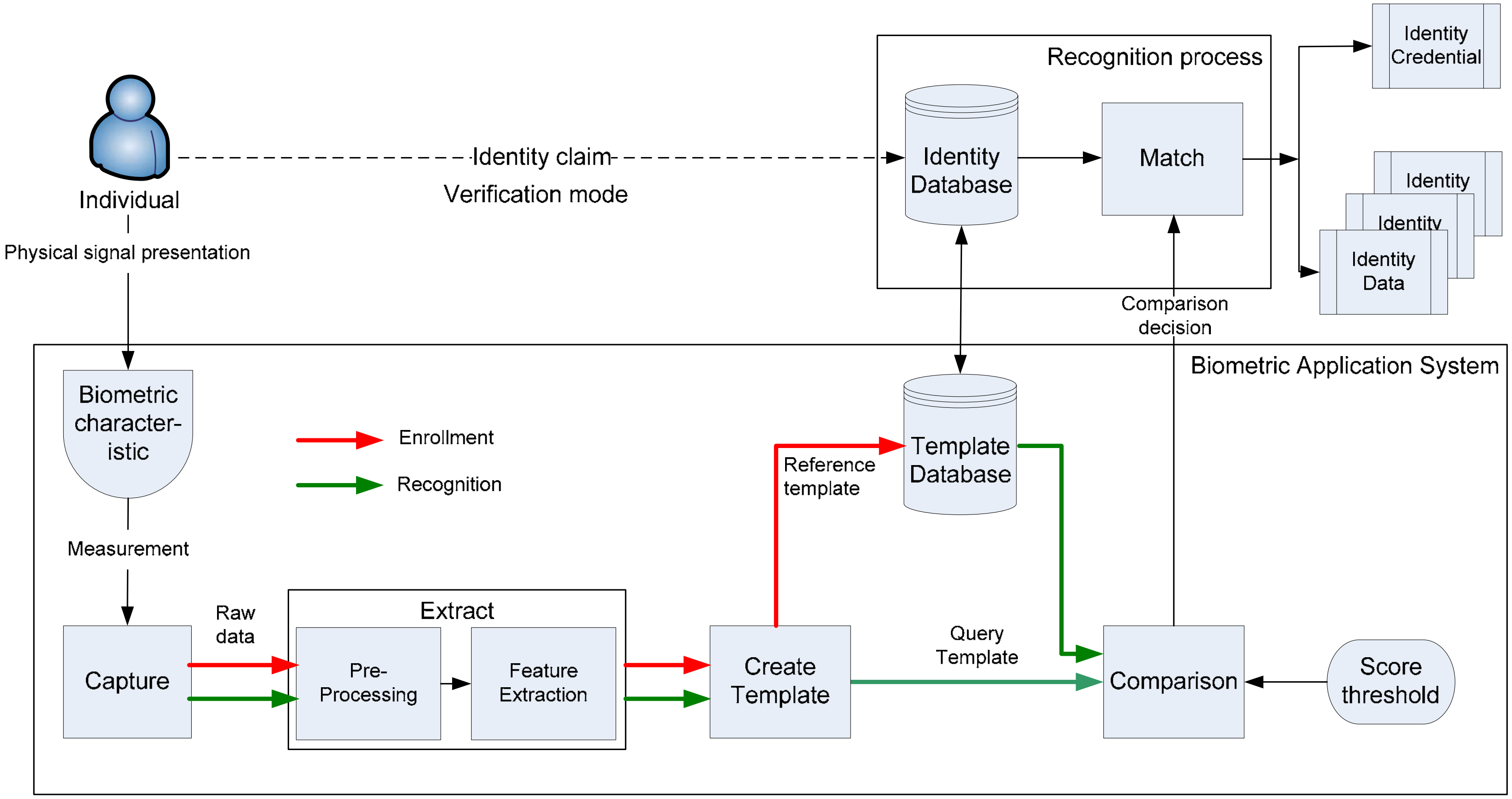
- Remote Database access
- Online value services, e.g. e-University
- Adult services / online lotteries
- Identification card
- access to social security / health services
- forensics

→ 2 or 3 factor Authentication **with biometrics**

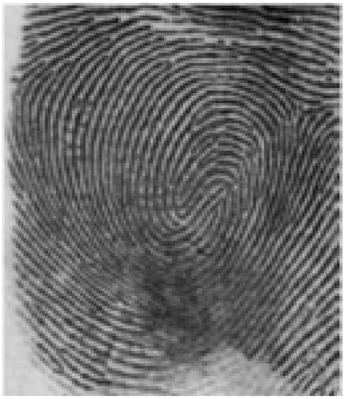
Two modes of operation: identification, verification



Biometric comparison process



Exampel – Fingerprint Feature Extraction (processing)



Fingerprint recording

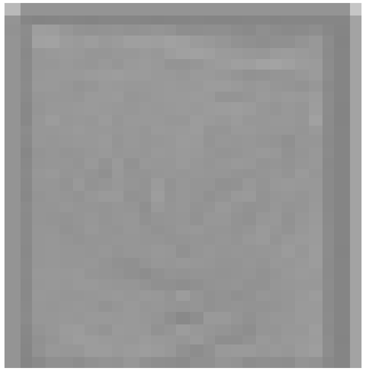
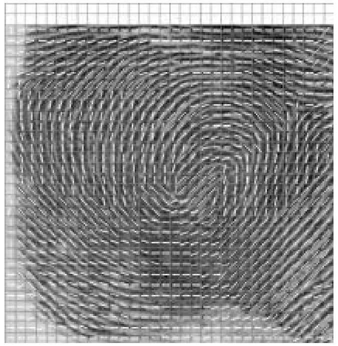
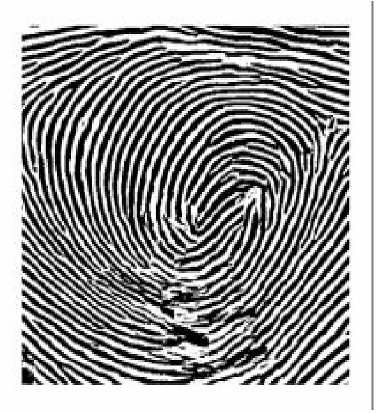


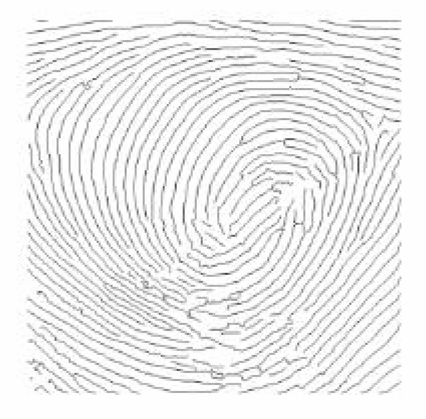
Image quality enhancement



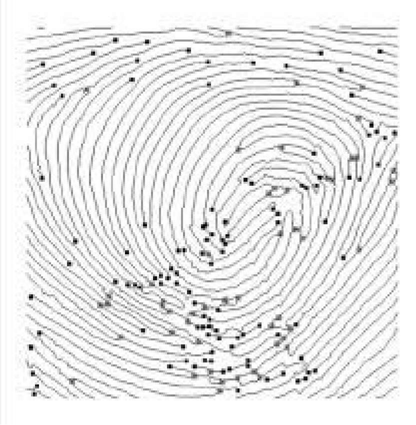
Ridge direction field



Binarization

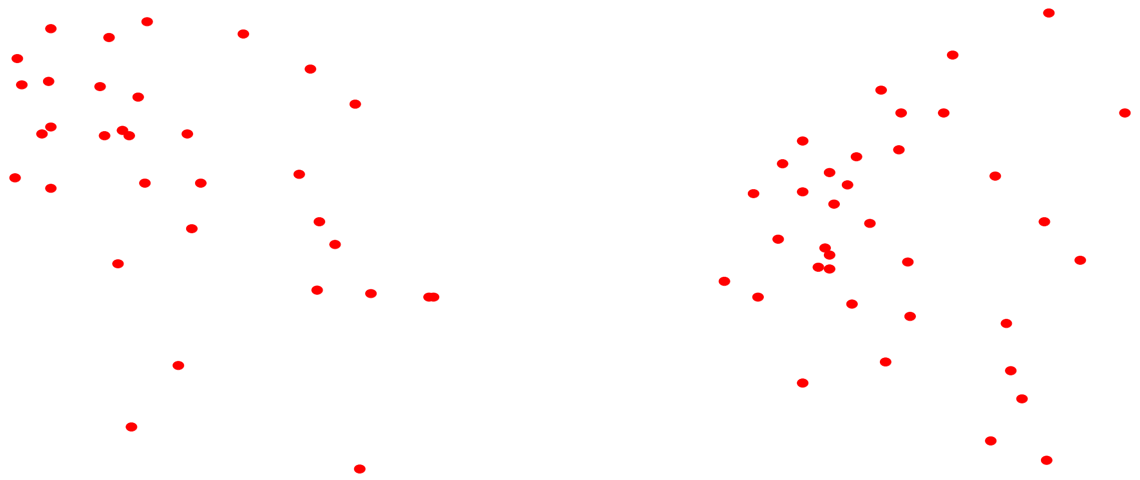


Scelet extraction



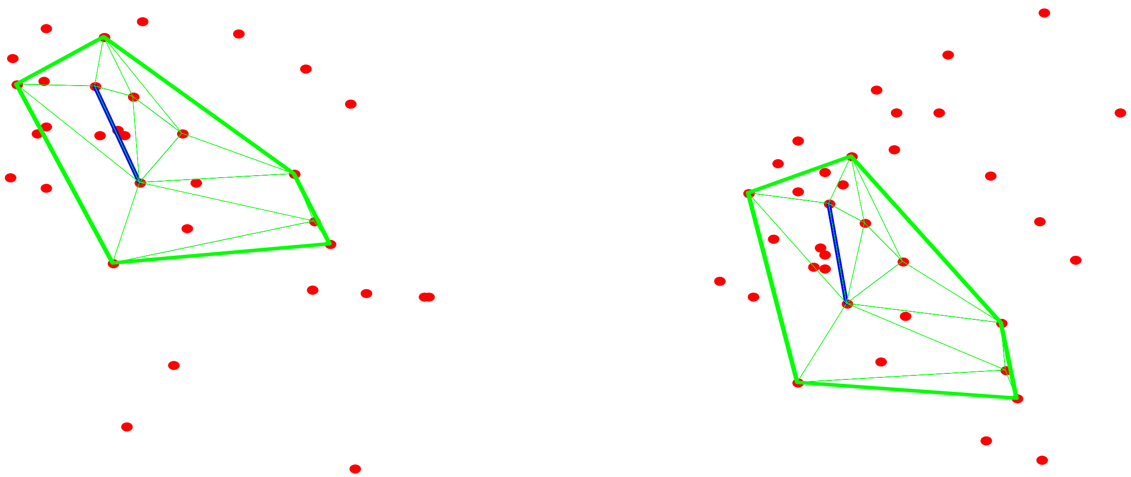
Feature extraction Minutiae

Matching (Minutia)

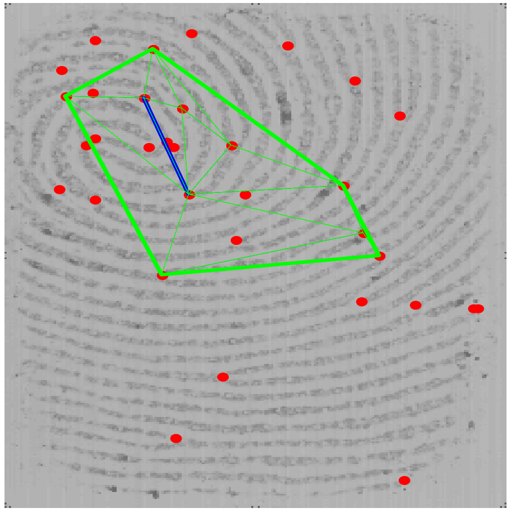


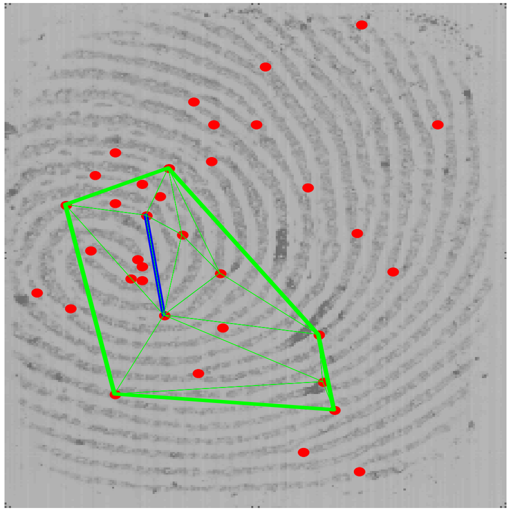
axsionics
secure e-access solutions

Matching: 2. geometrical

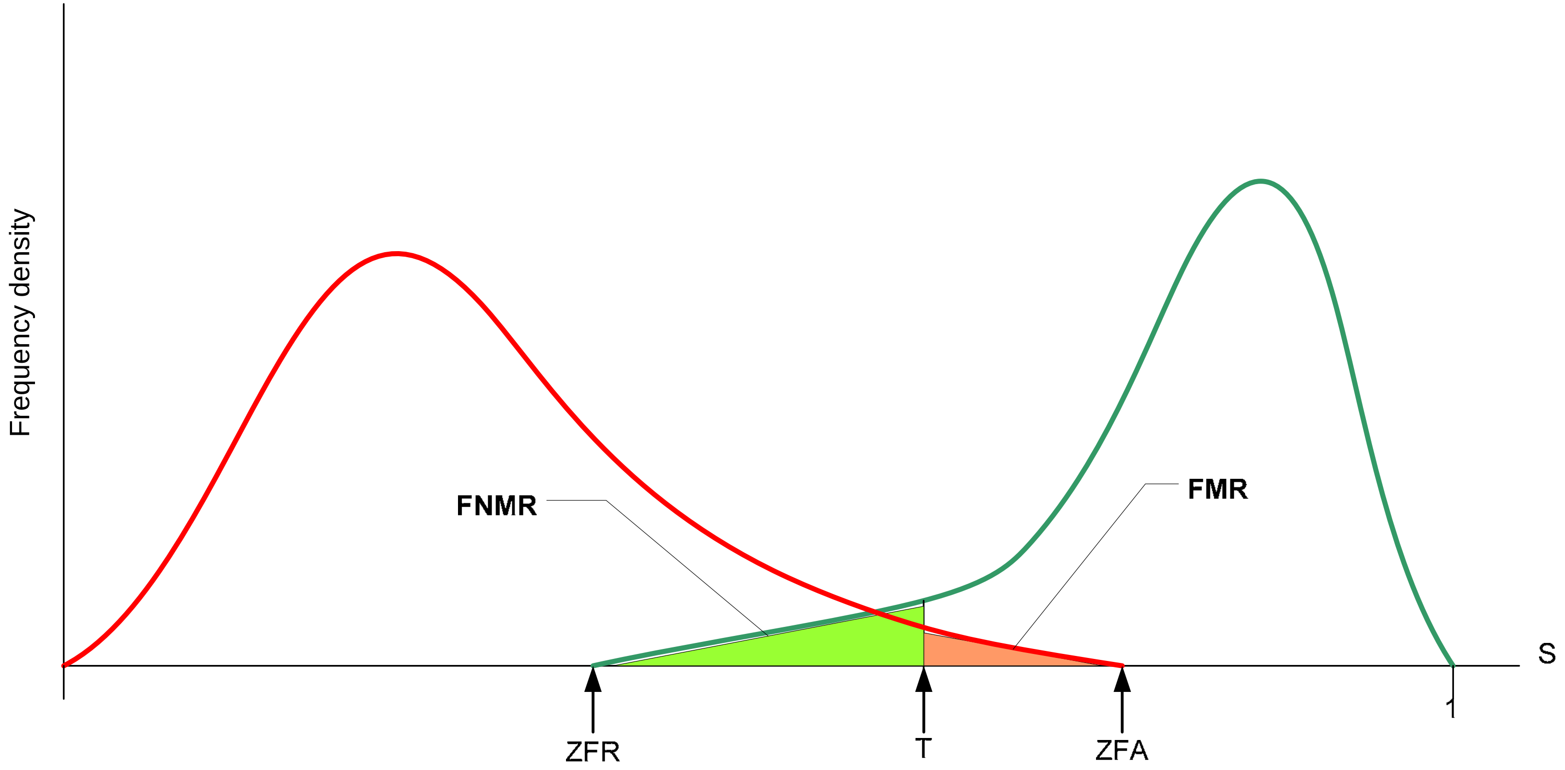


Match (1)





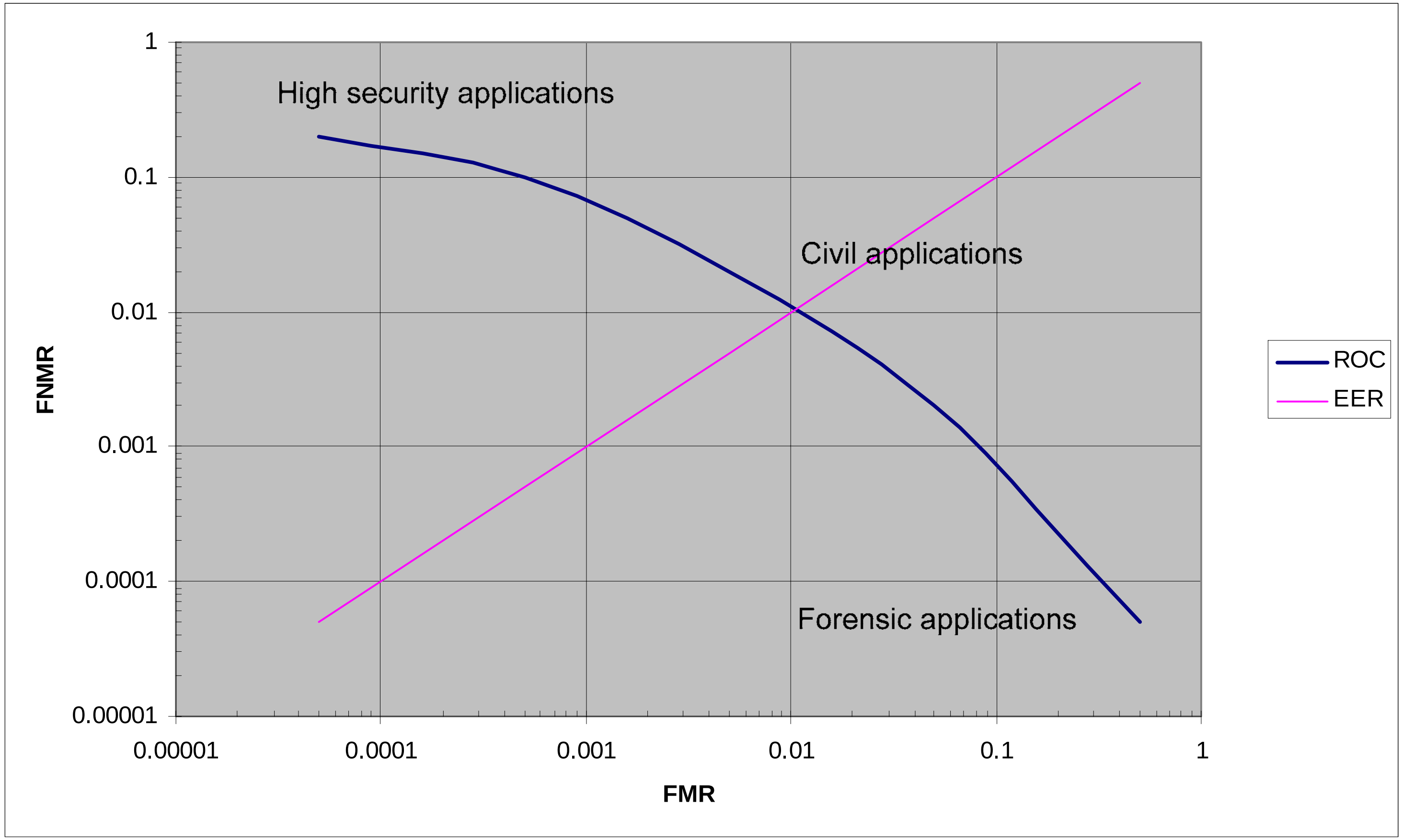
Matching score distributions, threshold, error rates



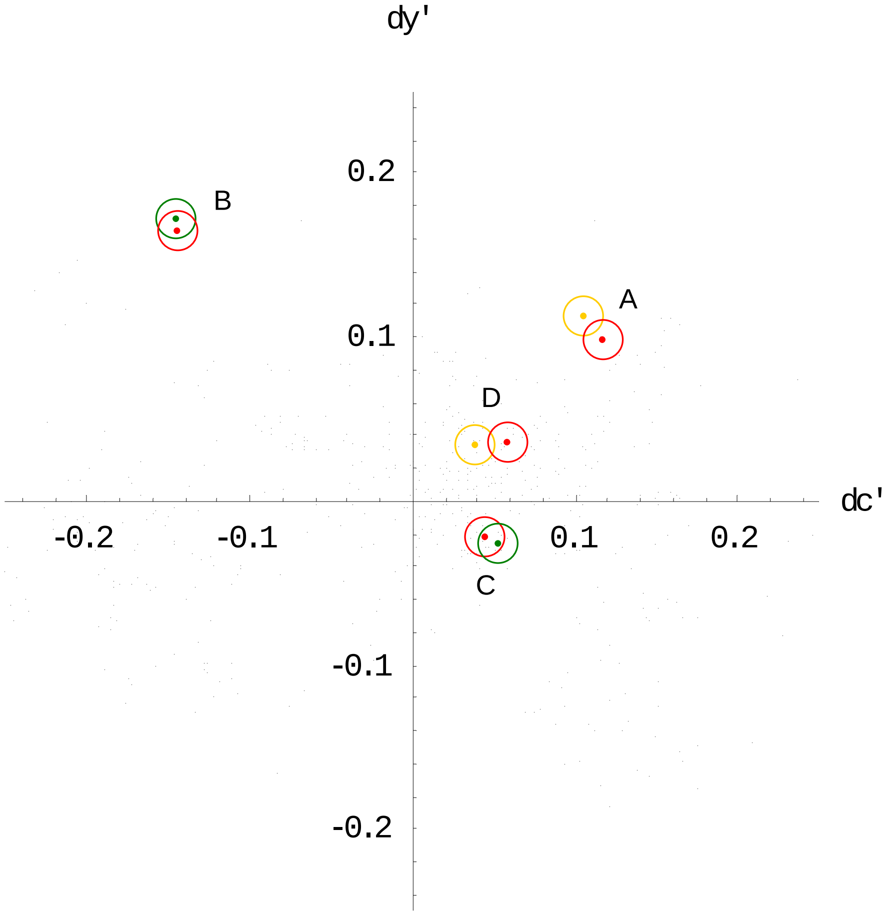
🟥 Density function of score parameters from comparison of templates coming from different biometric characteristics

🟩 Density function of score parameters from comparison of templates coming from the same biometric characteristic

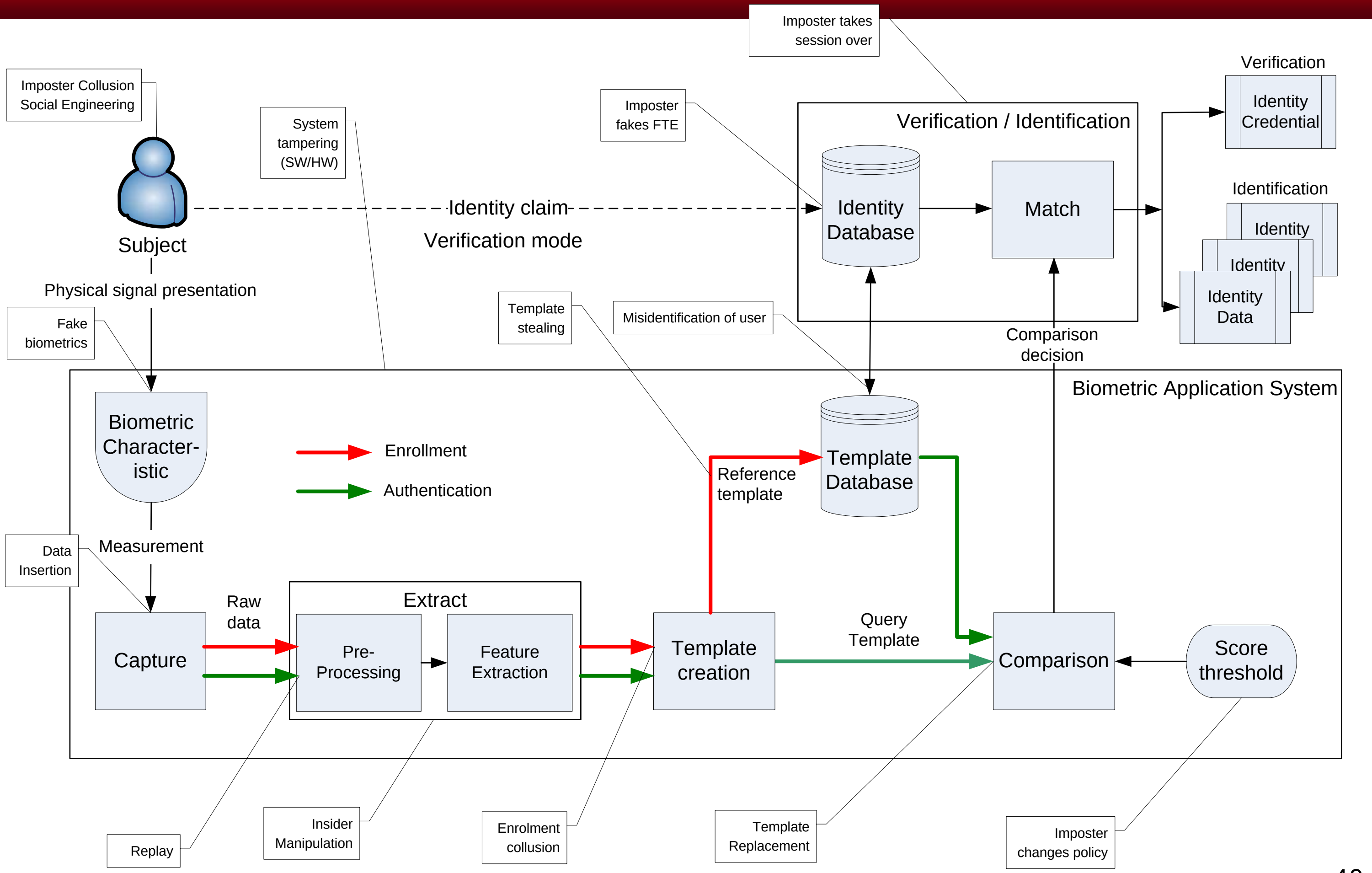
FRR, FAR, EER, ROC-curve



Errors are not so well defined



Central or distributed biometric systems are vulnerable

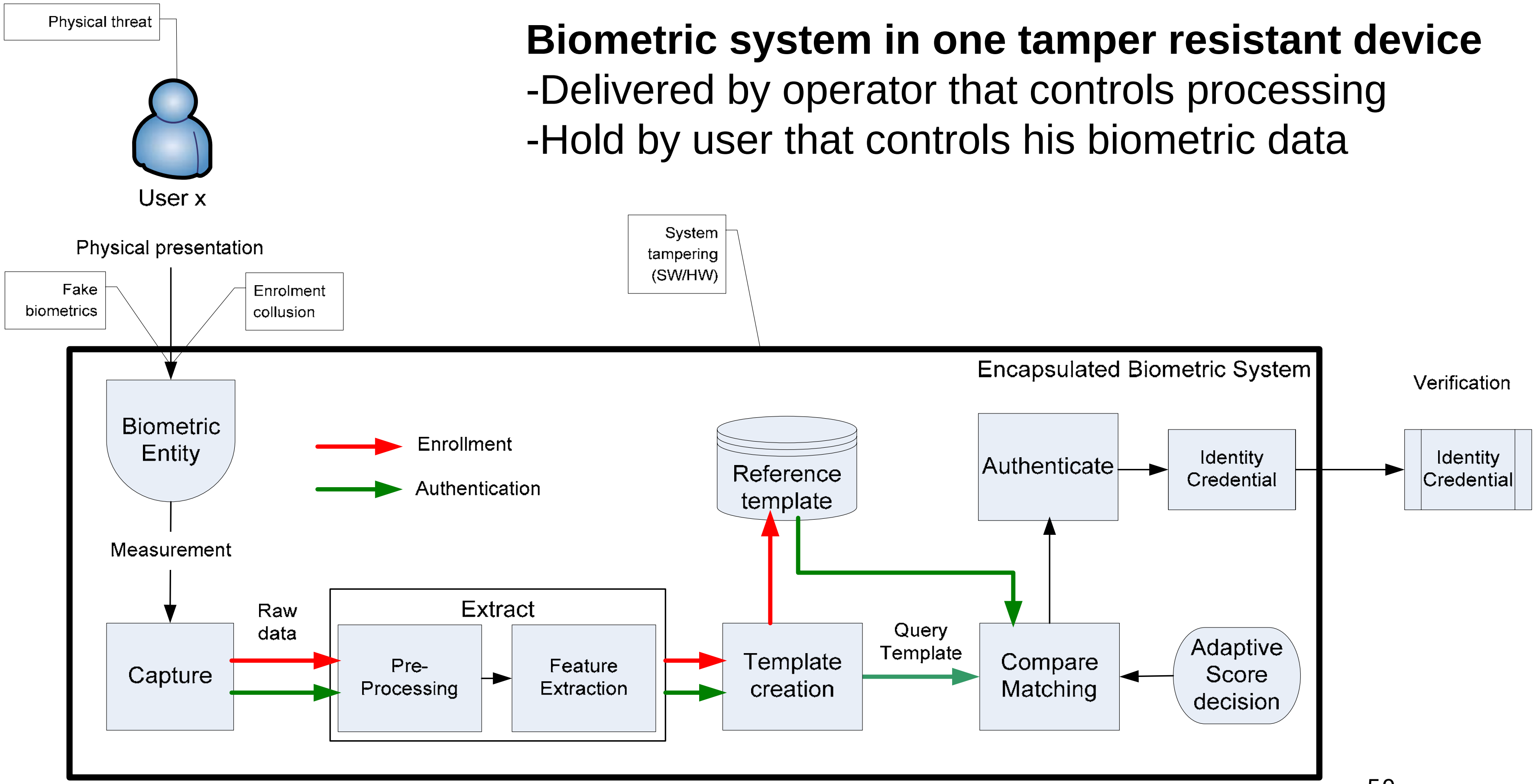


Reduced attack points with ‚encapsulated biometrics‘

Biometric system in one tamper resistant device

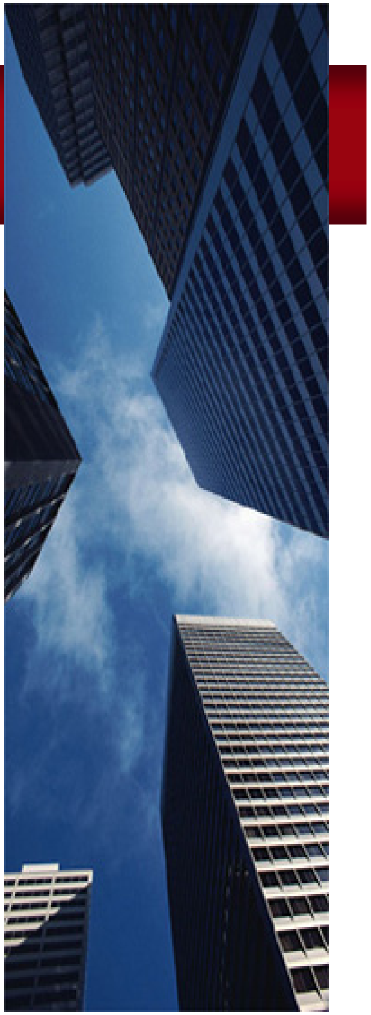
-Delivered by operator that controls processing

-Hold by user that controls his biometric data

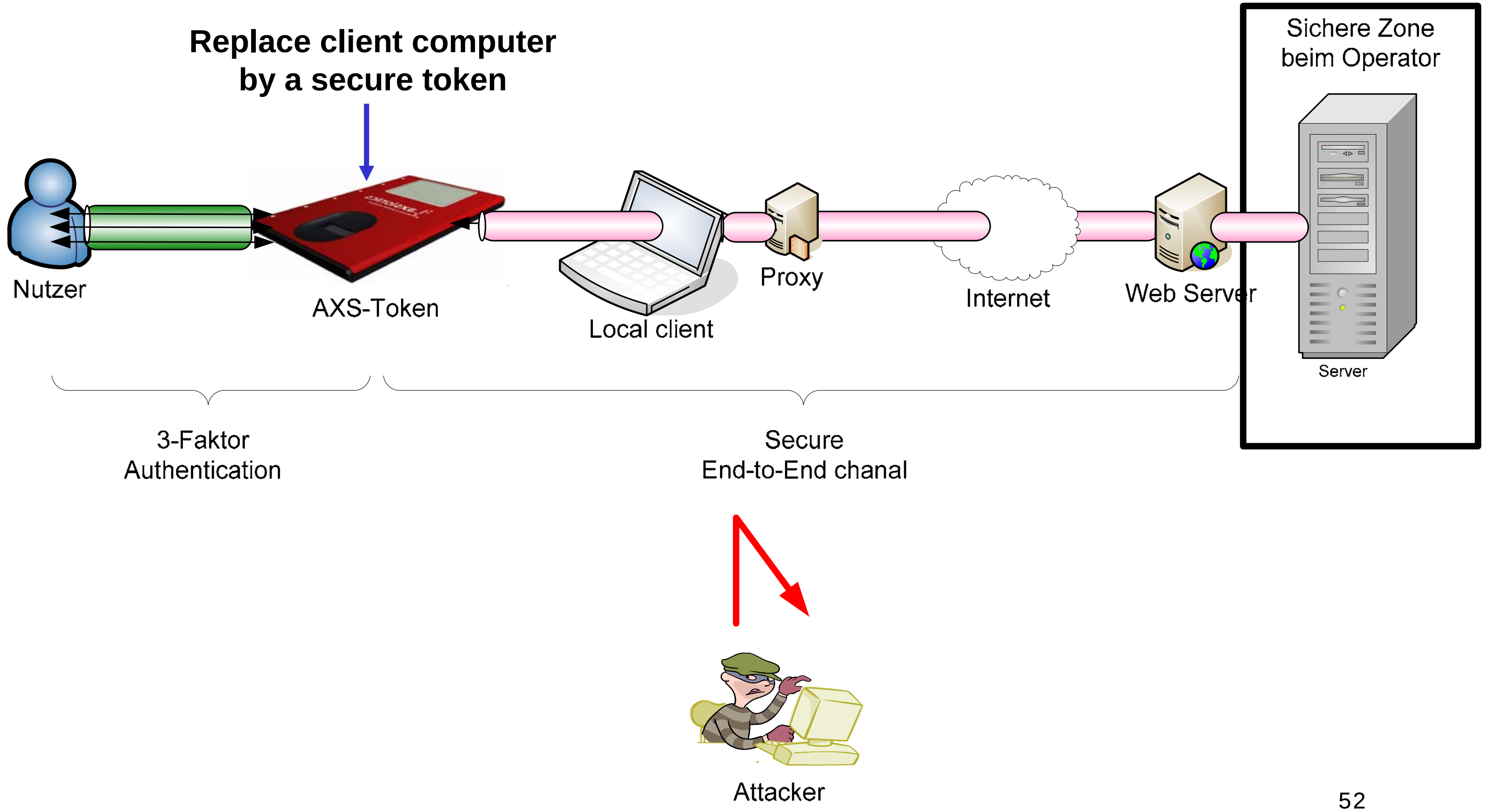


AXS-Authentication System^{TM}

- Architecture
- Key innovations – the advantages
- Demo

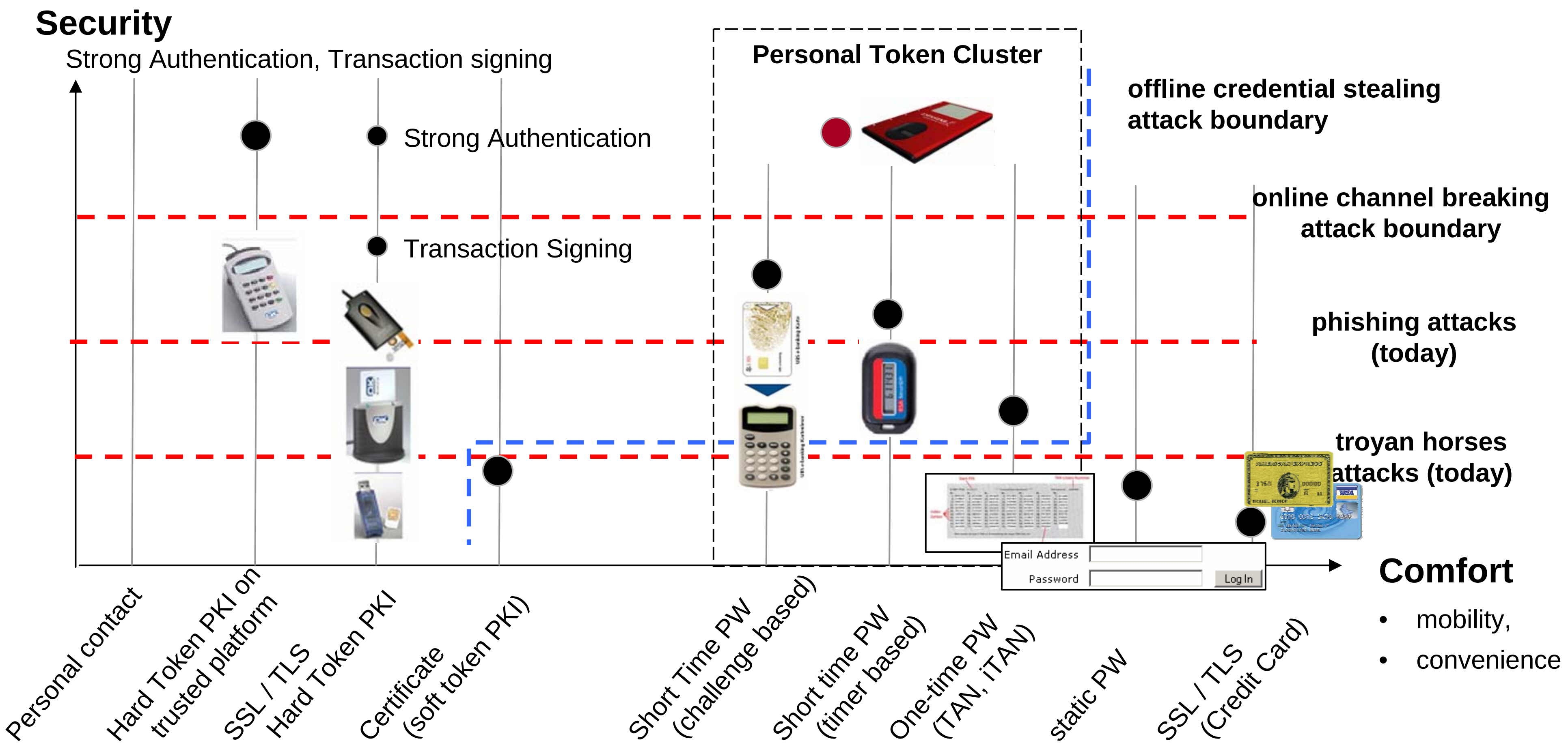


AXS – Authentication System^{TM} approach



Replace client computer by a secure token

AXS-Authentication System – Positioning



Security

Strong Authentication, Transaction signing

● Strong Authentication

● Transaction Signing

Personal Token Cluster

offline credential stealing attack boundary

online channel breaking attack boundary

phishing attacks (today)

troyan horses attacks (today)

Email Address

Password

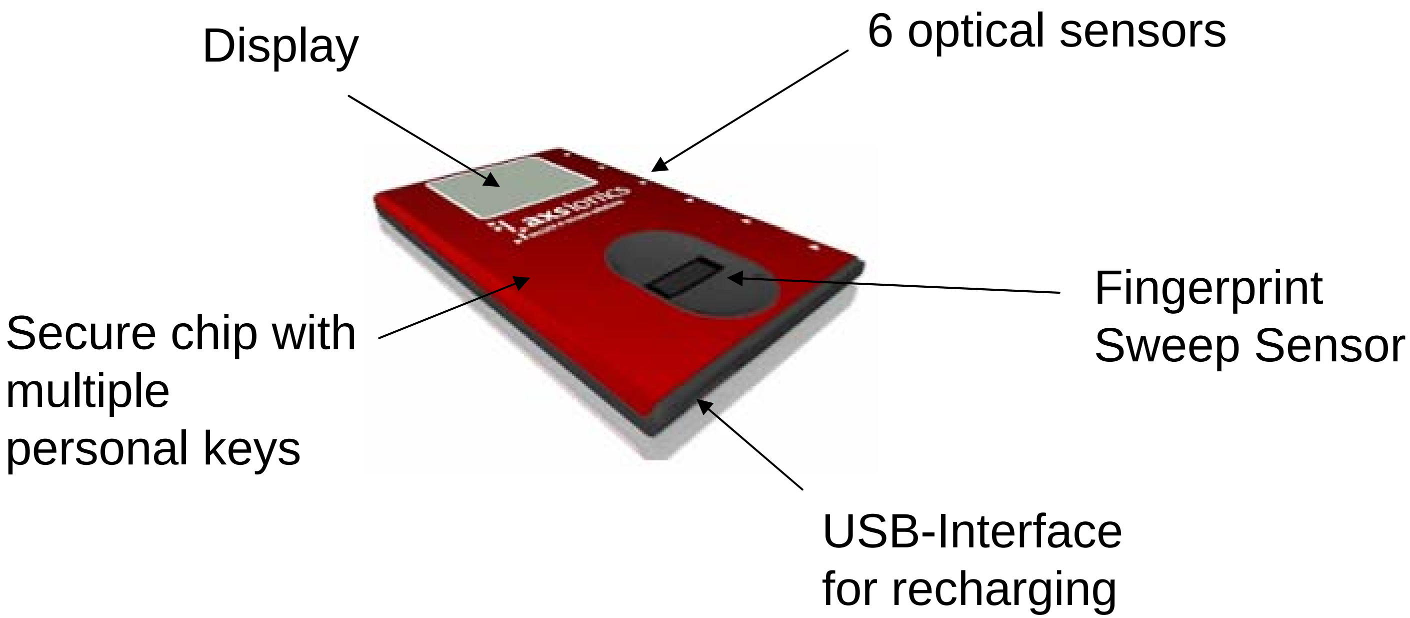
Log In

Comfort

- mobility,
- convenience

Personal contact
Hard Token PKI on trusted platform
SSL / TLS Hard Token PKI
Certificate (soft token PKI)
Short Time PW (challenge based)
Short time PW (timer based)
One-time PW (TAN, iTAN)
static PW
SSL / TLS (Credit Card)

The Internet Passport™
convenient security – for everyone, anywhere



Display

6 optical sensors

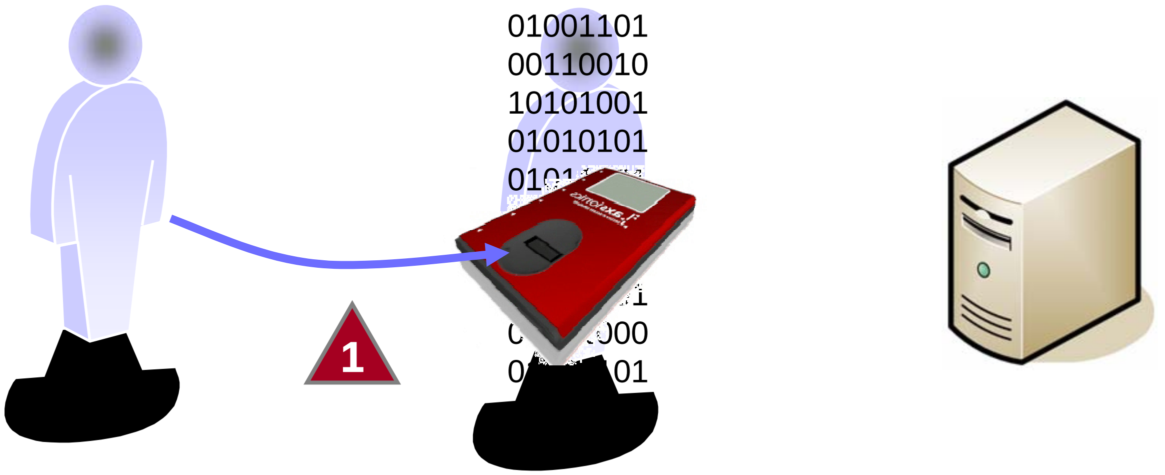
Fingerprint
Sweep Sensor

Secure chip with
multiple
personal keys

USB-Interface
for recharging

User authenticates himself to his personal “Internet Passport™” through the biometric sweep sensor

1 *Trusted transition from the physical to the digital identity*

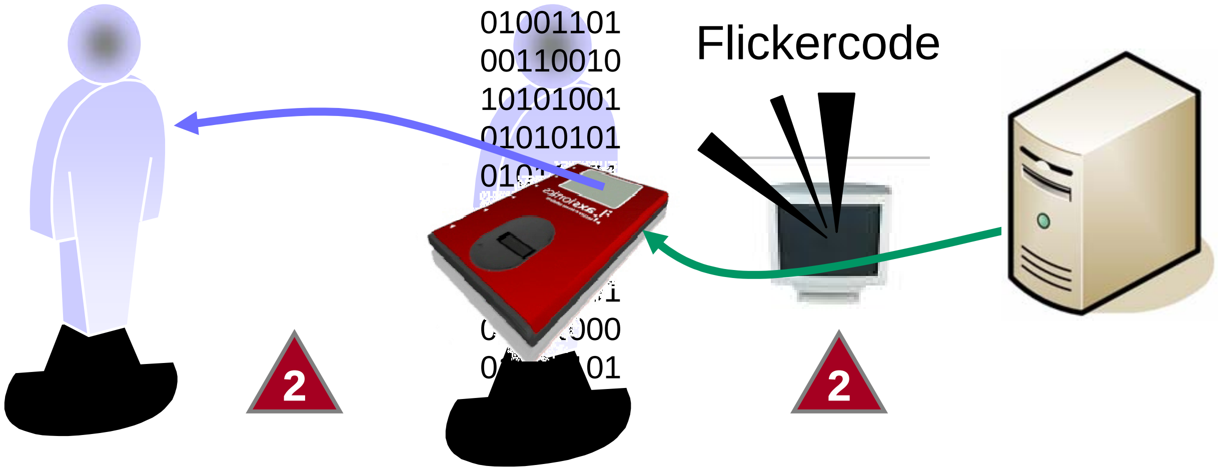


Biometric verification occurs <u>inside</u> the IPP

- Biometric data never leaves the token
- Link to digital identity highly secured

The service provider sends a code back through the optical interface

2 *End-to-end connection security check*



Optical interface - from any screen

- Optical communication interface enables downwards communication - anytime, everywhere
- Strong encryption used for the Flickercode

Convenient use of "The Internet Passport" enables convergence of logical and physical access

Physical Access / Applications

Payment @ POS

NFC

Building Access / e-ticketing

RFID

Logical Access / Applicatoins

Optical Interface

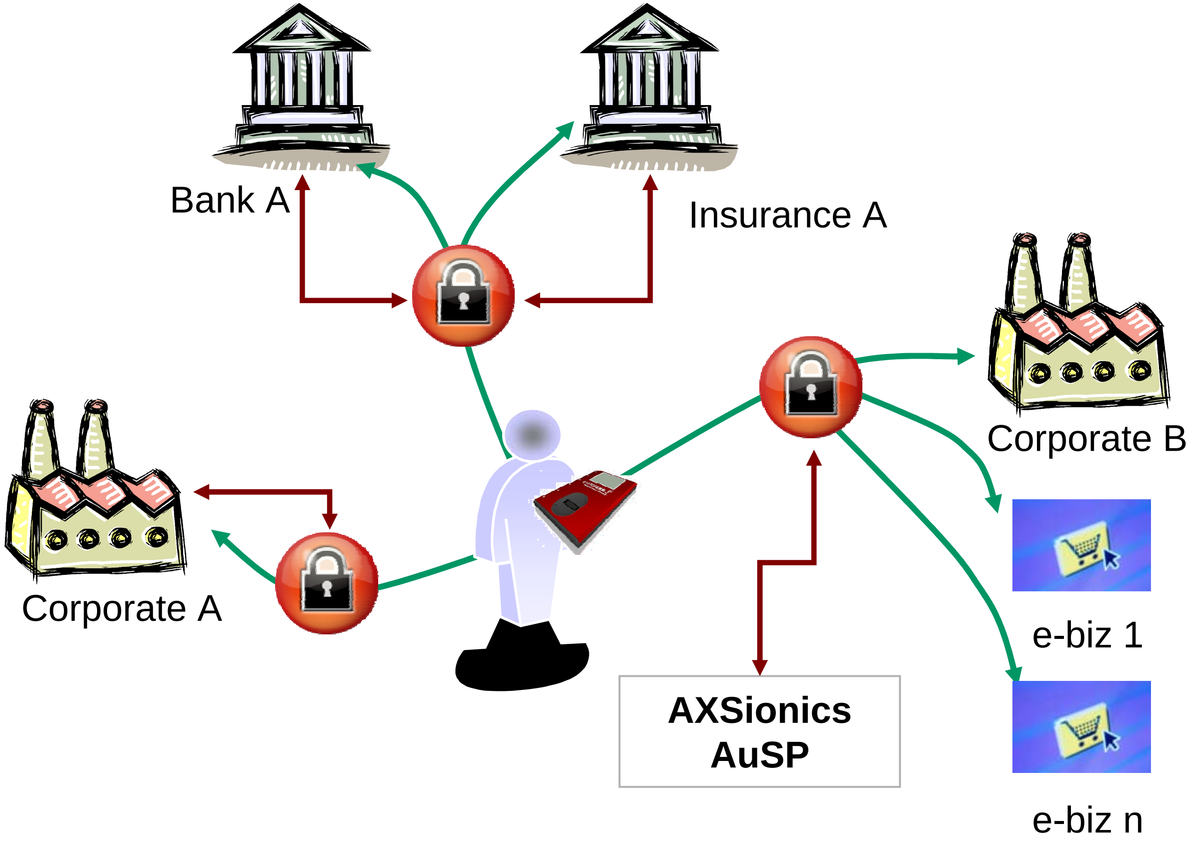
e-transactions, strong authentication

USB-Interface

Specific Smart Card application

axsionics
secure e-access solutions

Multiple personal keys enable to share the cost of infrastructure amongst several providers



Issuer **and/or** Authentication Service Provider

Card belongs to the Infrastructure of the Issuer

<u>one card</u>
multiple provider
no passwords
just convenience

Demo and conclusion

- **Major concerns of the E-society**
  - Endpoint authentication
  - Transaction security
  - Reliable and privacy respecting identity management
  - Credential proliferation for every user
- **Solutions**
  - Strong 3-factor link between person and his digital credentials
  - Cryptographic secured channel between server and user
  - Encapsulated biometrics
  - User Side Identity Management assistant
  - Personal identity federation

axsionics

secure e-access solutions

Thank you

Lorenz Müller
+41 79 341 03 26
lorenz.mueller@axsionics.ch
www.axsionics.com