28.05.98 © IIG Freiburg

See What You Sign

Distribution of Risks in Implementations of Digital Signatures

Arnd Weber

28.05.98 © IIG Freiburg

- **IIG-Telematics**
  - **Institut für Informatik und Gesellschaft, University of Freiburg, Germany**
  - **addressing economic, social and legal issues**

- **Arnd Weber**
  - **Economist**
  - **With ACTS-project SEMPER**
    Secure Electronic Marketplace for Europe

28.05.98 © IIG Freiburg

Overview

I Risk of Trojan Horses with Digital Signatures

II Computers With Secure User Input and Output

III Conclusions

28.05.98 © IIG Freiburg

I

Risk of Trojan Horses with Digital Signatures

28.05.98 © IIG Freiburg

Digital Signatures

- How to replace the signed paper document?
  - Signed offer
  - Signed order
  - Multi-party signed contract
  - Signed receipt
  - Signed invoice

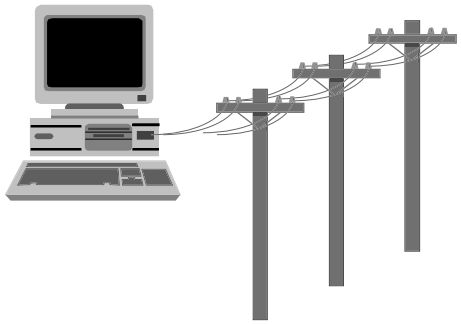
28.05.98 © IIG Freiburg

Main Risk to be Discussed: Trojan Horses

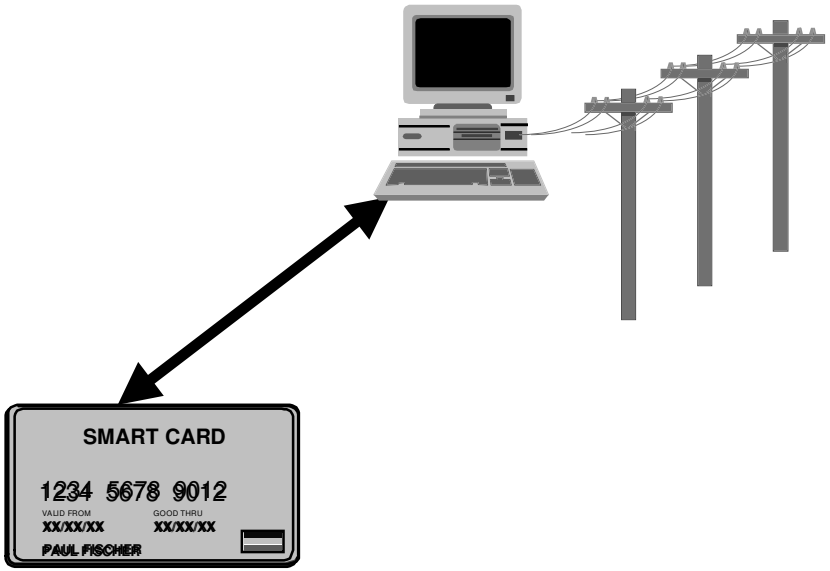
- Examples of malicious code:
  - Text changed on OS level, chipcard signing it
  - Homebanking with Java-applet attacked
  - Excessive phone bills caused
  - Attack on passwords with T-Online

28.05.98 © IIG Freiburg

Threats from Trojan Horses?



Secret Key
on HDD, in Memory



Secret Key and
Signature Function in Chip Card

28.05.98 © IIG Freiburg

Stay Free of Trojan Horses?

- Avoid installation of insecure code?
  - Updates, bug-fixes, attachments, applets, active-X components, helpers, plug-ins
- Code signing?
  - Will the signature help?
  - Trojan horse or signature deleted?

⇒ Not practical with today‘s computers and programs

28.05.98 © IIG Freiburg

Questions

Implementations of Digital Signature Technology

- How secure should the implementation be?
- Who should bear the remaining risk?

28.05.98 © IIG Freiburg

Digital vs. Handwritten Signature

- Impostor needs no physical access
- Impostor can be remote
- Distributed attacks possible
- Disputed signature technically perfect, no hope in graphological expertise
- Little experience with binding digital signatures, but high security image

28.05.98 © IIG Freiburg

Economic Risk with Trojan Horses

- For signer:
  - ECU 10k or 100k loss is significant for private person or small company
  - If insured: Difficult to tell between criminal and victim. Will insurer pay?
- For relying party:
  - Risk of not getting paid can be significant for small company
  - Damage to reputation possible
- For insurance, if there is one:
  - Today: Likelyhoood x size of damage unknown.
  - Future: Organized crime

28.05.98 © IIG Freiburg

Legal Risks With Trojan Horses

European Commission's proposal for a directive:

„a signature ... which ... is created using means that the signatory can maintain under his sole control."

German Digital Signature Law:

„technical components ... are necessary to make forgeries ... and the falsification of ... data ... visible and provide protection against unauthorised use of private signature keys."

28.05.98 © IIG Freiburg

What is Needed?

- Smartcard + software?
  - Unknown how difficult to attack
- Turn normal computers into secure ones?
  - Short run not imaginable

⇒ Special hardware, with secure user I/O

  - Portable „electronic wallets“

28.05.98 © IIG Freiburg

II

Computers With Secure User Input and Output

Steps towards Secure Computing

28.05.98 © IIG Freiburg

- Bull Safepad for C-SET
- Brokat „handysignatures“

- Screens too small
- Not open

How to View the Document?

28.05.98 © IIG Freiburg

Order

Buyer's organisation, address, country
Tel./fax/email/URL
Company registration no.
VAT-No.
Buyer's name
Certificate
Seller's organisation, address, country
Seller's name
Date
Buyer's reference number
Content description
Seller's article number
Buyer's article number
Number of items
Unit of item
Item price
Tax
Freight and delivery
Total
Currency
Shipping address
Comments
Appended files
Applicable Law
Agreed means of payment
Payment agreed by
Buyer's signature

Split User Interface

← **All Fields on Normal Screen**

↓ **Essential Fields on Secure Hardware**

```
Order
Buyer
Certificate
Date
Description
Total
Currency
Signature
```

28.05.98 © IIG Freiburg

Benefits of Special Secure Hardware I

- Security
  - For high values
  - In case Trojan horses emerge
  - If users are afraid of Trojan horses
  - To reduce abuse
  - With biometrics
  - With battery buffered key storage
- Mobility
  - Use with several computers
  - Use with several applications
  - Robust packaging possible

28.05.98 © IIG Freiburg

Benefits of Special Secure Hardware II

- **Functionality**
  - More memory
  - More transparency
  - More privacy
  - Logical add-on to phones, pocket calculators, organizers, modems, etc.
- **Efficiency**
  - Cheaper than full secure computer
  - Faster clock than SC
  - Robust, cheap interface

28.05.98 © IIG Freiburg

Challenges

- To build wallets which provide a securely implemented signature function
  - trustworthy design without holes
  - open
  - capable of displaying business documents
- To develop the business case for them
  - Build on benefits of electronic commerce
  - Build on benefits from replacing the paper documents
  - Build on other benefits of secure hardware

28.05.98 © IIG Freiburg

III

Conclusions

28.05.98 © IIG Freiburg

Who Should Bear the Remaining Risk?

- If the risk is practically zero, the signatory.
- If a known risk exists, the relying party or a third party should state they bear the risk.
- In any case, players must be given a chance to opt for a monthly liability limit.

28.05.98 © IIG Freiburg

How Secure Should the Implementation be?

- Penetration impossible
- Find a business case for secure implementations!
  - Develop secure hardware with high functionality and good interface
  - First address medium value commerce

28.05.98 © IIG Freiburg

Please Contact

Arnd Weber

IIG Telematics
Friedrichstraße 50
D 79098 Freiburg

Tel.: +49 - 761 - 203-5704
<aweber@iig.uni-freiburg.de>
<www.iig.uni-freiburg.de/~aweber> ***will put this presentation here***

See also: <www.semper.org>

with thanks to all colleagues in project SEMPER and the Institute