Dr. Stefan Probst
SSW Consulting – Security & Software Consulting
mailto: stefan.probst@ssw-consulting.net

Special Forum „Security“

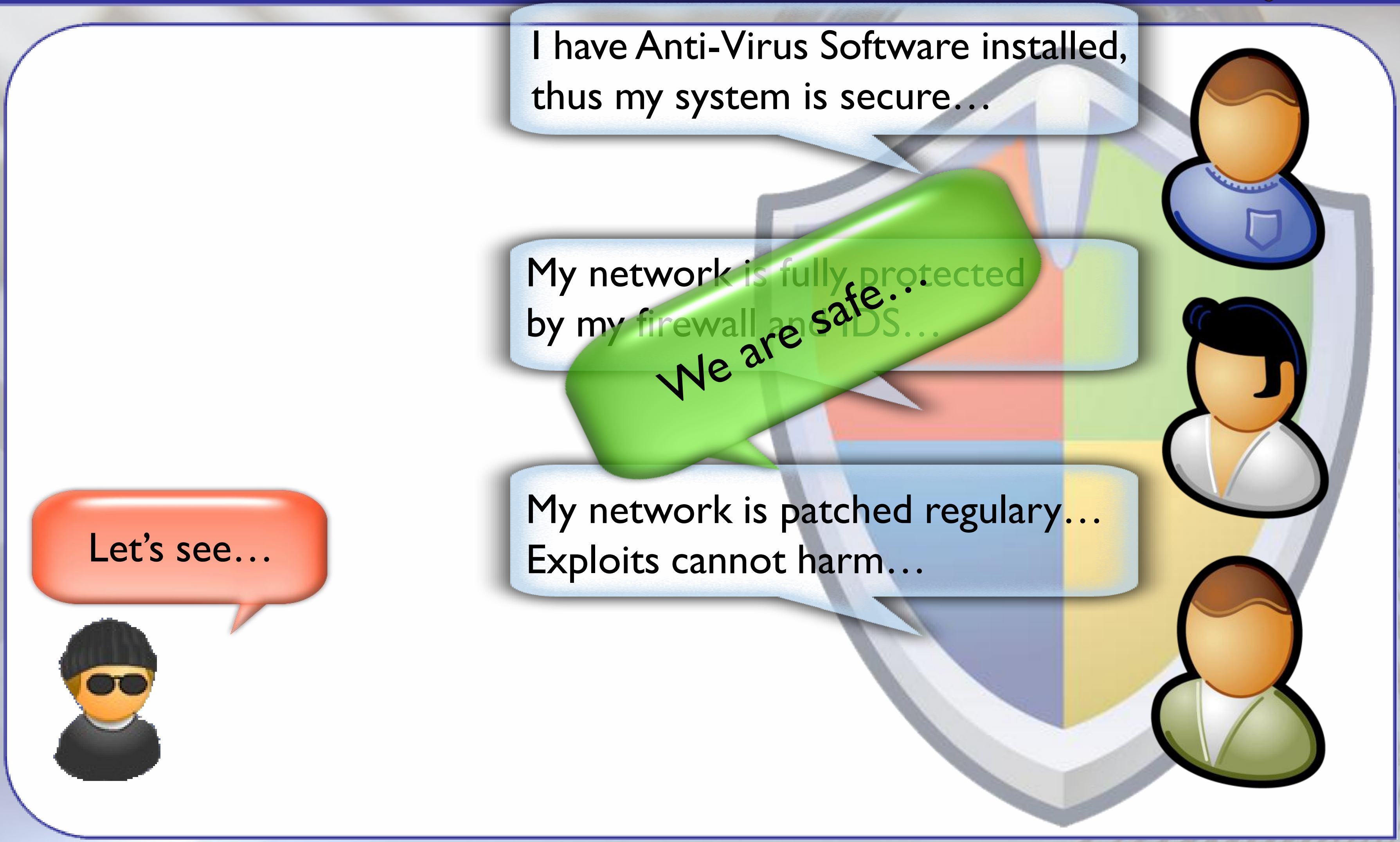
Information Roadshow 2008

About the presenter…

- Dr. Stefan Probst
  - 2003: Security consulting for small and medium sized companies
  - 2004: Wrote his PhD thesis in the field software security and passed with distinction
  - 2004: Conducting several security workshops for Microsoft Austria
  - 2005: Program Manager for Mobile & Workplace Security at Siemens AG
- „I don‘t want you to become a hacker, I want you to become aware of the danger!“

Do we need Security?

Some myths about security…



I have Anti-Virus Software installed, thus my system is secure…

My network is fully protected by my firewall and IDS…

We are safe…

My network is patched regulary… Exploits cannot harm…

Let’s see…

Some examples…

demo

- Improper configured systems…
  - Google… 🕵🕵
  - Google again… 🕵
- Human being…
  - ebay 🕵
- Existing flaws in today’s software…
  - Buffer Overflow

CSI / FBI Computer Crime Survey 2008

	2004	2005	2008
Participants	494	700	433
Web Issues	17%	10%	17%
Unauthorized access	37%	32%	29%
Average Loss (in U$)	~ $ 526.000	~ $ 204.000	~ $ 299.000*
Financial Fraud	8%	7%	12%

- Some facts for 2008:
- Average Cost on financial fraud: $ 463.100
- Average Cost on dealing with Bot Computers: $ 345.600
- 94% use firewalls (97% in 2005)
- 97% use anti-virus software (96% in 2005)
- 69% use Intrusion Detection Software (IDS) (72% in 2005)
- 36% use strong authentication (Smart Card, One-Time Pads) (42% in 2005)

Do we need security?

*The chain is no weaker than its strongest link
Photo by ToHell, 2003-09-23 in Slagsta, SE

Part I: Introducing Security

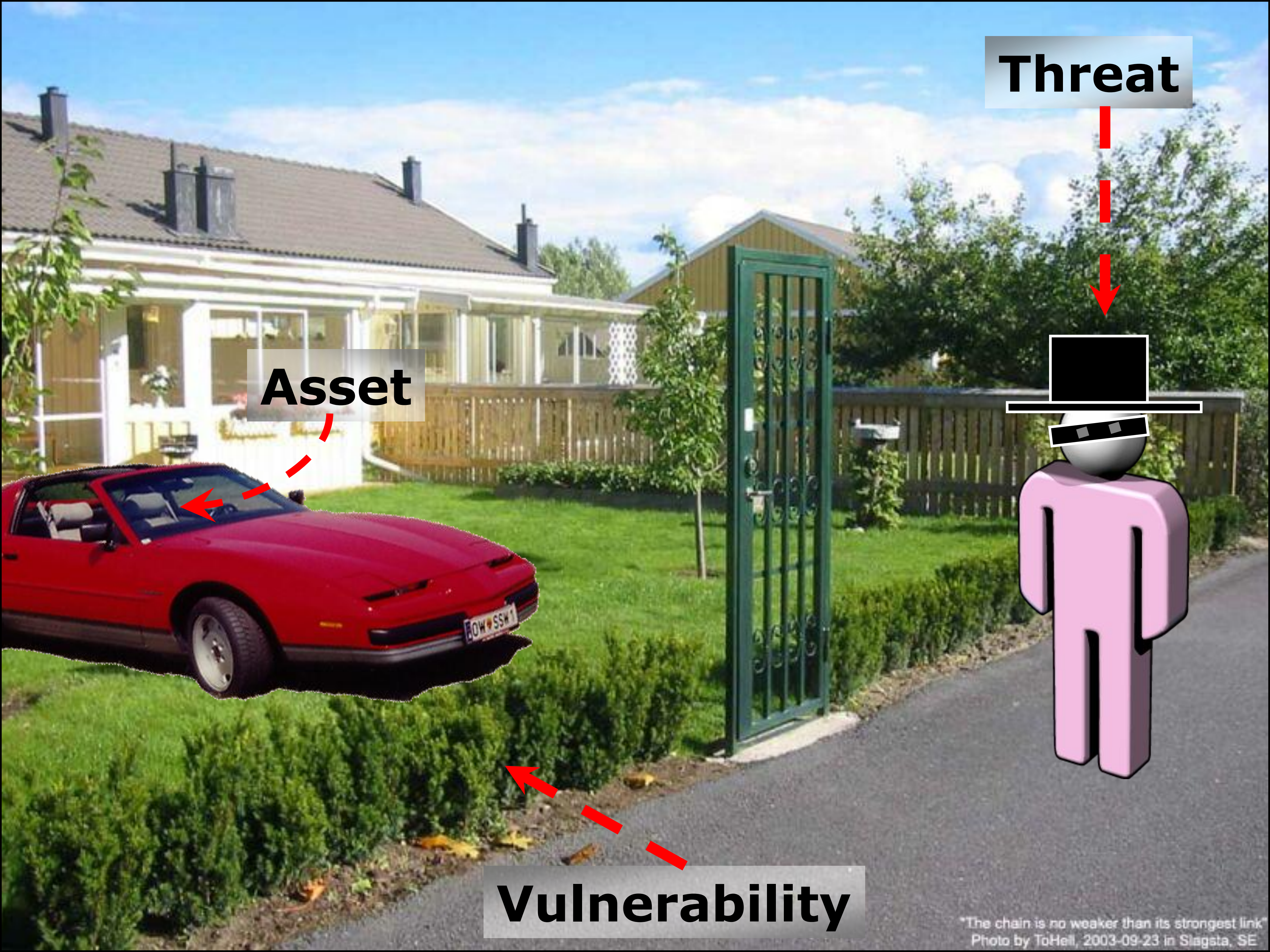
Motivation

- Security is required and a KO criterion
  - User require “secure” software applications
  - User has to be convinced of the security
- Existing Problems
  - Requirements are getting more and more complex
    - Passwords vs. Distributed authentication
  - Security is a complex area!
  - Target environment has many uncertainties
  - Contest between “good” and “bad”

Terms and Definitions

„What is security?“

- „Security is about the protection of assets“ (Gollmann)
  - We have to know our assets and their values
- Measures for increasing security
  - Prevention: prevent assets from being damaged
  - Detection: detect when an asset has been damaged, how it has been damaged, and who has caused the damage
  - Reaction: measures that allow to recover the assets or to recover from damage



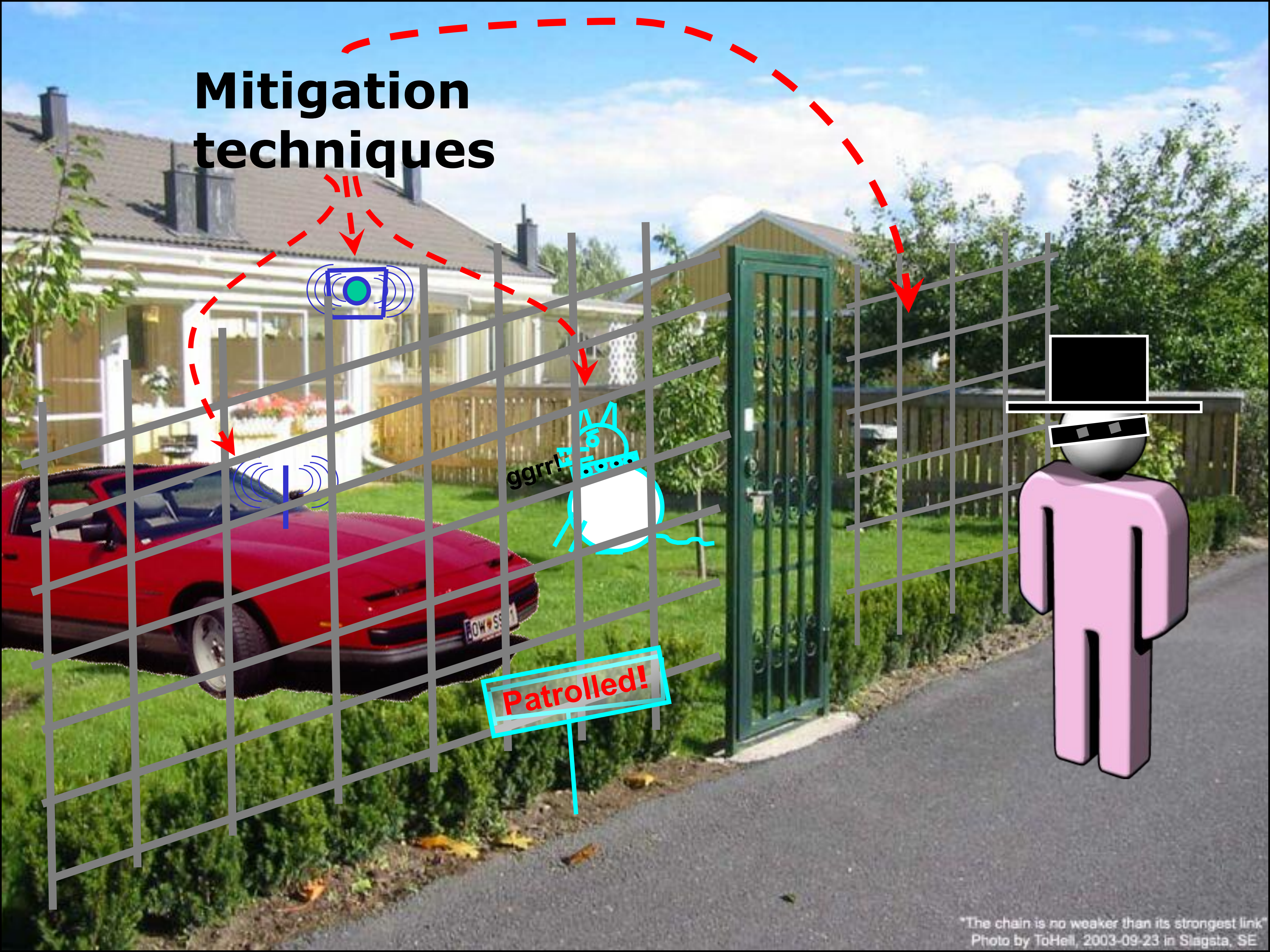
Threat

Asset

Vulnerability

"The chain is no weaker than its strongest link"
Photo by ToHell, 2003-09-23 in Slagsta, SE

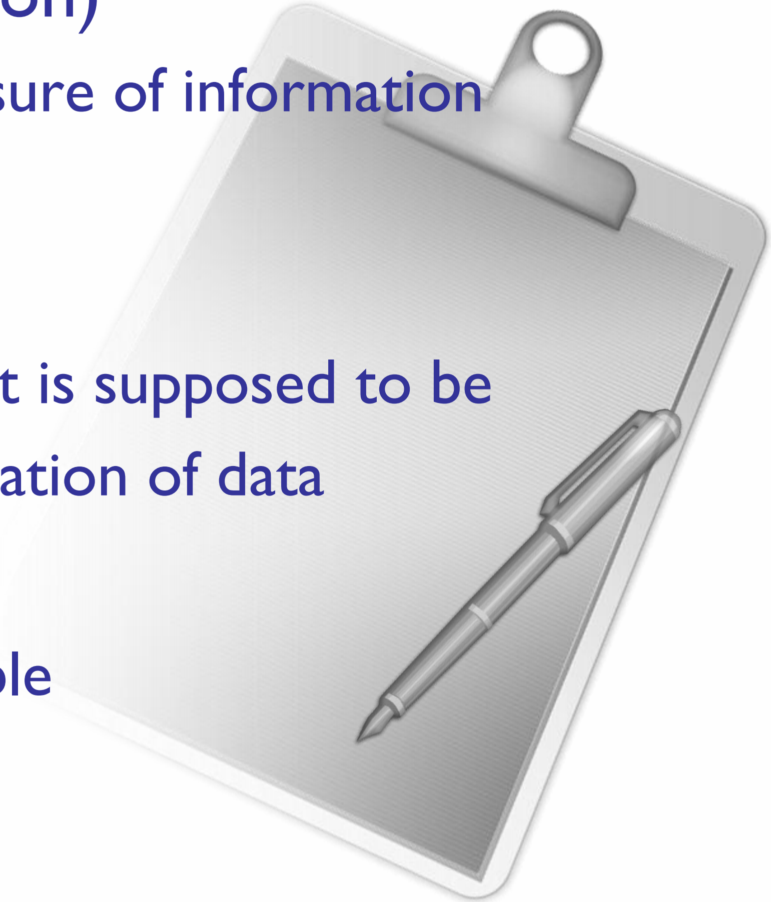
Mitigation techniques



"The chain is no weaker than its strongest link"
Photo by ToHell, 2003-09-23 in Slagsta, SE

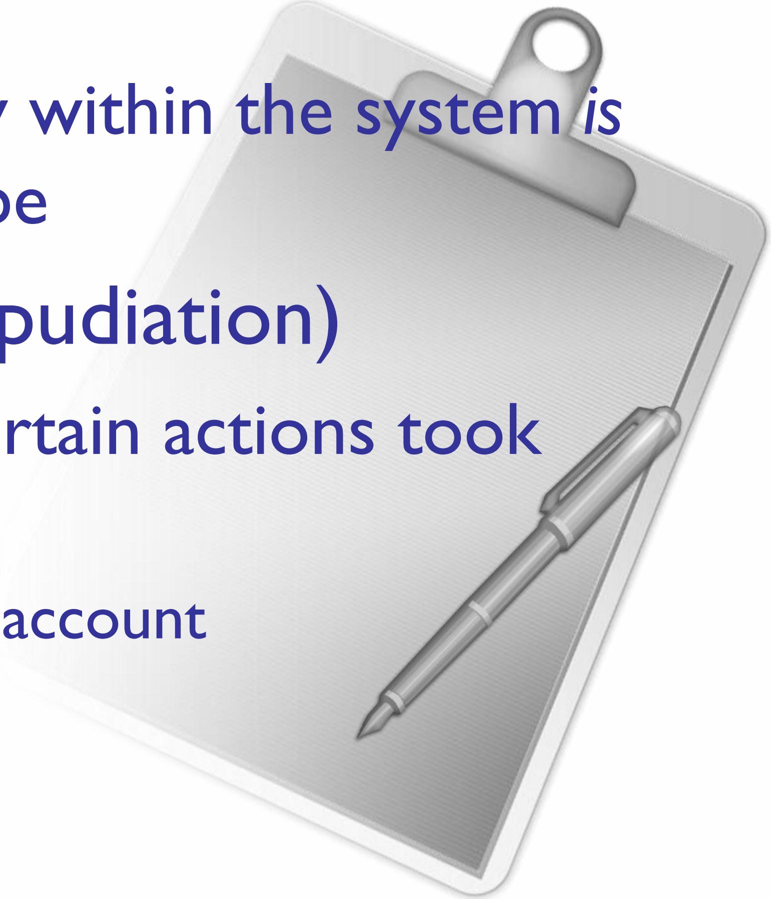
Responsibilities

- Confidentiality (Authorization)
  - prevent unauthorized disclosure of information
  - secrecy and privacy
- Integrity
  - Ensure that everything is as it is supposed to be
  - Prevent non allowed modification of data
- Availability
  - Ensure that data are accessible to authorized users

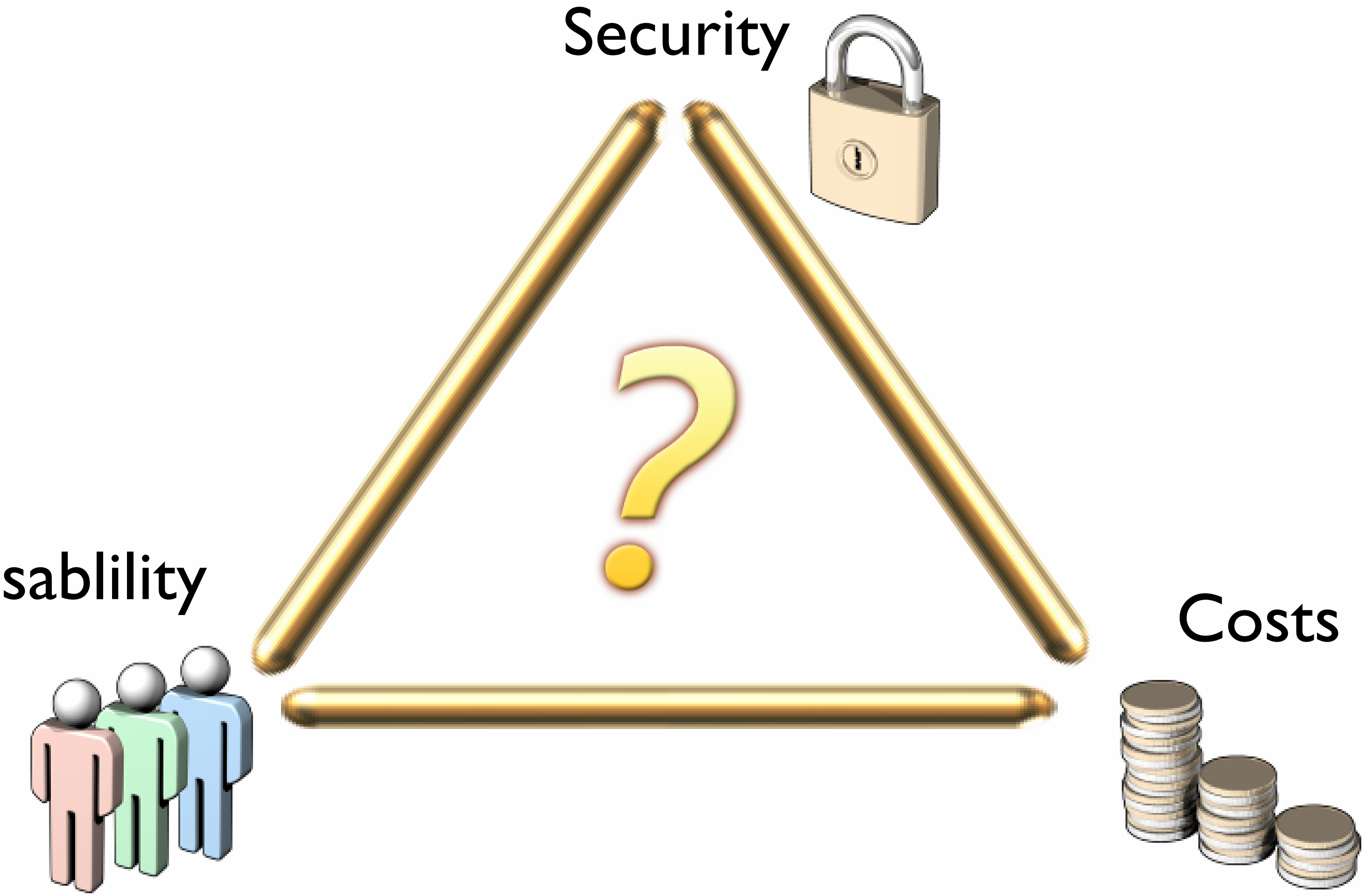


Responsibilities

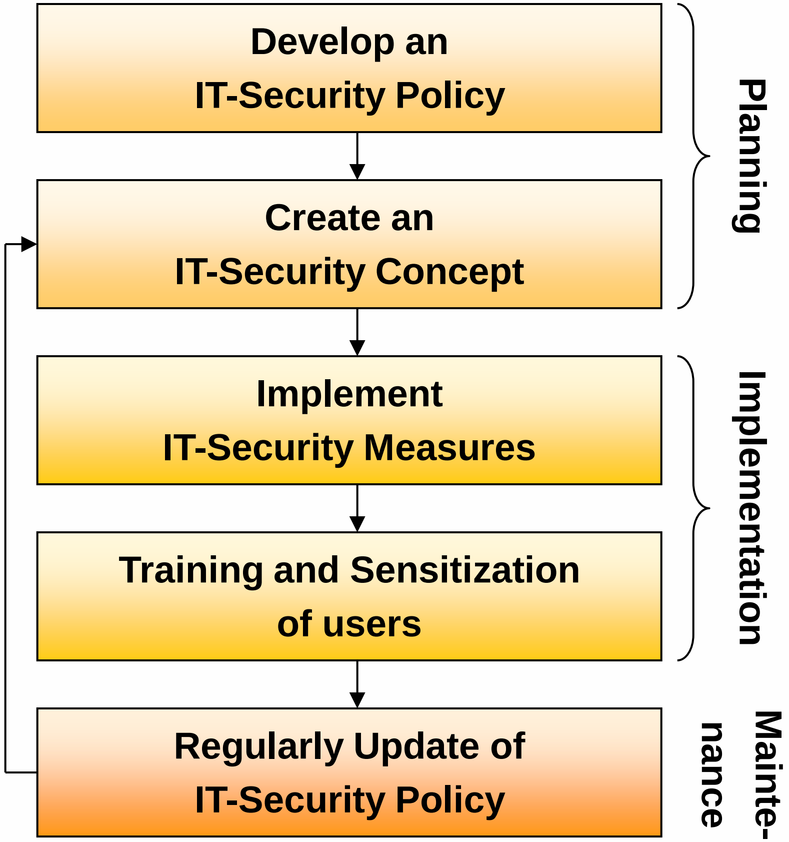
- Authentication
  - Ensure that each identity within the system *is* the identity it claims to be
- Accountability (Non-Repudiation)
  - Provide evidence that certain actions took place
    - e.g. transfer money from account



A big problem in IT security…



IT-Security Process



Develop an IT-Security Policy

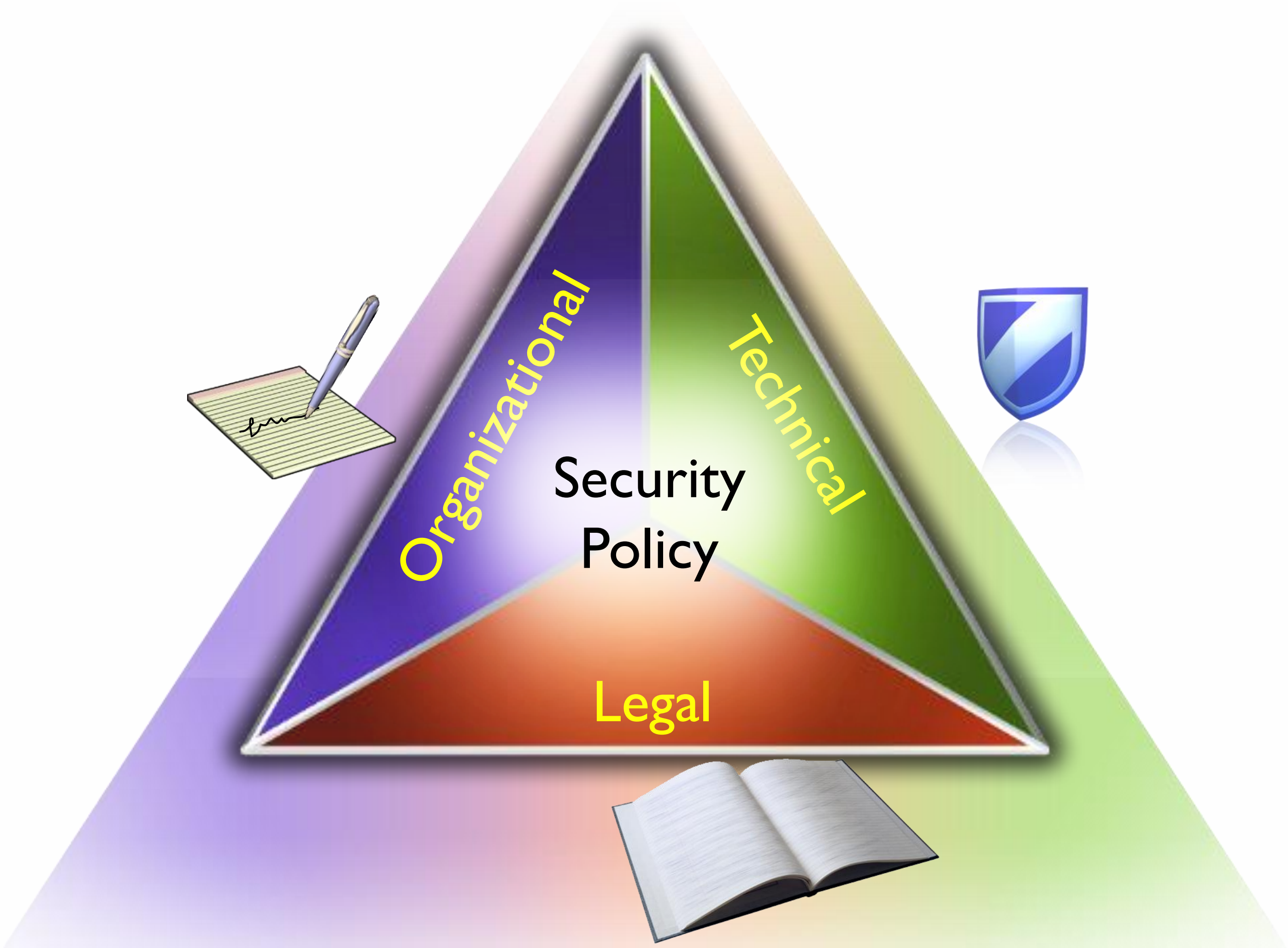
Create an IT-Security Concept

Implement IT-Security Measures

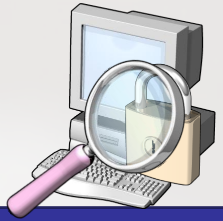
Training and Sensitization of users

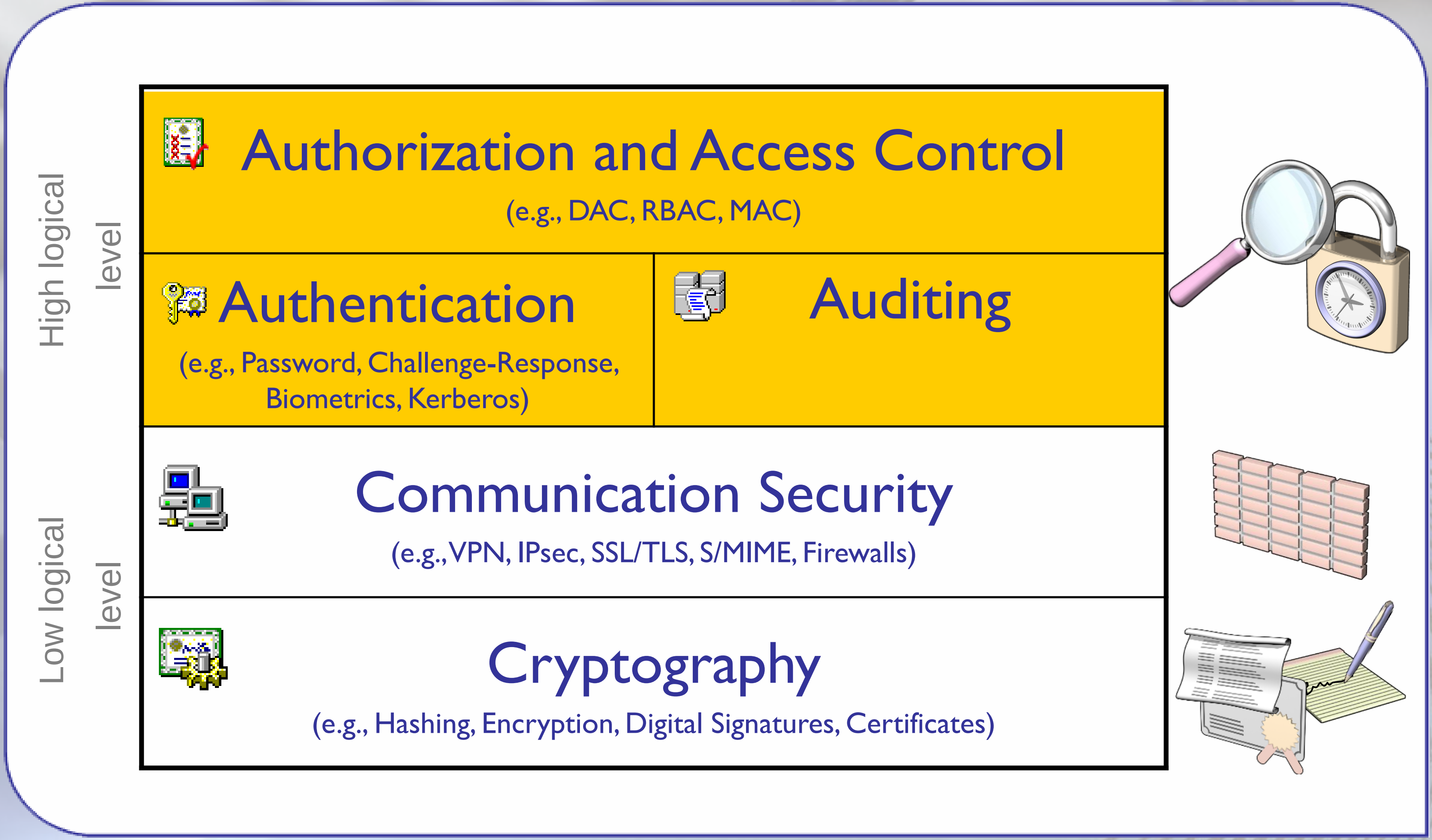
Regularly Update of IT-Security Policy

Security Measures



Various Levels of IT-Security





High logical level

Low logical level

Authorization and Access Control

(e.g., DAC, RBAC, MAC)

Authentication

(e.g., Password, Challenge-Response, Biometrics, Kerberos)

Auditing

Communication Security

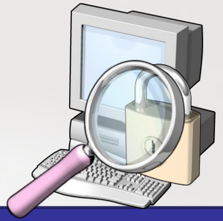
(e.g., VPN, IPsec, SSL/TLS, S/MIME, Firewalls)

Cryptography

(e.g., Hashing, Encryption, Digital Signatures, Certificates)

Part 2:
Main Security Issues

Main Security Issues



- Defective Implementation
  - Frowzy implementation of security mechanisms
- Security is addressed insufficient
  - TCP/IP: reliable but not secure!
- User with no or poor security awareness
  - You can do almost everything… It doesn't help if the user is not on your side!

Defective Implementations

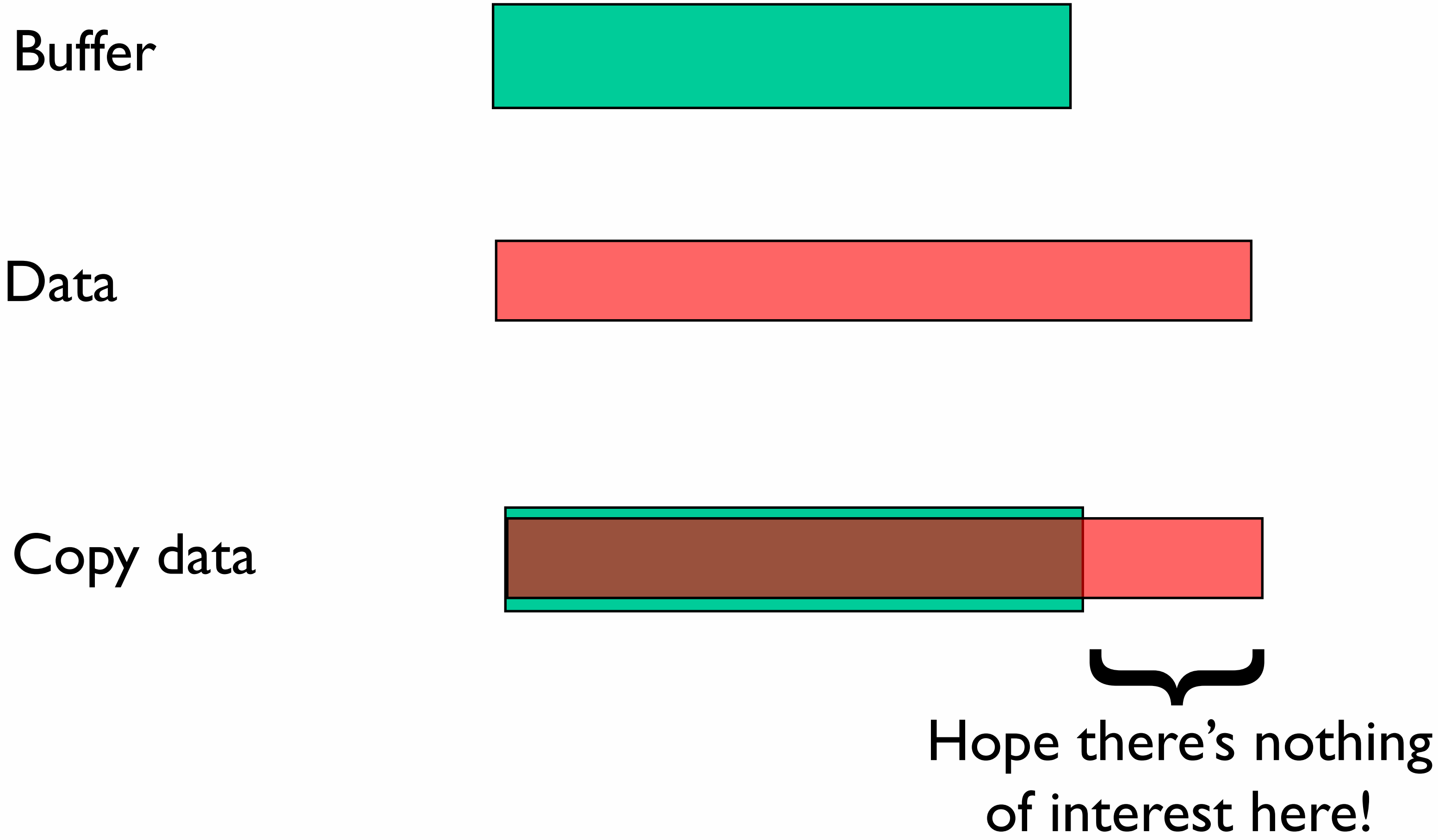
- Humans make mistakes…

  Developers are humans!

- Theory
  - Very good, thoroughly researched mechanisms for encryption.
  - Security depends on the selected key.
- Practice
  - WLAN / WEP:
    - Key length is too short (40 Bit)
    - 24 Bit Initial-Vector → 2^{24} variations, after 5h first recurrence

Anatomy of Buffer Overruns

demo



Buffer

Data

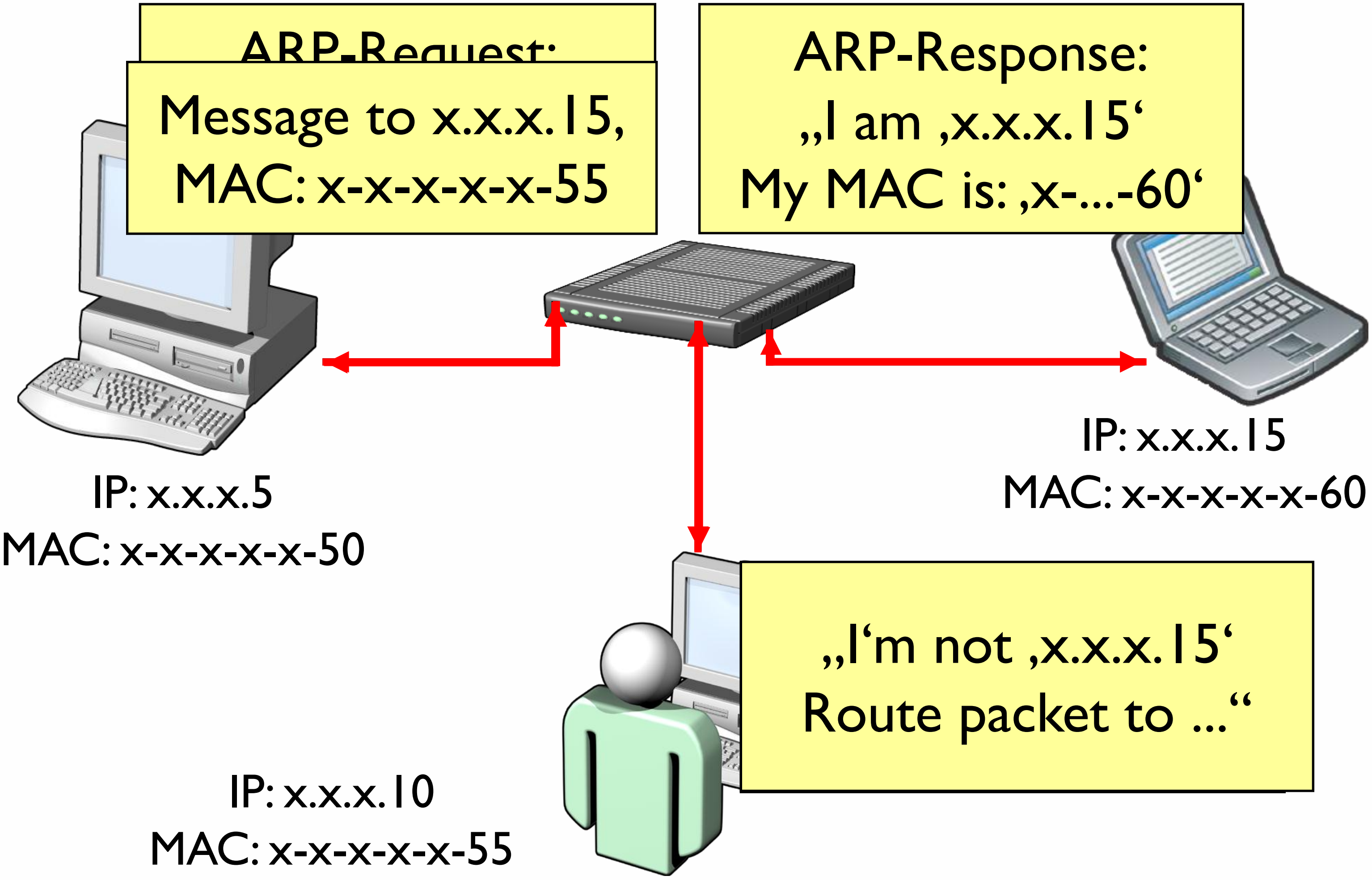
Copy data

Hope there's nothing of interest here!

Security is addressed insufficient

- TCP/IP
  - Very reliable, not secure!
  - Everything is transmitted in plain-text
  - Addresses are easy to spoof
- Samples:
  - Plain-text passwords: Mail, FTP, HTTP
  - Address-Spoofing: ARP-Spoofing

ARP-Spoofing



ARP-Request:

Message to x.x.x.15,
MAC: x-x-x-x-x-55

ARP-Response:
„I am ‚x.x.x.15‘
My MAC is: ‚x-...-60‘

IP: x.x.x.5
MAC: x-x-x-x-x-50

IP: x.x.x.15
MAC: x-x-x-x-x-60

„I‘m not ‚x.x.x.15‘
Route packet to ...“

IP: x.x.x.10
MAC: x-x-x-x-x-55

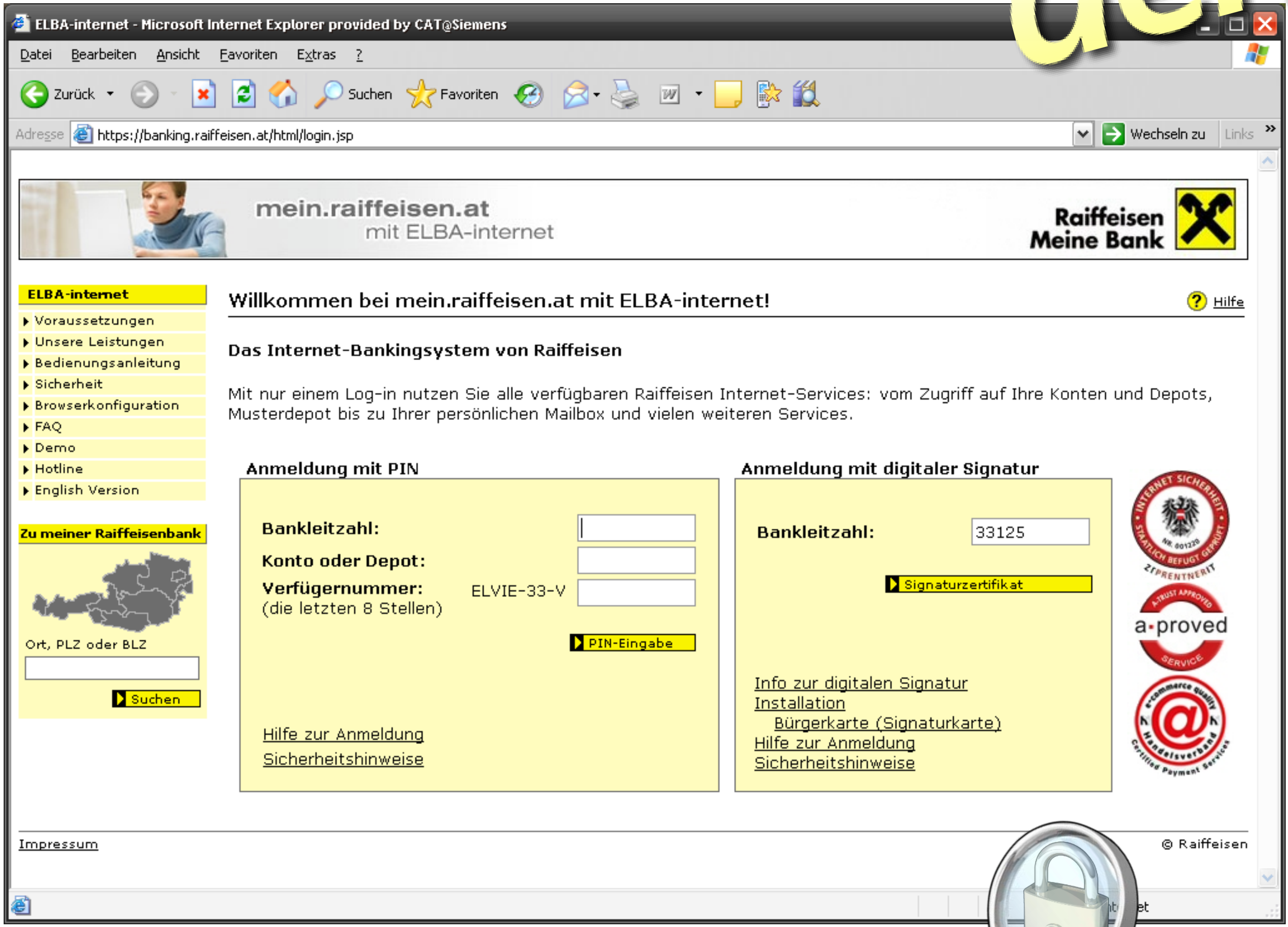
User with no security awareness

demo

- System enforces very good passwords.
- Passwords are transmitted via secure connection (encrypted)
  … but …
- … the user writes his password on a note that is adhered to the monitor.
- … the user prints out secret documents on a publicly accessible printer.
- … does not lock the computer or the office during coffee break.
- …

User with no security awareness

demo


ELBA-internet - Microsoft Internet Explorer provided by CAT@Siemens
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Adresse
Wechseln zu
Links

https://banking.raiffeisen.at/html/login.jsp

mein.raiffeisen.at
mit ELBA-internet

Raiffeisen
Meine Bank

ELBA-internet
- Voraussetzungen
- Unsere Leistungen
- Bedienungsanleitung
- Sicherheit
- Browserkonfiguration
- FAQ
- Demo
- Hotline
- English Version

Zu meiner Raiffeisenbank

Ort, PLZ oder BLZ

Suchen

Willkommen bei mein.raiffeisen.at mit ELBA-internet!

Hilfe

Das Internet-Bankingsystem von Raiffeisen

Mit nur einem Log-in nutzen Sie alle verfügbaren Raiffeisen Internet-Services: vom Zugriff auf Ihre Konten und Depots, Musterdepot bis zu Ihrer persönlichen Mailbox und vielen weiteren Services.

Anmeldung mit PIN

Bankleitzahl:

Konto oder Depot:

Verfügernummer: ELVIE-33-V
(die letzten 8 Stellen)

PIN-Eingabe

Hilfe zur Anmeldung
Sicherheitshinweise

Anmeldung mit digitaler Signatur

Bankleitzahl: 33125

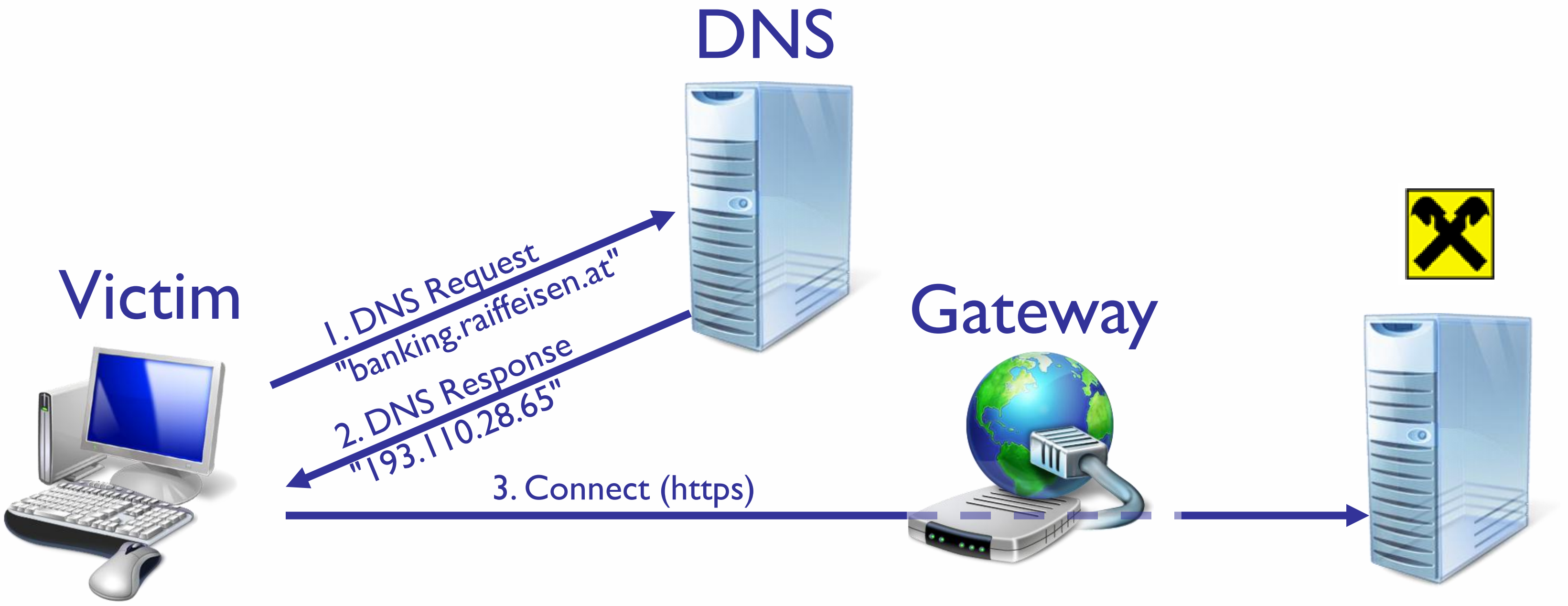
Signaturzertifikat

Info zur digitalen Signatur
Installation
Bürgerkarte (Signaturkarte)
Hilfe zur Anmeldung
Sicherheitshinweise

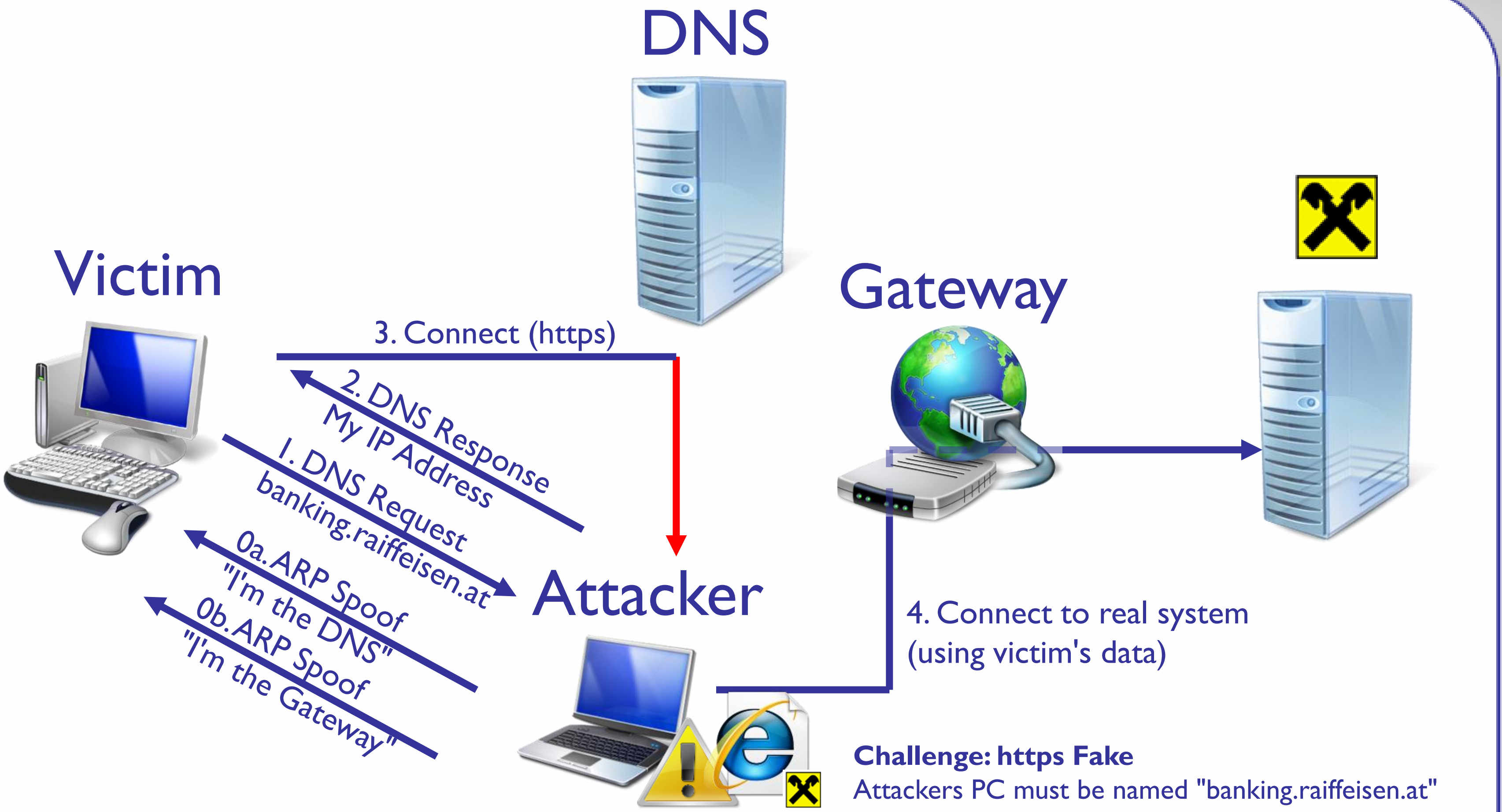
Impressum

© Raiffeisen

How the *** did this work???



How the *** did this work???



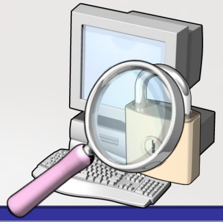
Challenge: https Fake
Attackers PC must be named "banking.raiffeisen.at"
We won't get an official SSL certificate → self issuing
Get the user to accept our self issued certificate

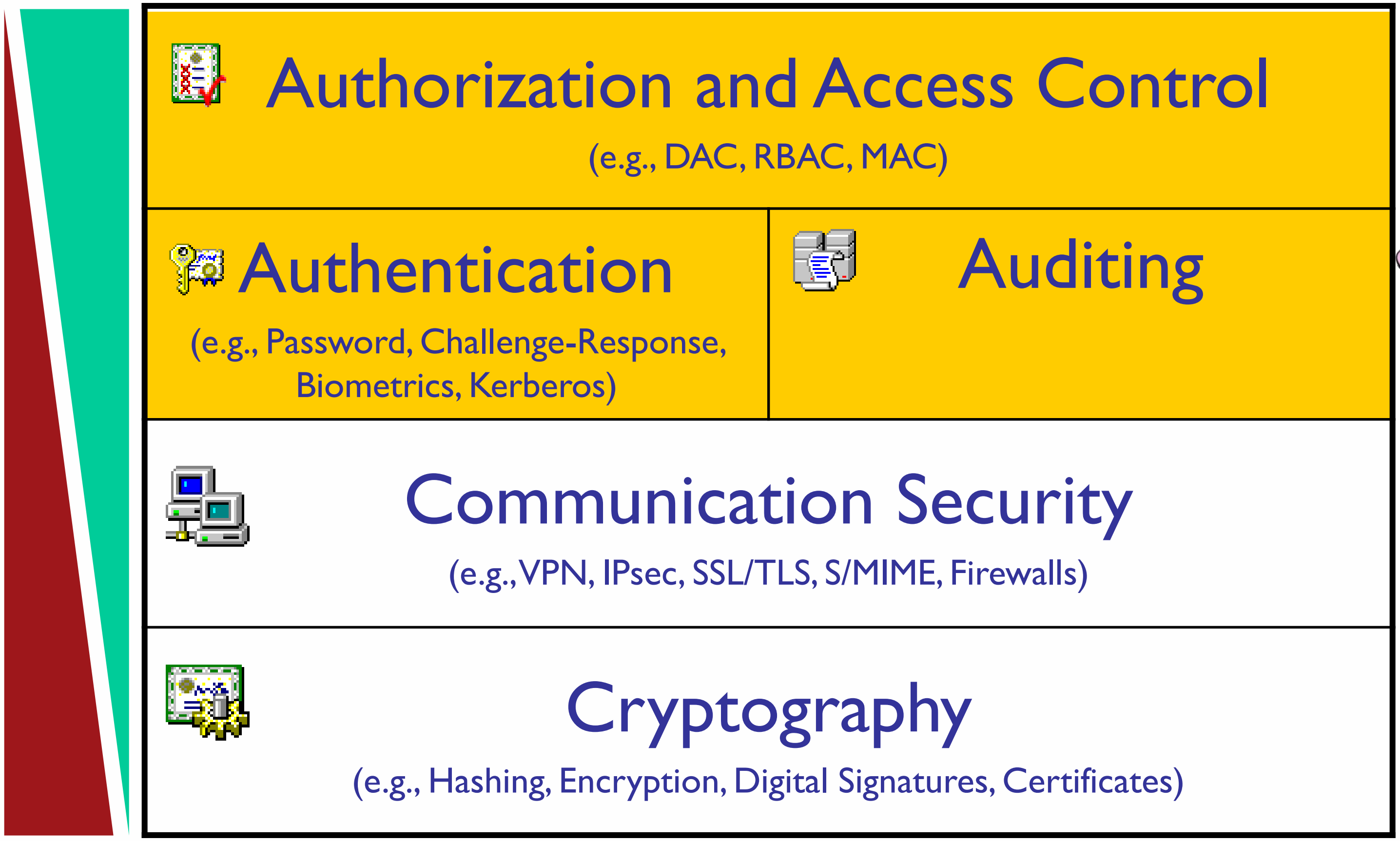
Part 3: Counter Strike

„Think like an attacker“

- In order to find or prevent an attack, you have to know how you are going to be attacked…
- Find mechanisms that allows you to take countermeasures!
- However: Attack is never the best form of defense!

Subjects to attack





Authorization and Access Control

(e.g., DAC, RBAC, MAC)

Authentication

(e.g., Password, Challenge-Response, Biometrics, Kerberos)

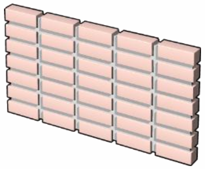
Auditing

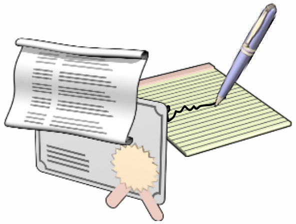
Communication Security

(e.g., VPN, IPsec, SSL/TLS, S/MIME, Firewalls)

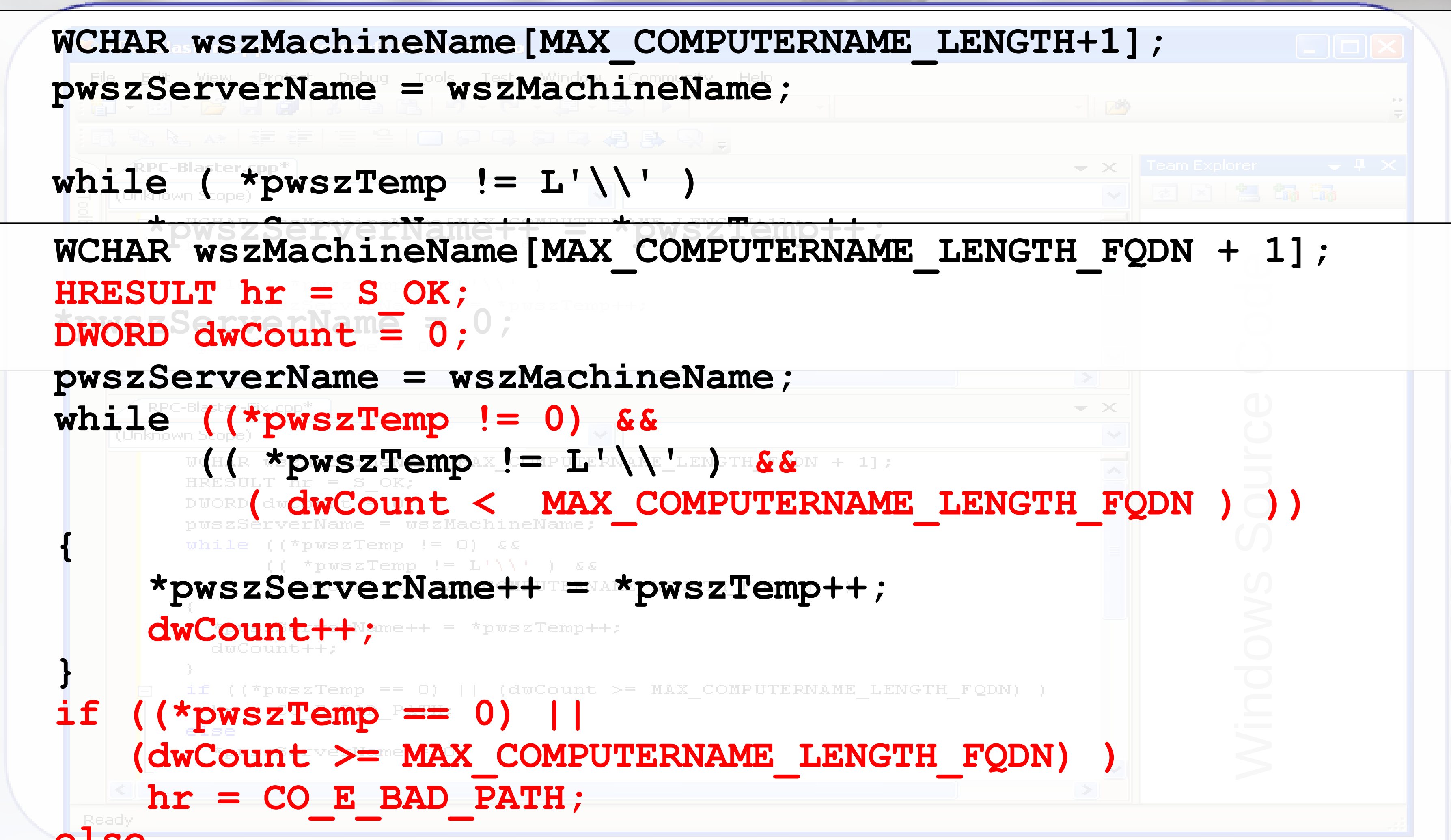
Cryptography

(e.g., Hashing, Encryption, Digital Signatures, Certificates)





Buffer Overflow: Blaster (MS03-026)

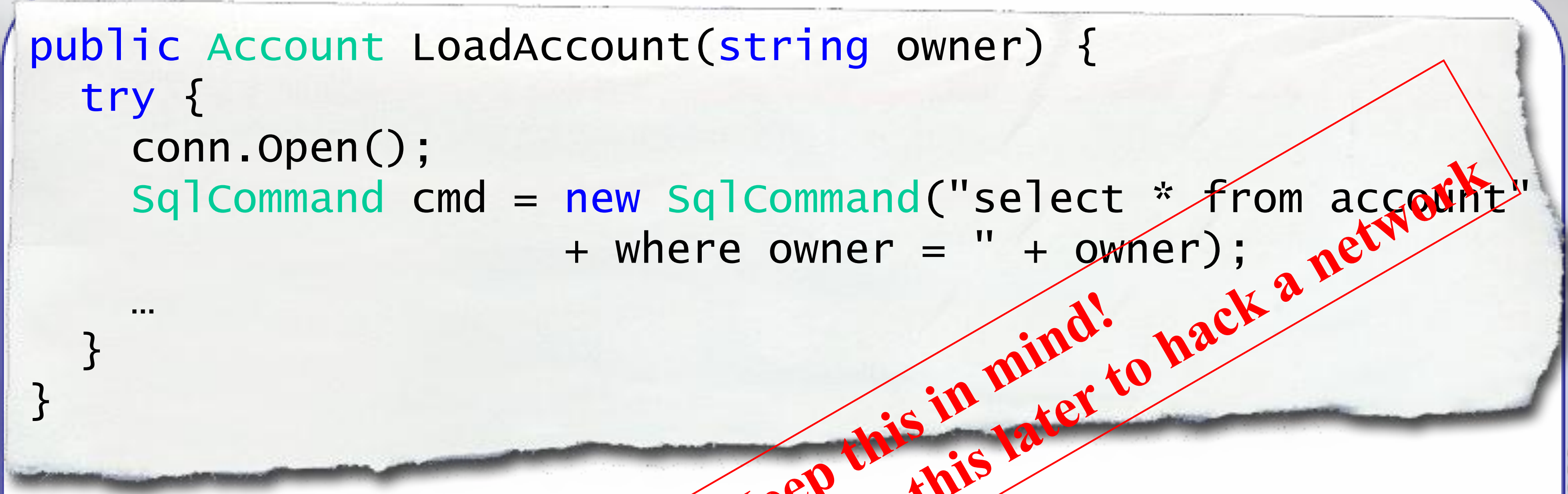


```
WCHAR wszMachineName[MAX_COMPUTERNAME_LENGTH+1];
pwszServerName = wszMachineName;

while ( *pwszTemp != L'\\' )
    *pwszServerName++ = *pwszTemp++;
*pwszServerName = 0;
```

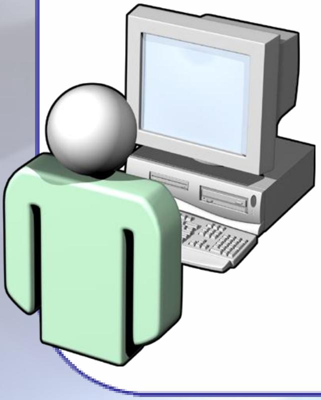
```
WCHAR wszMachineName[MAX_COMPUTERNAME_LENGTH_FQDN + 1];
HRESULT hr = S_OK;
DWORD dwCount = 0;
pwszServerName = wszMachineName;
while ((*pwszTemp != 0) &&
     (( *pwszTemp != L'\\' ) &&
       ( dwCount <  MAX_COMPUTERNAME_LENGTH_FQDN ) ))
{
    *pwszServerName++ = *pwszTemp++;
    dwCount++;
}
if ((*pwszTemp == 0) ||
   (dwCount >= MAX_COMPUTERNAME_LENGTH_FQDN) )
    hr = CO_E_BAD_PATH;
else
    *pwszServerName = 0;
```

SQL-Injection



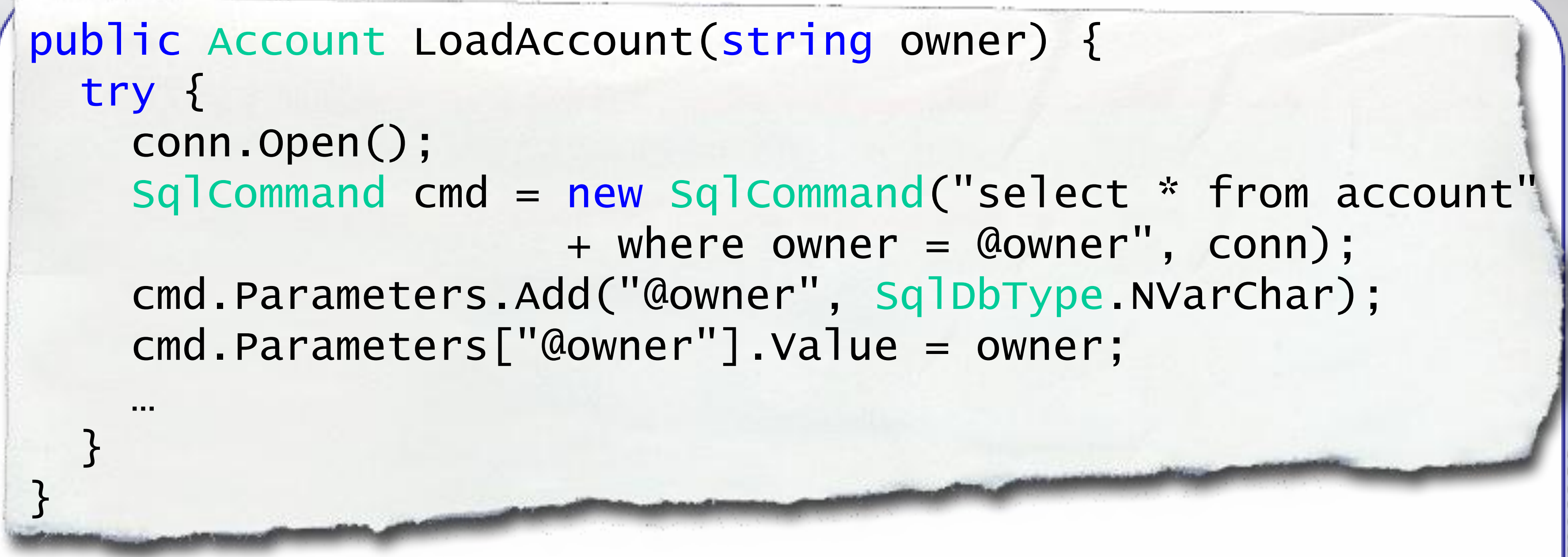
```
public Account LoadAccount(string owner) {
   try {
      conn.Open();
      SqlCommand cmd = new SqlCommand("select * from account"
                         + where owner = " + owner);
      …
   }
}
```

Keep this in mind!
I'll use this later to hack a network



owner: hansi.huber;
update set amount = 1000000 where accountId = *TheHackersAccID*

SQL-Injection



```
public Account LoadAccount(string owner) {
  try {
    conn.Open();
    SqlCommand cmd = new SqlCommand("select * from account"
                     + where owner = @owner", conn);
    cmd.Parameters.Add("@owner", SqlDbType.NVarChar);
    cmd.Parameters["@owner"].Value = owner;
    …
  }
}
```

owner: hansi.huber;
update set amount = 1000000 where accountId = *TheHackersAccID*

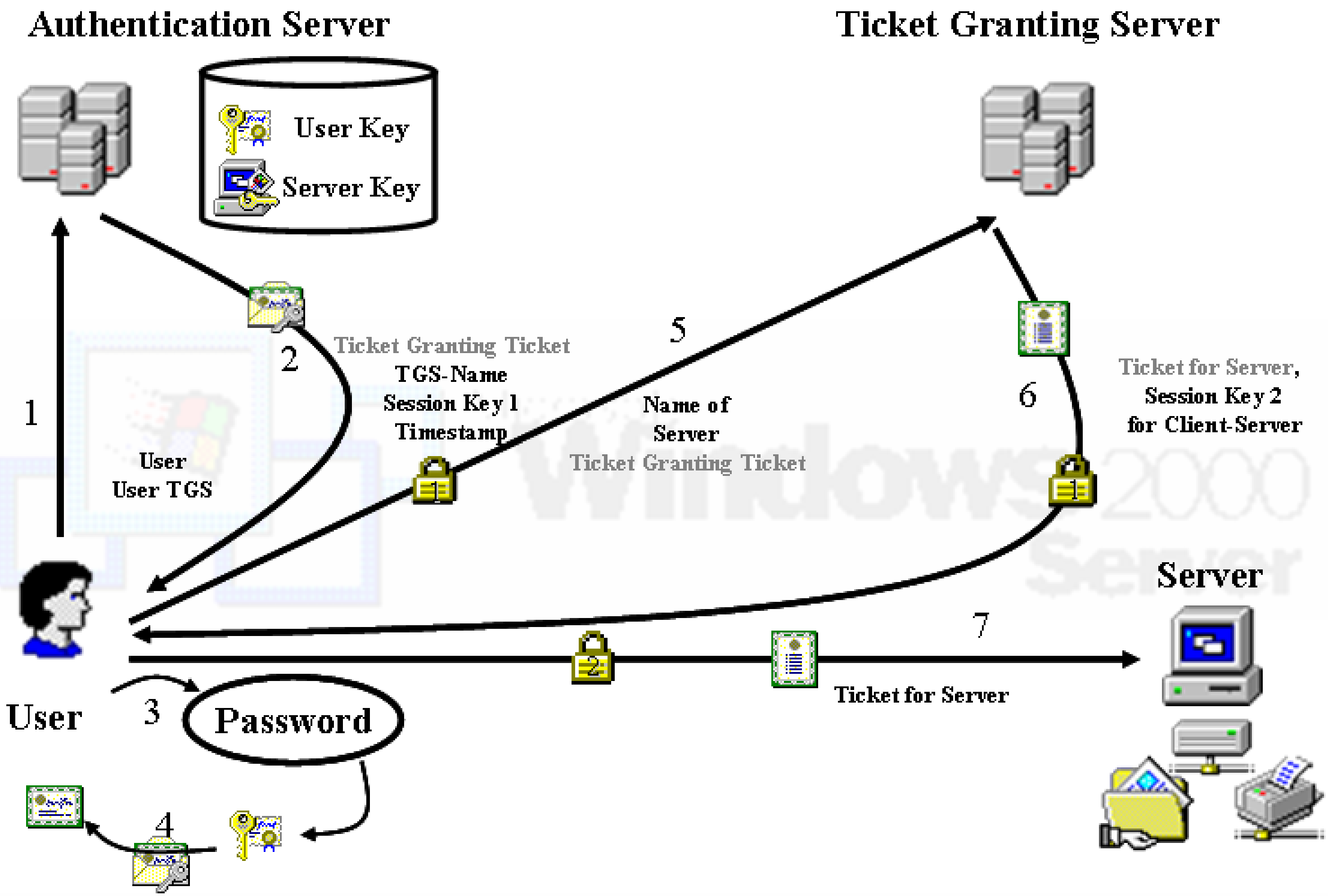
Network Analysis

- Sniffing
  - Ethernet is a Bus → each node gets the whole traffic
  - Node evaluates only messages that are directed to the node itself or to the complete network
  - Switches can be bypassed → ARP-Spoofing
  - Hacker monitors all traffic

Password-Analysis

- Transmission of Passwords
  - Plain text
    - Just monitor the traffic
  - Challenge-Response
    - Brute-Force Attacke
  - Distributed Authentication
    - Secure

Distributed Authentication



When do attacks occur?

Product release

Security hole found

Fix available

Fix installed

Conclusion

Threat	Counter Measure
Raiffeisen Certificate	User Training (Security Awareness)
Linux Boot	Organizational: Lock your office!
ARP-Spoofing	Use Encryption
Sniffer	Use Encryption
Trojan Horse	User Training (do not open attachments)
Virus	Up-to-date Anti-virus software
Attacks	Firewall
Passwords	Use strong mechanisms

The Stefan Probst‘s Horror Computer Show

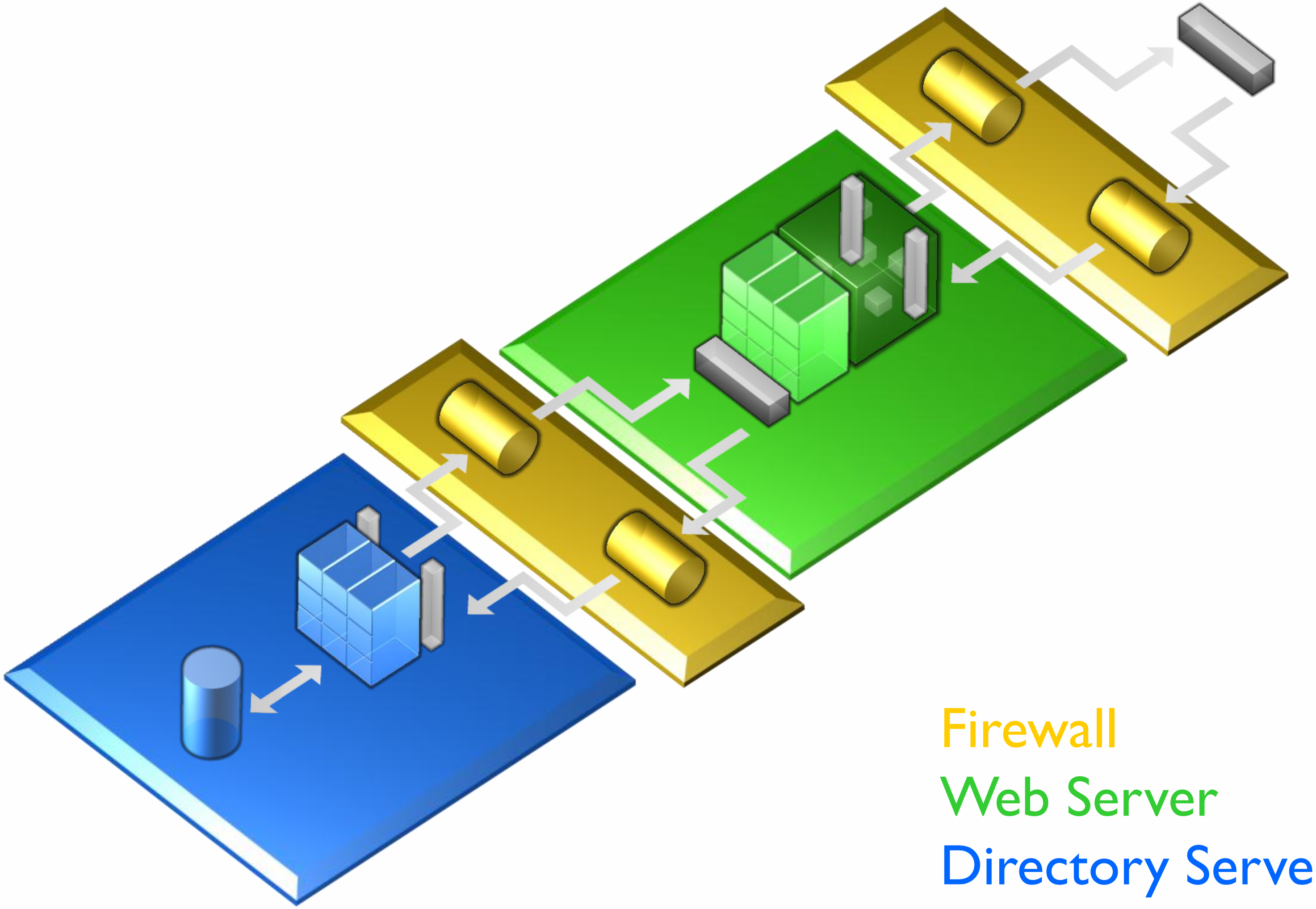
Before we start…

WARNING!

Hacking networks that you do not own is illegal and can be punished with jail!

Some tools that are presented in the following are custom made.
I will not give you my tools. It does not matter who you are or who you work for!

Common (good) Architecture

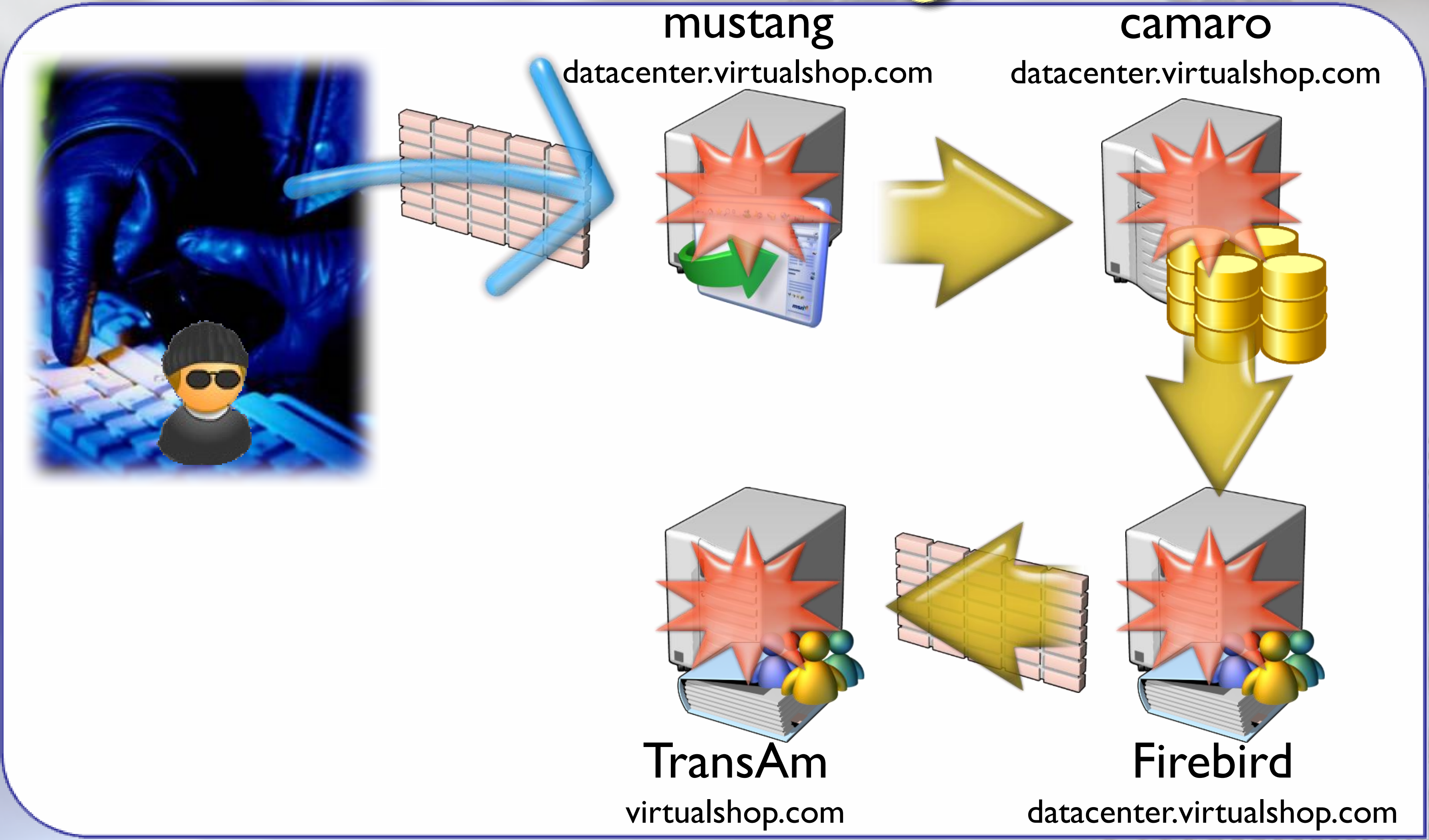


Firewall

Web Server

Directory Server

www.virtualshop.com



mustang
datacenter.virtualshop.com

camaro
datacenter.virtualshop.com

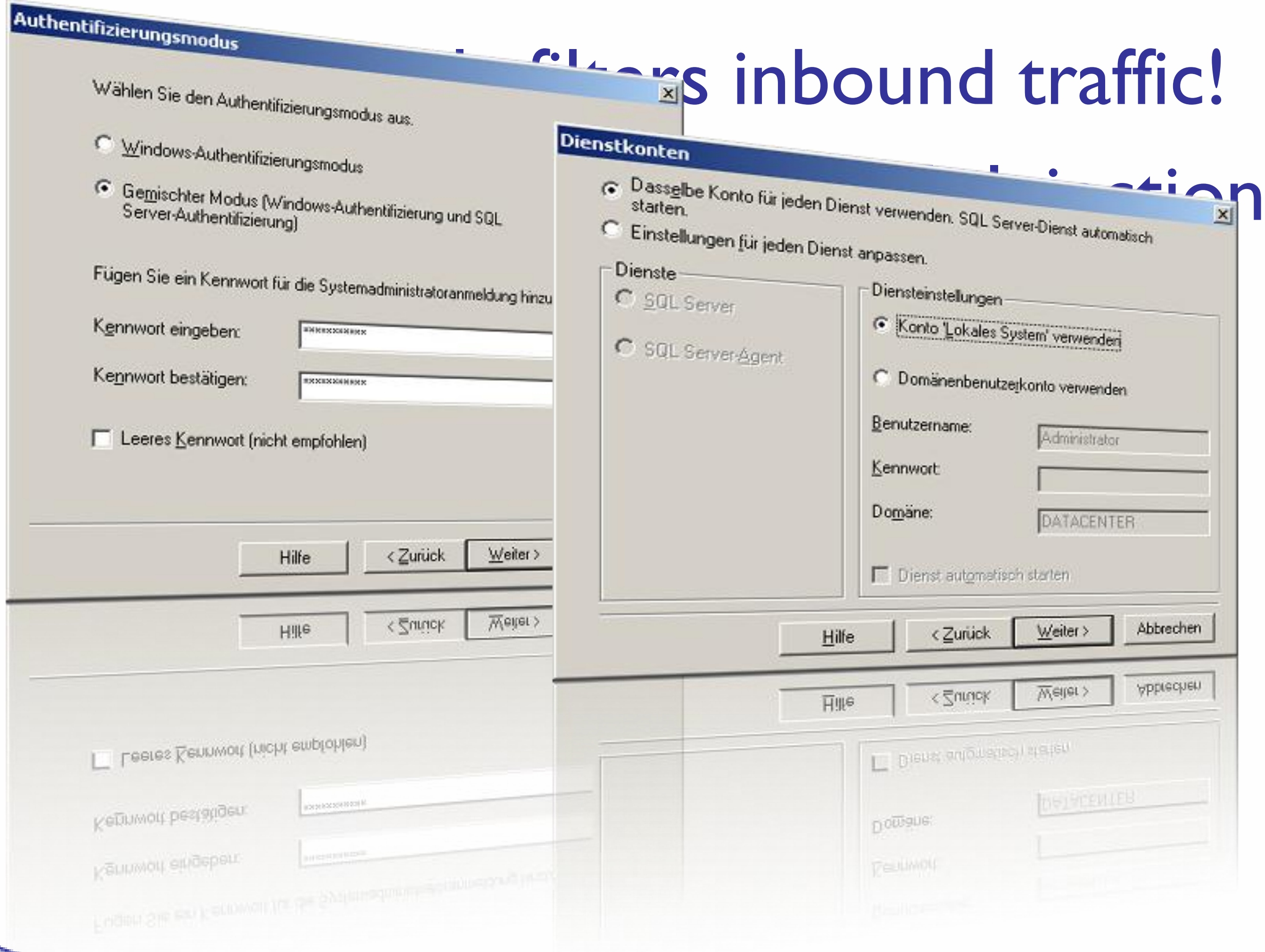
TransAm
virtualshop.com

Firebird
datacenter.virtualshop.com

What went wrong?

filters inbound traffic!

lication



Authentifizierungsmodus

Wählen Sie den Authentifizierungsmodus aus.

○ Windows-Authentifizierungsmodus

● Gemischter Modus (Windows-Authentifizierung und SQL Server-Authentifizierung)

Fügen Sie ein Kennwort für die Systemadministratoranmeldung hinzu

Kennwort eingeben: **********

Kennwort bestätigen: **********

□ Leeres Kennwort (nicht empfohlen)

Dienstkonten

● Dasselbe Konto für jeden Dienst verwenden. SQL Server-Dienst automatisch starten.

○ Einstellungen für jeden Dienst anpassen.

Dienste

○ SQL Server

○ SQL Server-Agent

Diensteinstellungen

● Konto 'Lokales System' verwenden

○ Domänenbenutzerkonto verwenden

Benutzername: Administrator

Kennwort:

Domäne: DATACENTER

□ Dienst automatisch starten

Fixing the Problem…

- Usage of SQL Parameters…
- Run database server with least privilege principle…
- Don’t connect to database as system administrator…
- Filter outbound connections…

The Moral of the Story

- Initial entry is everything
- Most networks are designed like egg shells
  - Hard and crunchy on the outside
  - Soft and chewy on the inside
- Once an attacker is inside the network, you can…
  - …update resume
  - …hope he does a good job running it
  - …drain it

How To Get Your Network Hacked in 10 Easy Steps

- Don’t patch anything
- Run unhardened applications
- Use one admin account, everywhere
- Open lots of holes in the firewall
- Allow unrestricted internal traffic
- Allow all outbound traffic
- Don’t harden servers
- Reuse your passwords
- Use high-level service accounts, in multiple places
- Assume everything is OK

10 Things Attackers Don’t Want You To Do

- Ensure everything is fully patched
- Use properly hardened applications
- Use least privilege
- Open only necessary holes in firewalls
- Restrict internal traffic
- Restrict outbound traffic
- Harden servers
- Use unique pass phrases or smart cards
- Micro-manage service accounts
- Maintain a healthy level of paranoia

thank you...

Security and Software Consulting