On the Gap between Network Security Research, Realization and Usage

Joachim Charzinski

EuroNGI Workshop Würzburg, Jul. 2007

Background

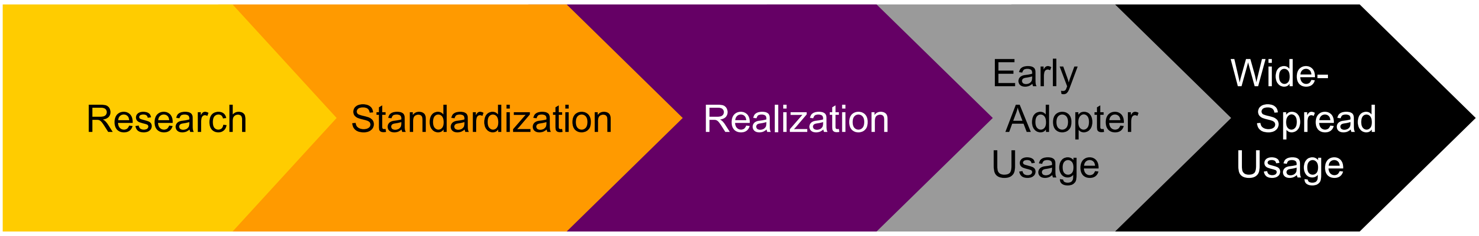
- This talk expresses my personal opinion
- This talk is for technically oriented researchers
  - to explain the gap between what is available and what is applied
- This talk is about normal people
  - the average employee
  - the average residential computer or communication user
- There are special people who do everything right
  - conservative network operators
  - security-conscious employees
  - security-conscious residentials

really?

Outline

- A Time line and some bar graphs
- Business
- Users
- Availability
- Networks

Time Line



Research

Standardization

Realization

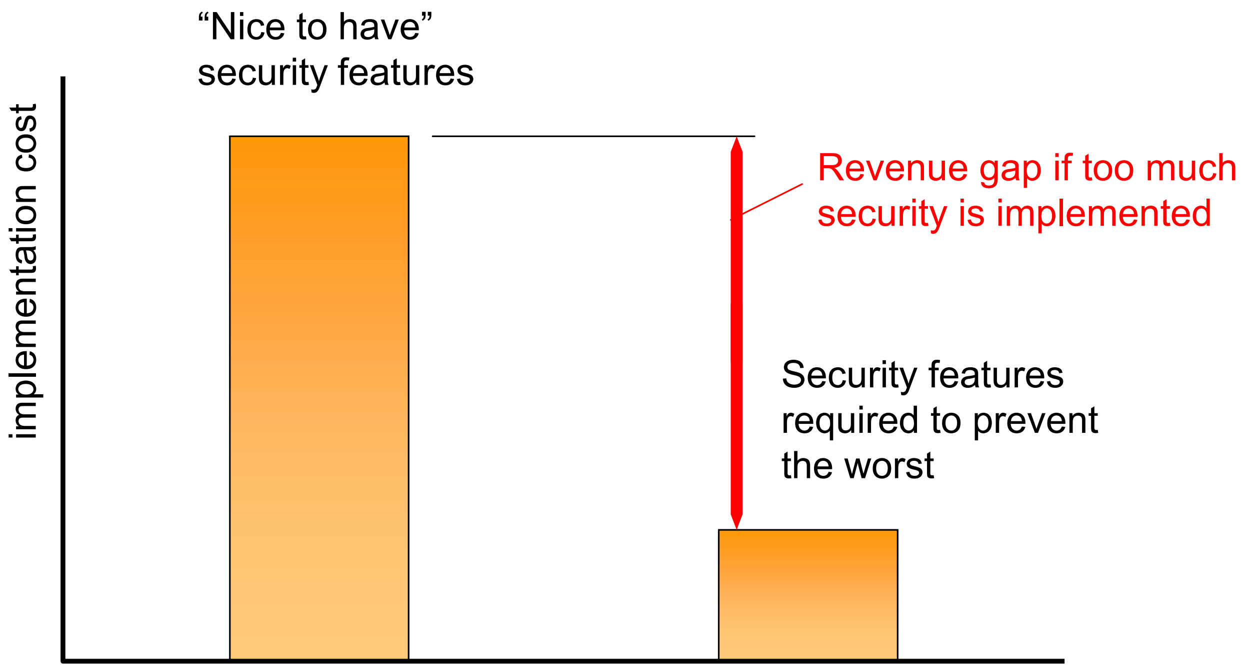
Early Adopter Usage

Wide-Spread Usage

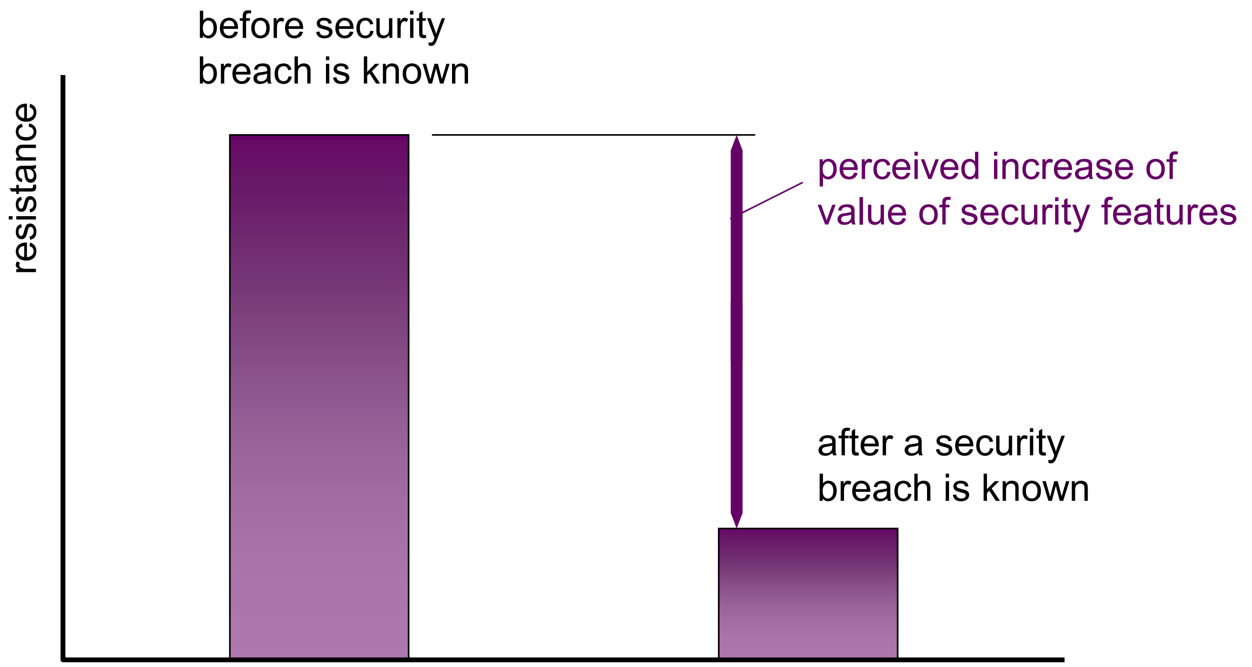
- Solutions are available from research for most security problems, ensuring confidentiality, integrity and non-repudiation
- Some of them are implemented
- Some are even used by early adopters
- Hardly any security feature has found wide spread usage

why?!

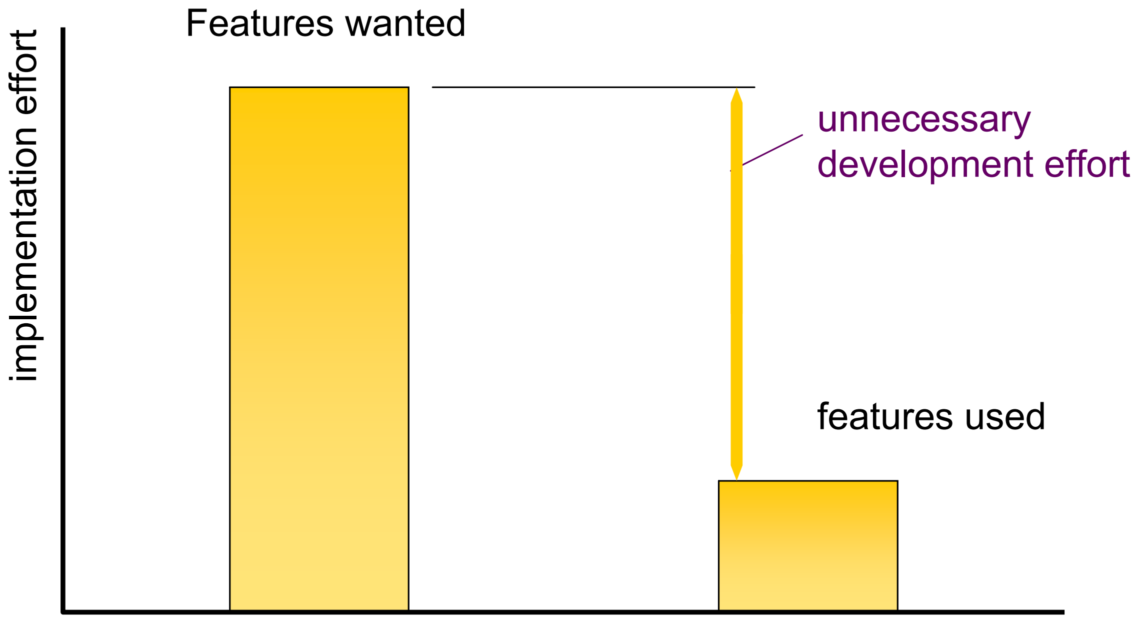
Essential Security Features



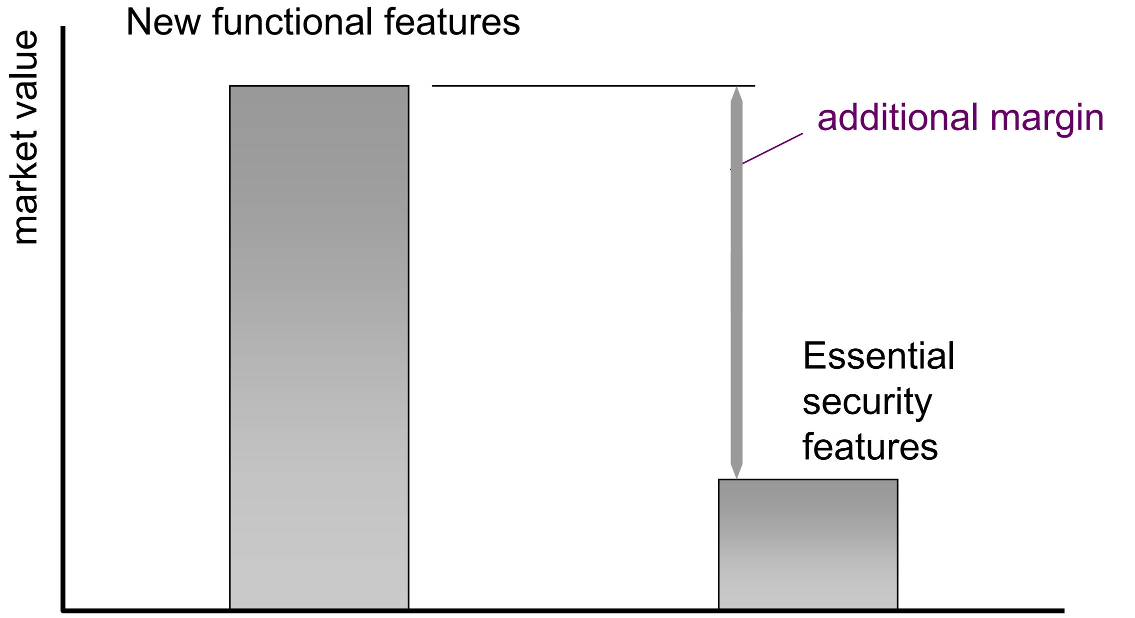
Resistance Against New Security Features



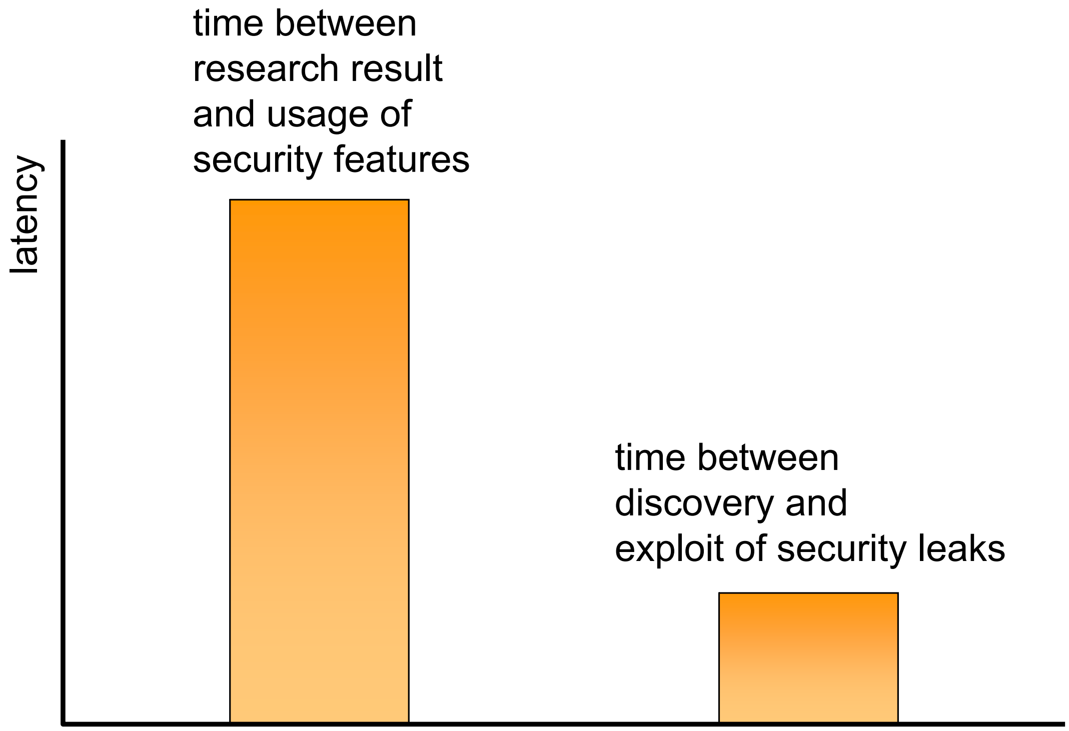
New Security Features



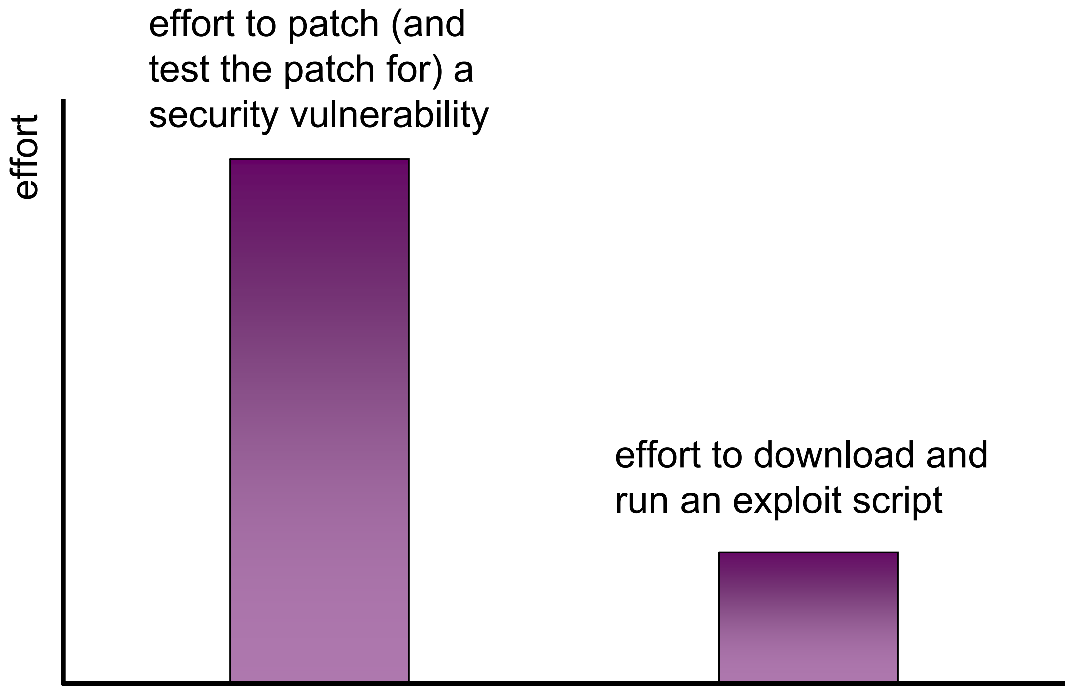
Security versus Functional Features



Security Timing



Vulnerability Patching and Exploitation



Two Kinds of Security Business

Preventing the Bad	**Enabling the Useful**
• ensure nothing bad happens • example: e-mail encryption	• new value add from security technology • example: smart cards • cost savings
• expensive • takes long to introduce • only minimal features realized • often not accepted by users	• fast break-even • takes the market or is being supported by interested parties

this is where the problems are

USERS and SSH Fingerprints

- State of the art ssh and TLS handling
  - compare fingerprint via second channel (phone or e-mail)

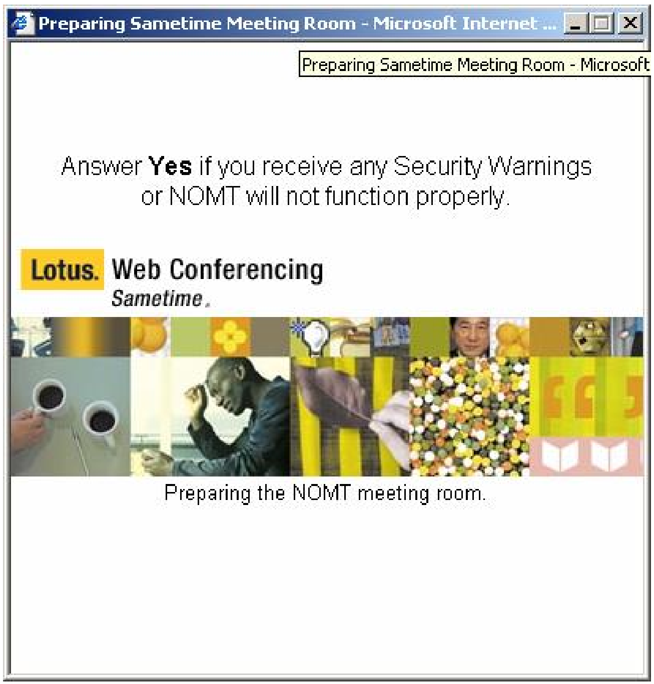
```
The authenticity of host '10.9.2.23 (10.9.2.23)' can't be established.
RSA1 key fingerprint is 29:3b:bf:d7:96:e9:69:3b:d1:99:bc:d2:68:97:4f:41.
Are you sure you want to continue connecting (yes/no)? yes
```

- Vulnerable to look-alike attack
  (humans are bad in doing precise bitwise comparison)
- Attack: generate host key that does not completely match the fingerprint
  - but is close enough for differences to be ignored by users

```
ffp -k rsa -t 29:3b:bf:d7:96:e9:69:3b:d1:99:bc:d2:68:97:4f:41
(checks 40k hashes/s on 800MHz Pentium III / Linux)
```

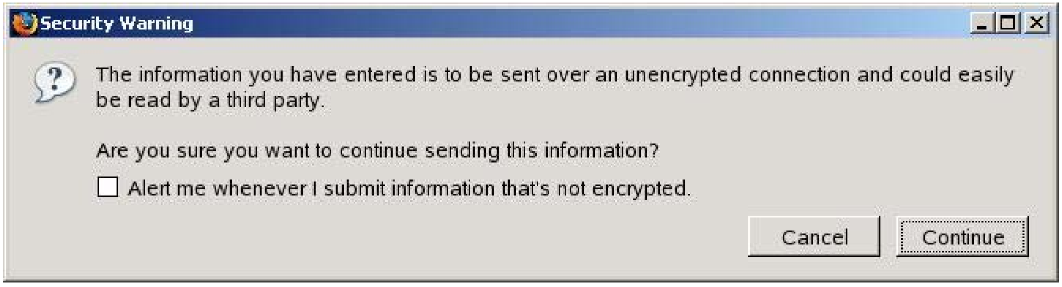
Users are Trained to Ignore Security Concerns

- Some services work only if security warnings are ignored
- Some Web sites do not care about updating server certificates for TLS
- Support personnel asking for passwords
- Risk comparison in security warnings is hard to do
  - unvalidated TLS certificates
  - unencrypted requests to google


Preparing Sametime Meeting Room - Microsoft Internet ...
Preparing Sametime Meeting Room - Microsoft
Lotus. Web Conferencing
Sametime.

Answer **Yes** if you receive any Security Warnings or NOMT will not function properly.

Preparing the NOMT meeting room.



The information you have entered is to be sent over an unencrypted connection and could easily be read by a third party.

Are you sure you want to continue sending this information?

□ Alert me whenever I submit information that's not encrypted.

Users Cannot be Trusted

- Nobody wants to be the bad guy
  - don't say "no", even to dubious requests
  - encryption is uncool
- People want to achieve a task
- People have a false sense of trust
  - if you warn them before, they will do everything
- People follow mass movements
  - everybody has a virus scanner
  - nobody encrypts their e-mails
- People have no idea about risks
  - bet on a <10^{-7} chance of winning a lottery
  - ignore a 10^{-1} chance of catching malware
- Users will
  - give away passwords or other soft credentials
  - prefer insecure communication over no communication
  - accept near-miss fingerprints

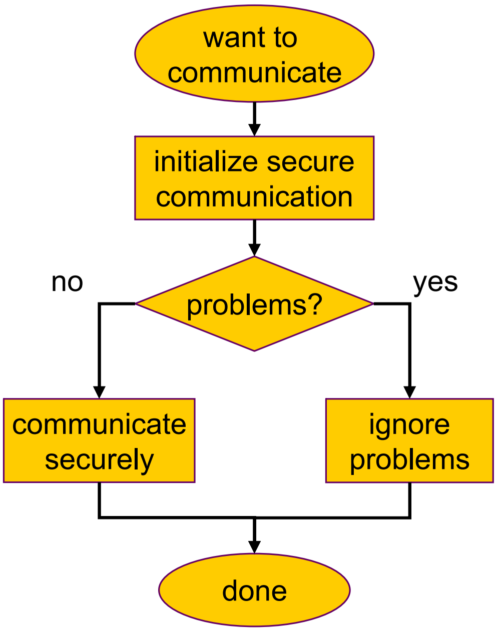
social engineering, phishing

user level bid-down attacks

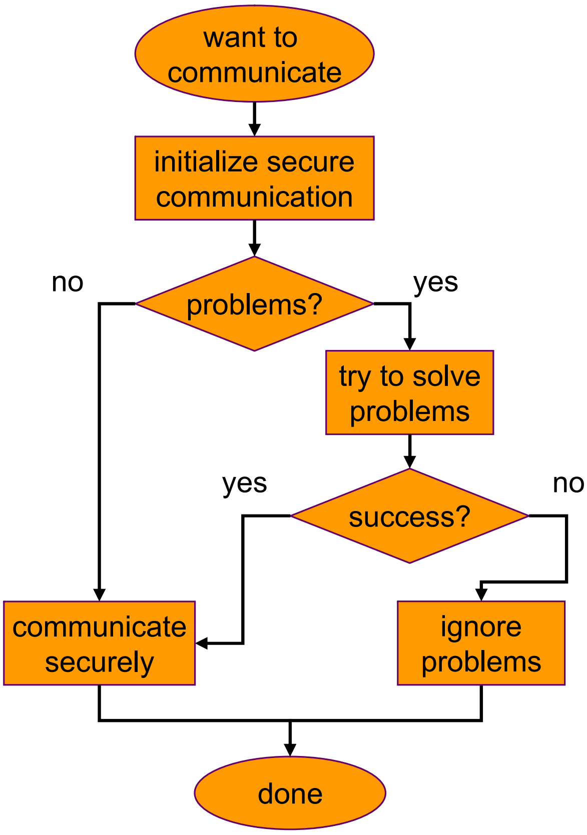
Users are highly vulnerable to bid-down attacks

- Users want to **communicate**!

Secure communcation model for normal users



Secure communcation model for security wizards



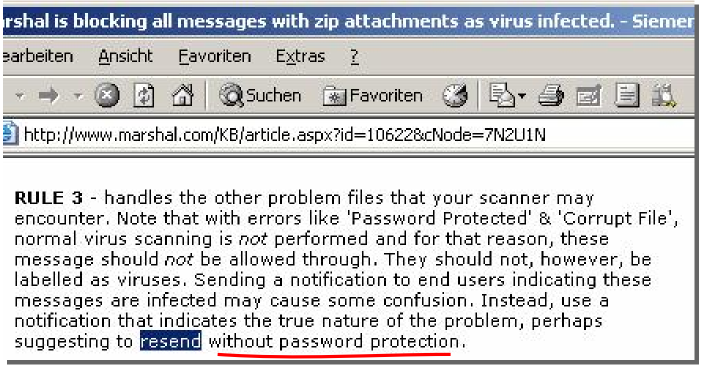
Availability

- User-level bid-down is supported by
  - lack of availability of security solution
  - hard-to use security solutions
  - lack of risk or mis-trained risk awareness
- Nobody dispenses with their communication needs only because the security solution does not work
  - default fall-back is to communicate insecurely
- This also holds for
  - outage of quantum cryptography links
  - outage of red telephones
  - incompatibility of S/MIME and PGP mail encryption
  - unavailability of key server (“could you please re-send without encryption”)

Fundamental Tradeoff between Network and End-System Security

- Firewalls
  - Tunneling through firewalls (everything is http nowadays)
  - DNS tunneling

- If PKI was available commonly:
  - encrypted viruses
  - virus scanner requires unencrypted mails
  - signed spam
  - encrypted spam


rshal is blocking all messages with zip attachments as virus infected. - Siemer
earbeiten Ansicht Favoriten Extras ?
Suchen
Favoriten
http://www.marshal.com/KB/article.aspx?id=10622&cNode=7N2U1N

RULE 3 - handles the other problem files that your scanner may encounter. Note that with errors like 'Password Protected' & 'Corrupt File', normal virus scanning is *not* performed and for that reason, these message should *not* be allowed through. They should not, however, be labelled as viruses. Sending a notification to end users indicating these messages are infected may cause some confusion. Instead, use a notification that indicates the true nature of the problem, perhaps suggesting to resend without password protection.

→ Tradeoff between system and communication security

Internet Threat Model

- Growth and utility of Internet services relies on being able to reach everybody everywhere
  - end system threats come from being able to reach everybody everywhere
- Internet worked well and rather securely when
  - it was a small, trusted community
  - it had village-like structures (you knew whose packets could come through a certain port)

- The Internet is a threat to end systems security.

- Network based security devices are a threat to the Internet’s openness and growth.

Fundamental Tradeoffs

- Security vs. usability
  - invisible security measures (like GSM SIM) are accepted
  - even smart card based encryption is too much hassle
- Education vs. scaring off users
  - many businesses live from uneducated users
- System security vs. communication security
  - virus scanning, malware detection ↔ e2e encryption
- Authentication vs. privacy
  - users want to browse information without being identified
  - sites want to trace back attacks to liable users
- Privacy vs. national security
- …

Research required

- Usability
- Suitable user interface and device metaphors
- Trust relations
- Identity Rights Management

Actions required

- Consider holistic usage scenarios already
  in research and standardization
- Implementation and roll-out of security functions
- User education
- Careful process integration