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 residents
Outline

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

Time Line

• 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
Essential Security Features

“Nice to have” security features

Revenue gap if too much security is implemented

Security features required to prevent the worst

Resistance Against New Security Features

before security breach is known

perceived increase of value of security features

after a security breach is known
New Security Features

Security versus Functional Features

New functional features

market value

Essential security features

additional margin

unnecessary development effort
Security Timing

- Time between research result and usage of security features
- Time between discovery and exploit of security leaks

Vulnerability Patching and Exploitation

- Effort to patch (and test the patch for) a security vulnerability
- Effort to download and run an exploit script
Two Kinds of Security Business

Preventing the Bad
- ensure nothing bad happens
- example: e-mail encryption
- expensive
- takes long to introduce
- only minimal features realized
- often not accepted by users

Enabling the Useful
- new value add from security technology
- example: smart cards
- cost savings
- 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.
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

(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

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
Users are highly vulnerable to bid-down attacks

- Users want to **communicate**!

  Secure communication model for normal users

  - want to communicate
  - initialize secure communication
  - problems?
    - yes: communicate securely
    - no: ignore problems
  - done

  Secure communication model for security wizards

  - want to communicate
  - initialize secure communication
  - problems?
    - yes: try to solve problems
    - no: ignore problems
  - success?
    - yes: communicate securely
    - no: ignore problems
  - done

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

→ 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