

Security and Usability, Psychology, Risk Analysis

Vašek Matyáš

PA018 –
Advanced Topics in IT Security

Social Engineering Attacks

- Pretexting: contacting somebody with a false pretext (context) in order to get unauthorized access
- Phishing: requesting auth. details or other sensitive info electronically

Vážený Beloved

Jsem Hakim Mrs.Mona od England.I hod. bezdětná vdova. Jsem vdaná za pozdní Engr. Sahad Hakim ... After smrti mého manžela, jsem se rozhodl, že se nepřipojím k re-manželství, nebo si dítě mimo moji manželského domova.

Bojoval jsem proti rakovině se 4 roky po jeho smrti, fibroidní problémy a poškození sluchu...

Useful psychology research

- Asymmetry computer vs. human (brain)
 - Decision science / behavioural economics
 - Mental processing – CAPTCHA
 - Passwords
- Trusted path
 - Delivery of information computer ↔ human
 - Trusted display issue
 - Trusted keyboard issue
 - Related issues of PIN delivery, initial key setting, etc.





Famous principles

- Segregation of duties
 - Four eyes (two person)
- Single point of failure
 - All eggs in one basket
- Need to know (compartmentalization)
- Secondary channel
 - Multifactor authentication
- Fail-deadly (vs. fail-safe)
- Trust, but verify

Shouldersurfing

- Issue investigated at FI MU w.r.t. PIN entry observation
- Open-space office issue
- Password entry “culture”
- Cameras as a big issue
- Acoustic emanations too

“Attacks” on SSL

- Man-in-the-middle as an evergreen
 - Build often on poor check of public-key certificates by users
 - ...or problems with inconsistent public-key certificate check by browsers or servers
 - ...or favorite icon display in the URL bar    
 - ...or abusing layers of indirection (HTTP to HTTPS)
- Public-key certificates overloaded – attribute certificates
- Issues beyond technology – adequate precautions, from both a legal and a personal view

Risk analysis

- Often rather risk assessment – less formal and rigorous process
- Quantitative vs. qualitative
- Quantitative
 - Easy to understand the results
 - Results usually in \$\$\$ (risk exposure)
- Qualitative
 - Discrete scale (not \$\$\$)
 - Easy to automate, not that easy to understand the results

Problems of quantitative risk analysis

- Unreliability and inaccuracy of the data used.
- Probability is hardly precise.
- Expectations based on data from the past can lead to ungrounded complacency.
- Countermeasures and controls can address some events that are inter-related.

Risk analysis – notes

- Information collection – questionnaires, interviews
- Control of completeness – formal checks, experience of the evaluator (!!!)
- Processing of inputs (semi-automated)
- Report with suggestions for risk reduction or even elimination

Incidents caused by

- Errors (not intended to happen): 50-70%
- Natural/utility influence: 10-15%
- Malicious software: 5-10%
- Intentional sabotage/attack/corruption by own/past employees/members: 10-20%
- External attackers: 1-5%

Impact of incidents is yet another issue!

Role of IT security manager

- Experience with IT security very important
- Art of persuasion critical!
- Experience: 60% management skills, 40% security expert skills
- Very demanding and challenging position
 - Criticized for incidents
 - Criticized for obstructions to “normal” processes
 - Can be appreciated for “nothing happening”? 😊

Security policy

- VERY IMPORTANT for improving the (IT) security in any company
- Company *business goals* → IT goals → IT security goals
- Helps with
 - Setting priorities (for IT, security departments)
 - Long-term goals vs. short-term goals
 - Improvement of services (vs.) company survival(!)
 - Getting management support and assuming direct responsibilities

Security policy and company culture

- The best security mechanisms are useless without effective support of all parties involved
- End-users must be trained and interested
- Management must be involved (or better lead!)
- Security is a process, not a product