User Interfaces and Security

Frank Kargl
frank.kargl@uni-ulm.de

Media Informatics Dep.
Ulm University

Why are user interfaces relevant to SEVECOM

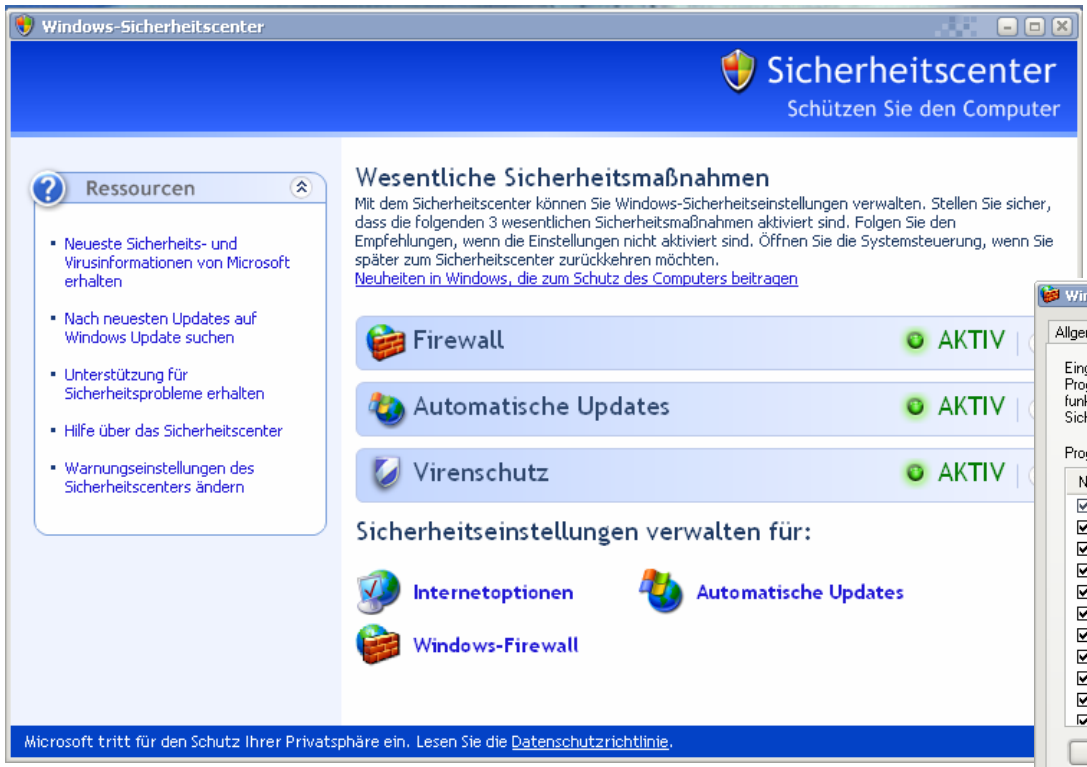
- Guideline:
  We want to prevent user interaction whenever possible
  - Interaction with security system while driving distracts driver unnecessarily
  - Drivers are no computer or security experts and will not understand the security issues anyway
- But:
  There may be cases when the system alone will not be able to work without user intervention or will only be able to make conservative decisions leading to DoS

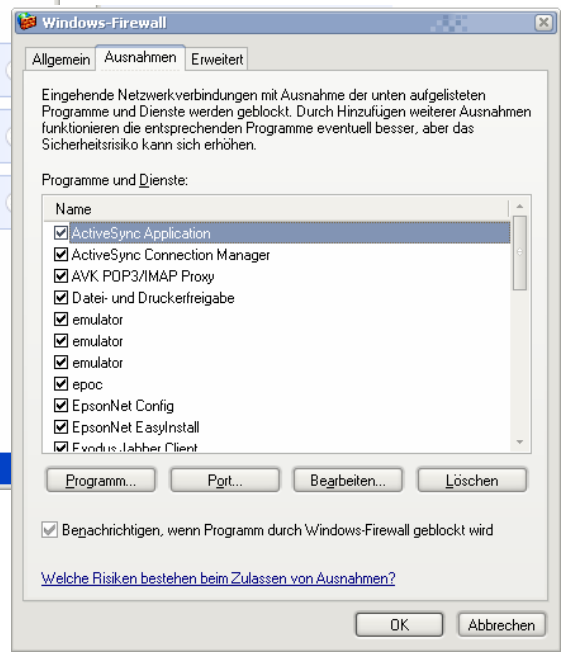
Examples from the PC world

- Authenticating to the system

Examples from the PC world

- Configuring security settings





Examples from the PC world

- Browsing the Internet

What might happen in vehicles

- “IDS determines that warning message come from a node that you trust only to 75.2%”
  - Display the warning or not?
  - How to display the warning?

What might happen in vehicles

- “Car receives C2C message with an expired or invalid certificate”
  - Display the message or not?
  - Ask the user to check the certificate?
  - How to display the message?

What might happen in vehicles

SEVECOM

- "You are about to send data that might compromise your privacy"
  - Ask the driver about a decision (while driving)?
    - Can this be realized in a safely manner?
    - When is a good time to interrupt the driver and how to do that?
  - Pre-configure your privacy requirements?
    - How to handle configuration dialogues?
  - Preset everything by the manufacturer/standard bodies, they know best about your privacy requirements!

What might happen in vehicles

SEVECOM

- “Your car or other car’s experience a malfunction in one of the systems, e.g. your car is sending bogus warning messages”
  - When and how to notify the driver about this?

Solution Guidelines

- Design unobtrusive interfaces
- Adaptive UI
  - Interact according to attention level of driver
  - Interact according to driving situations
  - Interact according to severity of event
- Delay interaction to a later time
  - Less risky driving situation
  - When arriving at destination

Examples for UI Design

- Warning messages with different trust levels

Severity: 50%
Trust: 70%

Foto: BMW

Severity: 95%
Trust: 100%

Related Work

SEVECOM

- Mostly (only?) focused on Desktop GUIs
- Lorrie Cranor, Simson Garfinkel:
  Security and Usability: Designing Secure Systems That People Can Use, O'Reilly, 2005
- Ka Ping Ye:
  User Interaction for Secure Systems,
  ICICS 2002, Singapore
  - http://www.sims.berkeley.edu/~ping/sid/
  - http://usablesecurity.com/
- Work on design of car cockpits?

Ten Design Principles

SEVECOM

1. **Path of Least Resistance**
   - Match the most comfortable way to do tasks with the least granting of authority.
2. **Active Authorization**
   - Grant authority to others in accordance with user actions indicating consent.
3. **Revocability**
   - Offer the user ways to reduce others' authority to access the user's resources.
4. **Visibility**
   - Maintain accurate awareness of others' authority as relevant to user decisions.
5. **Self-Awareness**
   - Maintain accurate awareness of the user's own authority to access resources.
6. **Trusted Path**
   - Protect the user's channels to agents that manipulate authority on the user's behalf.
7. **Expressiveness**
   - Enable the user to express safe security policies in terms that fit the user's task.
8. **Relevant Boundaries**
   - Draw distinctions among objects and actions along boundaries relevant to the task.
9. **Identifiability**
   - Present objects and actions using distinguishable, truthful appearances.
10. **Foresight**
    - Indicate clearly the consequences of decisions that the user is expected to make.

[Ka Ping Ye: User Interaction for Secure Systems, ICICS 2002, Singapore]

Conclusions for SEVECOM II

1. Clear idea of applications and security system
2. Background on car cockpit design
3. Design Interaction
4. Build prototype!
5. Run user trials