



## User Interfaces and Security

---

Frank Kargl  
frank.kargl@uni-ulm.de

Ulm University



- **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



- Authenticating to the system



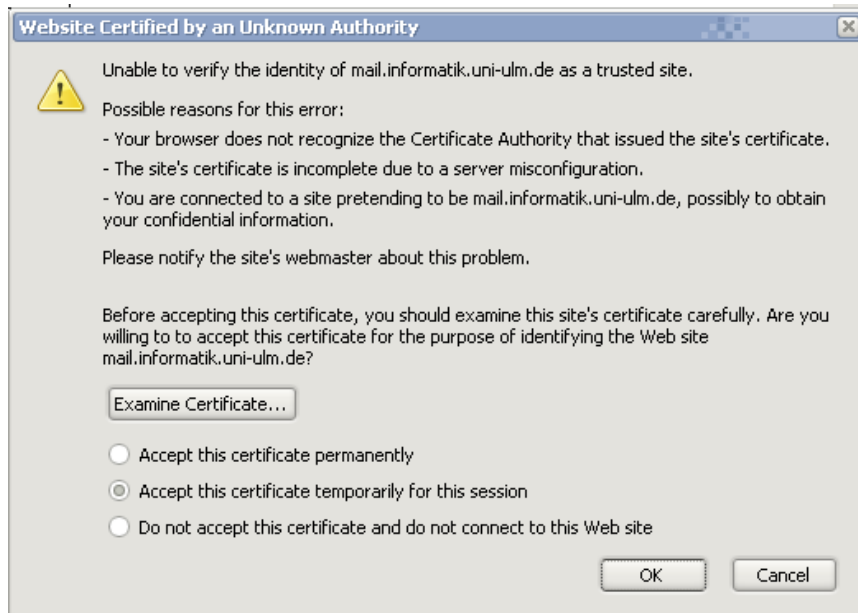


## ■ Configuring security settings

The image shows two overlapping windows from the Windows operating system. The background window is the 'Windows-Sicherheitscenter' (Windows Security Center). It features a blue header with the 'Sicherheitscenter' logo and the text 'Schützen Sie den Computer'. Below the header, there is a 'Ressourcen' (Resources) sidebar on the left with a list of links. The main area is titled 'Wesentliche Sicherheitsmaßnahmen' (Essential Security Measures) and lists three active settings: 'Firewall', 'Automatische Updates', and 'Virenschutz', each with a green 'AKTIV' indicator. Below this, there are links to manage settings for 'Internetoptionen', 'Automatische Updates', and 'Windows-Firewall'. A footer note states: 'Microsoft tritt für den Schutz Ihrer Privatsphäre ein. Lesen Sie die [Datenschutzrichtlinie](#).' The foreground window is the 'Windows-Firewall' control panel. It has tabs for 'Allgemein', 'Ausnahmen', and 'Erweitert'. The 'Allgemein' tab is selected, showing a warning about incoming network connections and a list of programs and services with checkboxes. The list includes 'ActiveSync Application', 'ActiveSync Connection Manager', 'AVK POP3/IMAP Proxy', 'Datei- und Druckerfreigabe', three 'emulator' entries, 'epoc', 'EpsonNet Config', 'EpsonNet EasyInstall', and 'Fondus-Labher Client'. At the bottom, there are buttons for 'Programm...', 'Port...', 'Bearbeiten...', and 'Löschen', along with a checkbox for 'Benachrichtigen, wenn Programm durch Windows-Firewall geblockt wird' and 'OK'/'Abbrechen' buttons.



## ■ Browsing the Internet





# What might happen in vehicles *SEVECOM*

- “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 *SEVECOM*

- “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?



- “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!





- “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?



- 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



- Warning messages with different trust levels

Severity: 50%  
Trust: 70%

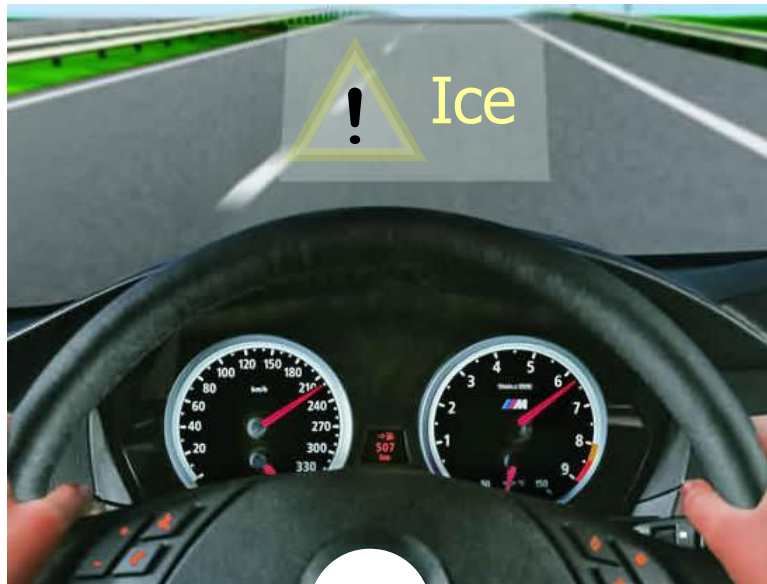


Foto: BMW

Severity: 95%  
Trust: 100%





- 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/>
- AIDE Project



# Ten Design Principles

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]



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