Secure Vehicle Communication



1

User Interfaces and Security

Frank Kargl frank.kargl@uni-ulm.de

Ulm University



Why are user interfaces relevant to **SEVEC**

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

		Microso	ft-	vn	
			ndow essional	S~P	
Copyright © 198 Microsoft Corpora			erere new new		Microso
	_				1
<u>U</u> ser name:					-
<u>U</u> ser name: <u>P</u> assword:	1				-
-	AD				[

SEVEC

Examples from the PC world



Windows-Sicherheitscenter				
	: 🔫	Sicherheitscente Schützen Sie den Comput		
2 Ressourcen	Wesentliche Sicherheitsmaßnahmen			
Neueste Sicherheits- und Virusinformationen von Microsoft erhalten	Mit dem Sicherheitscenter können Sie Windows-Sicherheitseir dass die folgenden 3 wesentlichen Sicherheitsmaßnahmen ak Empfehlungen, wenn die Einstellungen nicht aktiviert sind. Öl später zum Sicherheitscenter zurückkehren möchten. Neuheiten in Windows, die zum Schutz des Computers beitra	tiviert sind. Folgen Sie den ifnen Sie die Systemsteuerung, wenn		
 Nach neuesten Updates auf Windows Update suchen 	😝 Firewall	O AKTIV	Allgemein Ausnahmen Erweitert	
 Unterstützung für Sicherheitsprobleme erhalten Hilfe über das Sicherheitscenter 	🍓 Automatische Updates	O AKTIV (Eingehende Netzwerk verbindungen mit Ausnahme der unten aufgelisteten Programme und Dienste werden geblockt. Durch Hinzufügen weiterer Ausnahmen funktionieren die entsprechenden Programme eventuell besser, aber das Sicherheitsrisiko kann sich erhöhen.	
Warnungseinstellungen des Sicherheitscenters ändern	😺 Virenschutz	O AKTIV (Programme und Dienste:	
	Sicherheitseinstellungen verwalten	für:	ActiveSync Application ActiveSync Connection Manager ActiveSync Connection Manager AVK POP3/IMAP Proxy	
	🤣 Internetoptionen 🛛 👋 Automat	 ✓ Datei- und Druckerfreigabe ✓ emulator ✓ emulator 		
	indows-Firewall Windows-Firewall		 ✓ emulator ✓ epoc ✓ EpsonNet Config 	
crosoft tritt für den Schutz Ihrer Priva	stsphäre ein. Lesen Sie die <u>Datenschutzrichtlinie</u> .		EpsonNet EasyInstall Frodus: Jahber Client Programm Port Bearbeiten Löschen	
			✓ Benachrichtigen, wenn Programm durch Windows-Firewall geblockt wird	
			Welche Risiken bestehen beim Zulassen von Ausnahmen?	
			OK Abbrechen	

SEVEC

Examples from the PC world

SEVECOM

Browsing the Internet

Website	Certified by an Unknown Authority	ງ
Website	Certified by an Unknown Authority Unable to verify the identity of mail.informatik.uni-ulm.de as a trusted site. Possible reasons for this error: - Your browser does not recognize the Certificate Authority that issued the site's certificate The site's certificate is incomplete due to a server misconfiguration You are connected to a site pretending to be mail.informatik.uni-ulm.de, possibly to obtain your confidential information. Please notify the site's webmaster about this problem.	J
	Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site mail.informatik.uni-ulm.de? Examine Certificate Accept this certificate permanently Accept this certificate temporarily for this session Do not accept this certificate and do not connect to this Web site	
	OK Cancel	

Certificate Viewer:"mail.informatik.uni-ulm.de"

X

General Details

Could not verify this certificate for unknown reasons.

Issued To

Common Name (CN) mail.informatik.uni-ulm.de Organization (O) Organizational Unit (OU) URG Serial Number 00

University of Ulm, Computer Science Faculty

Issued By

mail.informatik.uni-ulm.de Common Name (CN) Organization (O) University of Ulm, Computer Science Faculty Organizational Unit (OU) URG

Validity

Issued On 16.09.2001 Expires On 14.09.2011

Fingerprints

SHA1 Fingerprint MD5 Fingerprint

A1:E2:1F:94:FE:41:F8:43:62:71:5F:67:FC:FC:2A:1E:E3:8D:06:C1
0B:F2:4A:48:87:B6:24:5D:B6:8F:E1:66:93:47:B1:2F

Close

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 **SEVEC**

- "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%



Severity: 95% Trust: 100%



Foto: BMW

SEVECOM

Related Work



- 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



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

SEVEL