LFE Medieninformatik • Max-Emanuel Maurer
Oberseminar - Abschlussvortrag Diplomarbeit

SeCuUI - Secure and Fast Data Submission to Public Terminals Using an Autocomplete Mechanism

Responsible Professor: Prof. Dr. Heinrich Hußmann
Supervisor: Dipl. Medieninf. Alexander De Luca
Start: February 01 2009
End: June 30 2009

7. Juli 2009
Overview

- Goals
- Related Work
- Explanation of SeCuUI
  - XUL
  - Autocomplete Function
  - Connection methods
- User study
- Conclusion

Source: sxc.hu
Goals

- Develop a system using mobile devices for terminal input
  - Client development
  - Not one specific server, but a framework
- Optimize the client and framework usage
  - External GUI information (XUL)
  - Faster input using autocomplete mechanism
  - Modularity throughout the system
    - Connection methods
    - Connection types
Related Work

- Either macroscopic / microscopic
  - Password entry alternatives
  - Remote control systems
- Missing happy medium
- 3rd group of biometric approaches
Related Work (Microscopic)

- Black and White PIN Pad
  - Roth et al. (2004)
- Spy-Resistant Keyboard
  - Tan et al. (2005)
- Convex hull password
  - Sobrado & Birget (2006)
Related Work (Macroscopic)

- Secure Mobile Computing
  - Sharp et al. (2004)
- Other more general approaches

Source: Sharp et al. 2004
Related Work (Biometrics)

• Biometric Verification at the ATM interface
  – Coventry et al. (2003)
• Already used in some areas
  – DVD rental

Source: Lenovo.com
SeCuUI - Secure Custom User Interface

- Entering data to public terminals using the own mobile device
  - Smaller screen
  - Closer proximity
  - Can not altered by someone else
  - Distributed risk
- Public terminal changes based on connection state
- Usage of a mobile device is not obligatory
SeCuUI - Secure Custom User Interface

XML-XUL-GUI

Device-Specific Synchronisation

Different Methods:
- QR-Code Connection
- SyncTap Connection
- Bluetooth / Socket

Encrypted / Unencrypted

Auto-Complete Values

XML:
```xml
<?xml version="1.0" encoding="UTF-8"?>
<xml>
  <userInterface>
    <subelement1/>
    <subelement2/>
  </userInterface>
</xml>
```
SeCuUI - User Perspective

- User has to perform only three simple steps
- One client software for all framework conform terminals
- Autocomplete values used for all applications
SeCuUI - Secure Custom User Interface

XML-XUL-GUI

Device-Specific Synchronisation

Different Methods:
- QR-Code Connection
- SyncTap Connection
- Bluetooth / Socket
  - Encrypted / Unencrypted

Auto-Complete Values

XML:
```xml
<?xml version="1.0"?>
<xul>
  <userInterface>
    <subelement1/>
    <subelement2/>
  </userInterface>
  <userInterface>
    <Another element/>
    </answer>
</answer>
<!-- Note: We need to add more elements later. -->
</xul>
```
XML-GUI

- Autonomous server application
- Transferable GUI parts not “hard coded”
- Framework parses external XML-File
  - Returns GUI container
  - Handles and synchronizes components
  - Programmer has direct access but does not need to care about connected devices
- XUL (XML User Interfaces) used as a container format
XUL (XML User Interface Language)

- Created by Mozilla
- Very powerful but only some part used for SeCuUI
- Additional attributes for SeCuUI

```xml
<?xml version="1.0"?>
<window id="findfile-window"
    title="Find Files"
    orient="horizontal"
    xmlns="http://www.mozilla.org/keymaster/gatekeeper/there.is.only.xul">

  <label id="lblAccountValue"/>

  <textbox
      id="tfInput"
      value="Eingabetext"/>

  <button id="btnNext" label="Next"/>

</window>
```
XUL (SeCuUI attributes)

- **asterisk**: Used to replace contents with echo characters (Possible values: ASTERISK_NEVER, ASTERISK_LOCAL, ASTERISK_OPTIONAL, ASTERISK_BOTH)
- **security**: Used to force input on the mobile device (Possible values: SECURITY_INSECURE, SECURITY_BOTH, SECURITY_SECURE_OPTIONAL, SECURITY_SECURE_FORCED)
- **dataType**: Used to define the type of data for this field (e.g.: TYPE_VISA_CARD_NUMBER, TYPE_ADDRESS)
SeCuUI - Secure Custom User Interface

XML-XUL-GUI

Device-Specific Synchronisation

Auto-Complete Values

Different Methods:
- QR-Code Connection
- SyncTap Connection
- Bluetooth / Socket
- Encrypted / Unencrypted

XML

<?xml version="1.0"?>
<xml>
  <userInterface>
    <subelement1/>
    <subelement2/>
  </userInterface>
  <userInterface>
    Another element
  </userInterface>
</xml>

Juli 2009
LFE Medieninformatik

Max Maurer
Autocomplete mechanism

- **dataType** attribute is processed
- all matching entries that have been previously entered are displayed beneath the corresponding input field
- no direct access for any server application
- possibility to disable autocomplete
- saving of new values on submit of a form
SeCuUI - Secure Custom User Interface

XML-XUL-GUI → Device-Specific Synchronisation → Auto-Complete Values

Different Methods:
- QR-Code Connection
- SyncTap Connection
- Bluetooth / Socket
  - Encrypted / Unencrypted
Modularity

- Connection process is very modular
- Module stack
- Three layers:
  - connection method
  - connection type
  - connection medium
- Connection independent message stack is used after connecting
- Protocol classes use simple MessageTransmitter

<table>
<thead>
<tr>
<th>Secure Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionManager</td>
</tr>
<tr>
<td><strong>ConnectionMethod</strong></td>
</tr>
<tr>
<td>QrCodeConnection</td>
</tr>
<tr>
<td>SyncTapConnection</td>
</tr>
<tr>
<td><strong>Connection</strong></td>
</tr>
<tr>
<td>NormalConnection</td>
</tr>
<tr>
<td>SecureConnection</td>
</tr>
<tr>
<td><strong>ServerConnection</strong></td>
</tr>
<tr>
<td>BluetoothServerConnection</td>
</tr>
<tr>
<td>SocketServerConnection</td>
</tr>
<tr>
<td><strong>ClientConnection</strong></td>
</tr>
<tr>
<td>BluetoothClientConnection</td>
</tr>
<tr>
<td>SocketClientConnection</td>
</tr>
</tbody>
</table>
Connection Manager

![Connection Manager Window]

Please select a connection method

SyncTap!!

Cancel
QrCodeConnection

- One completely implemented connection method
- Many different methods can be imagined
Userstudy

- Userstudy with client and test server was conducted
- 21 participants
- Scenario: Buy a product out of three different products and enter personal data
  - Shipping address
  - Payment details
- Two fake companies to demonstrate the portability
Userstudy - Variables

- Two independent variables
  - Autocomplete: On/Off
  - Number of values entered on the phone
    - Security related only
    - All values
- Fifth reference task: No phone connection at all
- Questionnaire at the end of the study
Userstudy - Setup

- MacBook served as Public Terminal
- Nokia N80 as mobile device
- Users could practice as long as they wanted to
- Issues noticed during test:
  - No real public terminal
  - Sitting instead of standing
  - Computer keyboard much faster
Userstudy - Vending machine usage

- People tend to use machines very often
- 62% are worried about their security at such machines
- Using a machine or ordering at a counter depends on the situation for most of them
- Security was also the highest rated non-functional requirement
Userstudy - Task results

Without mobile device:

<table>
<thead>
<tr>
<th>Task</th>
<th>Average connection</th>
<th>Average overall</th>
<th>Task 1 ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1</td>
<td>0</td>
<td>76</td>
<td></td>
</tr>
<tr>
<td>Task 2</td>
<td>28</td>
<td>238</td>
<td>3.3</td>
</tr>
<tr>
<td>Task 3</td>
<td>27</td>
<td>178</td>
<td>2.4</td>
</tr>
<tr>
<td>Task 4</td>
<td>35</td>
<td>129</td>
<td>1.8</td>
</tr>
<tr>
<td>Task 5</td>
<td>29</td>
<td>163</td>
<td>2.3</td>
</tr>
</tbody>
</table>

With mobile device:

- Number of Values: All 3
- Task 2: Off
- Task 3: Off
- Task 4: On
- Task 5: On

Auto-complete function

Average connection time: 29.74 seconds
Userstudy - Task interpretation

- Task 1 fastest
  - Probably due to laptop usage
- But task 4 significantly faster than task 2
  - Autocomplete speeds up data entry
- Participants had a different feeling
Userstudy - Task interpretation

Graphs showing the speed and simplicity of tasks 1 to 5.

- **Speed**
  - Task 1: Highest speed
  - Task 2: Lowest speed
  - Tasks 3, 4, and 5 are in between

- **Simplicity**
  - Task 1: Highest simplicity
  - Task 2: Lower simplicity than Task 1
  - Tasks 3, 4, and 5 are in between
Conclusion

- People are aware of security risks at public terminals
- Still PINs at ATMs as in 1967
- SeCuUI is a new approach between macroscopic and microscopic ideas
- Autocomplete feature increases the input speed whilst still more secure
Thank you!