User Authentication Methods for Mobile Systems

Dr Steven Furnell
Network Research Group
University of Plymouth
United Kingdom
Overview

- The rise of mobility and the need for user authentication
- A survey of mobile phone subscribers
- Advanced authentication options
- An experimental example
- Conclusions
Introduction

- Substantial growth of mobile devices
  - e.g. mobile phones - 768m in 2001 to 1,848m in 2004
- Increasing device functionality
  - e.g. convergence of PDA and phone devices
- Mobile devices contain an increasing amount of sensitive information
- What protects these devices from attack?
Introduction

- Mobile devices are already prime targets for theft
- Advanced capabilities of new devices will make them even more desirable
- Increased bandwidth and wireless connectivity will facilitate new services
- Expansion of services and private data will require increased level of protection
Background

Network Research Group
- Postgraduate and postdoctoral research
- 13 current PhD projects
- Significant focus in IT security

Links to Orange in a number of projects
- Including two sponsored PhDs relating to authentication for mobile devices
The need for Authentication

- Expansion of services will lead to storage of more sensitive information:
  - full contact details of family and associates
  - financial details enabling mobile electronic commerce transactions
  - commercially sensitive miscellaneous information (e.g. scheduler/notepad files)
  - medical records
- PLUS potential for remote access into corporate systems
Making Headlines

“Huge surge in mobile phone thefts”
BBC News (Jan 2002)

“MoD ‘loses 600 laptops’”
BBC News (Jan 2002)

“Laptop theft causing global havoc”
ZDNet News (Aug 2001)

“Worm turns on Wireless”
Wired News (June 2000)
Authentication Strategies

Three main approaches to user authentication:

- Something the user *knows* (e.g. password or PIN)
- Something the user *has* (e.g. a card or other token)
- Something the user *is* (i.e. a biometric characteristic)
Weaknesses of traditional methods

- Passwords and PINs are often:
  - badly selected (and easily guessed)
  - written down
  - shared with colleagues or friends
  - infrequently changed
  - the same on multiple systems
Assessing Attitudes Towards Security

- Relevant to determine user attitudes towards security
- Questionnaire distributed to 161 mobile phone subscribers
- Aim to assess:
  - usage of mobile services
  - usage of current authentication methods
  - likely acceptance of more advanced methods
Usage of Mobile Services

- Voice: 99% Yes, 1% No
- Text Messages: 90% Yes, 9% No, 1% Unavailable
- Info. Services: 66% Yes, 19% No, 15% Unavailable
- WAP: 48% Yes, 46% No, 6% Unavailable
Future Mobile Services

- Respondents support convergence of devices
- In total, 88% of respondents want some form of additional service from their phone:
  - 73% would like personal organiser functions
  - 58% would use the web
  - 53% to download music
  - Additional services suggested included: Digital money, radio, GPS
PINs on mobile handsets

- 4 - 6 digit number to be entered on the numerical keypad of the phone.

- Two possible levels of protection, both of which can be independently enabled or disabled:
  - at switch on (all phones)
  - to enable phone to come out of a standby mode (some phones)
Use of the PIN in practice

- 89% had knowledge of the PIN facility
  - The 11% that were unaware would scale to approximately 84.5 million users worldwide
- Although 89% knew about the PIN facility only 56% used it
  - 65% of those who did *not* use it blamed inconvenience
- 41% did not have confidence in the protection of the PIN facility
- Of the 24% who had 2 level PIN security, 64% did not use it, finding it inconvenient
### Compromising the PIN

<table>
<thead>
<tr>
<th>Action</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forgot it</td>
<td>17%</td>
<td>83%</td>
</tr>
<tr>
<td>Told it to someone else</td>
<td>26%</td>
<td>74%</td>
</tr>
<tr>
<td>Wrote it down</td>
<td>6%</td>
<td>94%</td>
</tr>
</tbody>
</table>
Attitudes towards Future Security

- 81% believed additional security a good idea
  - Of these, 63% would even accept continuous authentication / supervision
- Only 2 out of 161 respondents considered additional security to be a bad idea

- Users are already concerned about security . . . but don’t use available protection
- Need to consider alternative approaches
Future Authentication Requirements

- Inconvenience was a major reason why survey respondents did not use PINs
  - require methods that can be non-intrusive
- Also desirable to have methods that users cannot easily invalidate
- Token based methods not likely to be viable for mobile systems
  - tokens could be carried with devices or left permanently in situ
### Biometric Approaches

<table>
<thead>
<tr>
<th>Physiological</th>
<th>Behavioural</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprints</td>
<td>Voiceprint</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Signature Recognition</td>
</tr>
<tr>
<td>Vein Checking</td>
<td>Keystroke Analysis</td>
</tr>
<tr>
<td>Iris Scanning</td>
<td>Mouse Dynamics</td>
</tr>
<tr>
<td>Retinal Scanning</td>
<td></td>
</tr>
<tr>
<td>Faceprint</td>
<td></td>
</tr>
<tr>
<td>Facial Thermogram</td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
- Biometric Approaches include both Physiological and Behavioural techniques.
Error Rates

- **False Acceptance Rate (FAR)**
  - errors where impostors are falsely believed to be legitimate users

- **False Rejection Rate (FRR)**
  - errors where the system falsely identifies the legitimate user as an impostor
FAR / FRR relationship

- False Acceptance Rate (FAR)
- False Rejection Rate (FRR)
- Equal Error Rate

Rate (%)

Slack

Tolerance / Threshold Setting

Tight

Increasing end-user rejection
Biometrics on mobile devices?

Face recognition

- An internal camera could capture a digital image
- Processed to determine a series of characteristic vectors
Biometrics on mobile devices?

Speaker recognition

- An internal microphone could capture voiceprint information
- Verification may be text dependant or independent
Biometrics on mobile devices?

Signature verification

- A touch screen could capture the user’s signature
- May be measured statically or dynamically
Biometrics on mobile devices?

Iris Scanning

- Based upon unique characteristics of the eye
- Could be done using a high resolution still image camera
Biometrics on mobile devices?

Keystroke Dynamics

- Based upon analysis of typing rhythms
- May be implemented in static or dynamic modes
Biometrics on mobile devices?

Fingerprint Recognition

• Same principle as standard approach in criminology
• Based upon forks and ridge
• Requires specialist reader on mobile device
Advanced Mobile Authentication in action

- British Government's computerised ministerial red box
- Unlocked through a combination of:
  - a minister's fingerprint
  - special personal signet ring
Biometric Preferences

- Fingerprint: 74
- Voiceprint: 55
- Facial Recognition: 29
- Iris Scanning: 41
- Typing Style: 28
Mobile biometrics in practice

- Initial experiments to assess keystroke dynamics on a mobile phone
  - aim to authenticate users by assessing keypad activity
  - build profiles of characteristic inter-keystroke latency timings for different users

- Two distinct advantages:
  - no additional hardware required
  - completely transparent to the user
Mobile biometrics in practice

- The study involved 16 test subjects and assessed two types of keypad input:
  - 4-digit PIN codes
  - standard telephone numbers
- Neural networks were trained to differentiate between legitimate users and impostors
- Samples collected from a modified handset, via a PC
## Mobile biometrics in practice

<table>
<thead>
<tr>
<th>PIN Code</th>
<th>FAR</th>
<th>FRR</th>
<th>EER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>18.1%</td>
<td>12.5%</td>
<td>15%</td>
</tr>
<tr>
<td>Telephone numbers</td>
<td>16%</td>
<td>15%</td>
<td>15%</td>
</tr>
</tbody>
</table>
Mobile biometrics in practice

Performance of Keystroke Dynamics in the PIN experiments

![Graph showing FRR and FAR percentages for different thresholds.](image)
Potential for improvement

- The initial study was limited in terms of:
  - test samples obtained
  - network training

- Some individual users performed as well as 0% FRR and 1.3% FAR
  - Previous experiments with full alphanumeric keyboard have observed similar results as the average
Potential for improvement

- Keystroke dynamics will work for *some* users in *some* contexts
  - e.g. only non-intrusive if user is already interacting with the keyboard
- Other techniques will exhibit similar characteristics
- Potential solution – combine techniques in a hybrid manner
  - utilise context and user profile to determine appropriate method
A future scenario?
Conclusions

- User authentication is a key security requirement for mobile systems
- Survey results show that current methods may be compromised
- Biometric technologies offer a means to make authentication more transparent
- Unfortunately, one size does not fit all
Dr Steven Furnell
sfurnell@plymouth.ac.uk

Network Research Group
www.plymouth.ac.uk/nrg