Enhancing User Authentication for Mobile Handsets

Sevasti Karatzouni

sevasti.karatzouni@postgrad.plymouth.ac.uk

Network Research Group
The Research Project

- This research is funded by the Eduserv Foundation.
  - Founded in 2003, Eduserv is a not-for-profit IT services group delivering innovative technology services. With contributions from Eduserv, the Eduserv Foundation funds initiatives supporting the effective application of IT in education
  - Grant awarded in 2005 for a 2 year study into *Flexible and Non-Intrusive User Authentication for Mobile Devices*

- Research is being conducted by the Network Research Group (NRG)
  - Established in 1985, the NRG conducts research into IT Security, Internet and WWW technologies and mobility
  - Researchers active on the project:
    - Prof Steven Furnell
    - Dr Nathan Clarke
    - Miss Sevasti Karatzouni
Overview

- The need for authentication
- Authentication approaches
- End user views and attitudes
- Research project - Flexible and Non-Intrusive Authentication
- Future work
The Need for Authentication

- More than 2.5 billion mobile subscribers worldwide

![Mobile Subscribers Chart](GSM Association 2006)

- Estimated to reach **3.96 billion** by 2011 – Close to 2/3 of world’s current population.
- Mobile theft in the UK comprises the 45% of overall theft.
- More than 54,000 mobile handsets were left on the back of London cabs within only six months.
The Need for Authentication

What protects this data from unauthorised access?
Authentication Approaches

- Three main categories of 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)
End User Attitudes & Opinions

- What do consumers think about mobile phone security?

- Quantitative approach
  - Online survey of 297 cellular subscribers

- Qualitative approach
  - Focus group including various stakeholders including a cellular network provider, corporate network provider, end users and academics


“Perceptions of User Authentication on Mobile Devices” (Karatzouni et al. 2007. Proceedings of ISOOneWorld, Las Vegas, USA)
Quantitative - Survey

- 66% of respondents use the PIN
- 30% considered the PIN inconvenient
- 85% of respondents were in favour of additional security
Qualitative – Focus Group

● Research Questions:
  – Do participants recognise a need for security on their current devices?
  – How do participants perceive the current authentication facilities?
  – Do participants envisage a need for greater security provision in the future?
  – How do participants perceive the potential alternative methods of authentication?
Current Need for Security

Participants did not feel at risk as their usage was limited and not involving highly sensitive information

“As a general user who is only using it for personal use, there’s no data on there that I class that sensitive”

“I use this [Pocket PC] just for access to the exchange server and nothing else…So the issue of security hasn’t arisen with this yet, but probably will do at some stage”

“I think it depends from which context you are using it in, cause the security you are going to need in it, is going to depend on the sensitivity of the data…the only thing that I got that is sensitive is friends’ phone numbers and address details”
Perception of Current Authentication

- Only one third of the participants use PIN protection

- Some consider it inconvenient or insufficient:

  “I think any security that is going [to] lock me out every now and then…is the reason I don’t use PINs now cause I always forget my PIN…”

  “I never turn my phone off so if I lost it would be on anyway”

  “I’ve used them before. It’s simple to use, it’s just…I don’t see any point using it myself cause I never turn my phone off”
Perception of Current Authentication

- Only one third of the participants use PIN protection
- Some consider it inconvenient or insufficient:
- Some just don’t feel they require any protection

“I’m not sure that anybody would want to steal my information, I don’t perceive myself to be that important”
Need for Greater Security?

The majority agreed that use of more data-centric and sensitive services would increase their need for protection.

“If you are using it from a business context, obviously you know the more important the data then the stronger security is going to be needed.”

“Although I don’t use my phone for an awful lot more than texting at the moment, as phones get more sophisticated and easy to use etc … I’m going to start using it for mobile banking or whatever the nature of the data that I’m gonna be using is going to become more sensitive definitely”
Another aspect that was highlighted was the fact that stronger security would be desirable in certain uses of the phone, as the danger of misuse would be increased.

“If I make a local call … maybe I’m not that worried … But certainly when I want to start dialling international number or something maybe I do want to make sure that it’s stronger authenticated. Maybe when I start to accessing documents that sit in a specific area of my device which is business documents then I want to be authenticated”
Participants were not receptive to using tokens.

“*My first opinion would be that is just something else to lose…you still have the same issues with the token, because somebody could pinch the token, or I would lose it more likely*”

“It’s also the annoyance. Unless it’s something you wear all the time… if I want to make a phone call I also have to take my watch or my key ring or whatever”
Participants were receptive to using biometrics.

“Personally I’d use fingerprint, it’s easy…”

“I think fingerprint recognition would be fine on a phone…”

“Fingerprint is the most appropriate”

“Voice as well…obviously when you are talking”

“The thing is even though it’s a telephony device, the one I would be more uncomfortable using is voice, because anyone else can hear it”
Although acknowledging the level of security that biometrics can provide, participants would have little tolerance of getting falsely rejected and being locked out of the device:

“If it always let me through I’d be prepared to put up with that [false acceptance errors], because it’s still a greater level of security that I use now and it’s still not bothering me….I’m prepared to let the mistake happen as long it’s not for me, as long as I am always let through”
Novel Authentication - Objectives

Authentication for mobile handsets must meet the following objectives:

- Increase security beyond secret-knowledge techniques
- Provide transparent authentication
- Authenticate the user continuously/periodically throughout the day in order to maintain confidence in the identity of the user
- Tie the level of security to the type of service
Biometrics on Mobile Devices

- Signature Recognition
- Voice Verification
- Keystroke Dynamics
- Facial Recognition
- Service Utilisation

Facial Recognition
Keystroke Dynamics
Signature Recognition
Voice Verification
Project Issues – Future work

- Device-centric versus network-centric topologies
  - Device requirements/capabilities
  - Network server requirements
- Scalability
- International roaming
- Personal mobility
- Configuration and management
Thank you

Any Questions?

http://www.network-research-group.org/nica