Non-Intrusive Biometric Authentication for Mobile Devices

Nathan Clarke, Dr Steven Furnell, Prof Paul Reynolds and Philip Rodwell
Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, UK

Introduction

In the vast majority of mobile devices, the only protection against unauthorised use comes from a Personal Identification Number (PIN). With the convergence of devices and the extended range of services that will be accessible through 3G networks, a strong argument exists for stronger and more robust methods of user authentication. The research relates to the investigation, design, and evaluation of advanced subscriber authentication techniques, suited to application within the context of a mobile device. This poster presents the continuing research from the Network Research Group, University of Plymouth, which is being conducted in collaboration with Orange.

The Current Problem

Subscriber authentication in current mobile networks, such as GSM, is relatively limited, with the vast majority of devices relying upon a Personal Identification Number (PIN) method.

A survey of 275 mobile subscribers reveals the problems of the PIN approach:

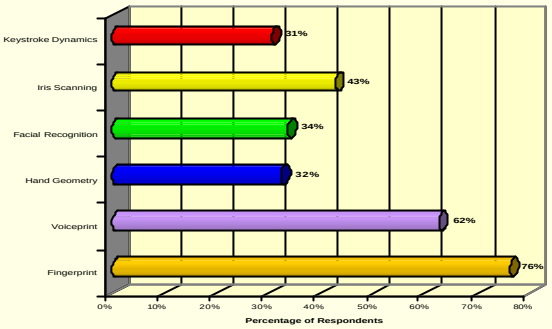
- ✗ 39% of respondents do not use the PIN
- ✗ 43% of respondents find the PIN an inconvenient authentication method
- ✗ 58% of respondents do not have confidence in the PIN

Third generation (3G) devices demand improved authentication methods due to their convergence with Personal Digital Assistant (PDA) devices, and the subsequent expansion in the range of possible services enabled as a result. The potential consequences of a masquerade will be far more severe.

The survey revealed opportunities for enhancing authentication methods:

- ✓ 84% of respondents believe more security to be a good idea
- ✓ 50% of respondents supported a continuous and non-intrusive authentication method.

Respondents' opinions regarding the use of biometric techniques on a mobile handset are illustrated in the graph on the right.



Acceptability of biometric authentication options

The New Concept

Facial Recognition

- An internal camera could capture a digital image
- Processed to determine a series of characteristic vectors

Service Utilisation

- Profiling subscriber's typical interactions with their device
- Analysing usage patterns, utilising time and frequency

Keystroke Dynamics

- Based upon analysis of typing rhythms
- May be implemented in static or dynamic modes

Iris Scanning

- Based upon unique characteristics of the iris
- Could be done using a high resolution still image camera

Signature Recognition

- A touch screen could capture the user's signature
- May be measured statically or dynamically

Voice Verification

- An internal microphone could capture voiceprint information
- Verification may be text dependant or independent

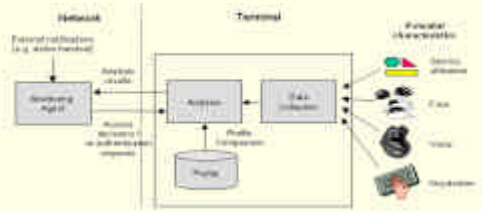
The Realisation

Authentication Framework

Advanced authentication may be handled within a flexible framework, which intelligently monitors the available biometrics based upon the subscriber and their current activity.

For example, voice verification could be utilised during a voice call, but during an e-commerce transaction it could be replaced by other characteristics that are more appropriate to the context, such as keystroke analysis.

The terminal would collect and locally compare the data against the subscriber profile, and then securely send the results to a network-based monitoring agent for access decisions (ensuring that the network operator is aware of potential compromise).



Potential Subscriber Monitoring Scenario

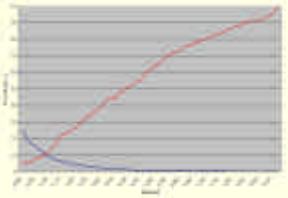
Example Biometric – Keystroke Dynamics

Initial experiments have been conducted to assess keystroke dynamics on a mobile phone - to authenticate users by assessing their interactions on the keypad.

The initial study involved 16 test subjects and utilised two types of keypad input: 4-digit PIN codes and standard telephone numbers.

Keystroke data was collected from a modified mobile phone handset, connected to a PC, in order to preserve the tactile context of a mobile device.

Neural networks were trained to differentiate between legitimate users and impostors.



4-Digit PIN Network Performance

	FAR	FRR	EER
PIN code	7.9	3.1	5.5
Fixed telephone	4.5	1.8	3.2
Varying telephone	17.1	15.1	16.1

Note: Individual networks performed as well as **0% FRR** and **0% FAR**

Summary

The capabilities of 3G mobile systems open up a range of new service opportunities and, as a consequence, impose new requirements for security. The survey findings indicated a weakness of the current provisions, in that the authentication technology is optional and, therefore, often unused. However, subscribers have shown the desire for additional security, and have responded positively to a number of alternative techniques. Given that many respondents do not use the current security techniques that are available to them, it can be assumed that a non-intrusive method of authentication may prove to be most acceptable and widely utilised by end users. Viable architectural frameworks can be specified to support this, and suitable biometrics can be identified to provide the underlying authentication methods.

www.network-research-group.org