Biometrics for secure mobile communications

July 20 2006

SecurePhone. Credit: SecurePhone

Though security applications that verify a person's identity based on their physical attributes, such as fingerprint readers or iris scanners, have been in use for some time, biometric security has only recently started to appear in mobile phones, PDAs and notebook computers where the need for miniaturisation represents a technological challenge.

So far biometric data has been used to tie the device to a person to prevent it from being used illegitimately if lost or stolen. But the IST project SecurePhone is taking a new approach, employing physical attributes to enable the user to digitally sign audio, text or image files, providing proof of their origin and authenticity.

"As far as we know there is no other biometrically-enabled digital signature application available for mobile devices that can guarantee security by storing and processing all sensitive information on the device's SIM card," explains SecurePhone technical coordinator Roberto Ricci at Informa in Italy. "Because biometric data never leaves the device's SIM card and cannot be accessed, except by the verification module which also runs on the SIM card, the user's biometric profile is completely safe. This is important to meet the highest privacy requirements."

Although existing communications infrastructure based on the GSM, GPRS and UMTS mobile systems provides a secure means of communication, it lacks any robust method of user identification. Text, audio and image files can be sent by anyone to anyone with no authentication and there are no guarantees the person you are talking to in a phone conversation, if you've never met them before, is really who they claim to be.

The upshot is that data exchanged over mobile devices is of limited use for legally binding transactions even though mobile devices, given their ubiquity, would be a prime candidate for carrying out e-commerce (or m-commerce), managing business processes such as signing contracts or even in securing the exchange of data in e-healthcare and e-government systems. A digitally signed and authenticated voice recording during a telephone conversation would, for example, give the speaker's words legal value.

"The aim is to enable users to exchange information that can't be disputed afterward. That could be a voice recording that is authenticated to eliminate any doubt about who the speaker is, what they actually said and prove that it has not been manipulated," Ricci explains. "To achieve that it is necessary to digitally sign the data and to ensure that only the legitimate user can perform the signing."

The system developed by the SecurePhone project partners consists of two main elements. The first, an authentication module, uses biometric security applications to verify the user's identity. That in turn gives them access to the second module which digitally signs the data using a Public Key Infrastructure (PKI).

"Rather than relying on something you possess – you can forget a PIN code or write it down and lose it – biometric security relies on what you are," Ricci notes.

The system, which is designed primarily for PDA-phones but could also be used in new generation smart phones and WiFi-enabled PDAs, offers three methods of biometric identification. One employs the digital cameras that have become commonplace in mobile devices along with a face recognition application to identify the user based on their facial features. Another uses voice recognition software – also detecting any asynchrony between speech and lip movements - and the third verifies the handwritten signature of the user on the device's touch screen. The three methods are used in combination to enhance the overall levels of security and reliability, and most importantly they require no hardware additions to mobile devices.

"The SecurePhone platform is entirely software based. This is important if it is to be adopted by device manufacturers as it keeps costs down and makes implementing it much easier. There is no need to add fingerprint or iris scanners. Instead, the system uses elements that already exist in

the device and which serve alternative purposes as well, while the type of verification carried out is non-intrusive for the user," Ricci says.

The project partners are currently working on the final integration of the system ahead of trials of a finished prototype that are expected to begin in August. Ricci notes that so far the different elements of the application have performed well during laboratory testing.

Despite SecurePhone's focus on research, Ricci notes that the resulting application is commercially appealing and that the project partners are planning a further project with the aim of bringing the technology to market.

"We would probably aim at niche markets at first, such as busy executives, e-government or e-healthcare, and then expand from there," he says.

Source: IST Results