Ileana Buhan

You meet someone at a conference and, after chatting for a while, you decide to exchange confidential information stored on your respective PDAs. How can the security of the information be guaranteed in this kind of spontaneous situation? Ileana Buhan wants to use biometrics for this.

Exchanging pictures for security's sake

"The spontaneous interaction of two mobile devices implies that you had nothing in common beforehand. There's no connection to a server, and no security policy. How can you safely send confidential information in that case, within an environment that is inherently insecure? Of course, you could use Bluetooth and a four-digit PIN code. But a code of that kind can be cracked in less than a second, and our research even shows that most people would happily choose '1234'. That can hardly be called security!"

"You'll have to figure out a fast and easy way of generating a stronger password or key. Both devices will calculate the password and, if there is a match, a connection will be made. But based on what information can you calculate a key? The usual way of doing this involves a public and a private key. However, if you never met before, you won't be able to verify to whom the key belongs. Therefore, our aim is to use biometrics, which is user friendly. If Alice stores her own picture on her PDA and Bob does the same, they can take a picture of each other. Both PDAs then generate a password based on the two pictures. This is a powerful password: it would take years to crack."

"The problem, of course, is that the picture that Alice takes of Bob will never be exactly the same as the picture Bob has saved of himself. And the same holds for the picture of Alice. That would seem to imply far too much uncertainty when you're trying to generate a common password. We treat the differences between pictures as noise, and use statistics to decide how much noise is acceptable. This uncertainty also rules out the use of existing encryption techniques. If you have two pictures that closely resemble each other, and you encrypt both of them, the result will still be two codes that don't match up at all. So you'll just have to compare the pictures before encrypting them. In fact, we don't use the actual pictures for the comparison, but a set of characteristic features, like the positions of the eyes, or the dimensions of the lips."

"The original idea of using biometrics came from the SecureGrip project, in which police hand guns are secured by their 'hand print', or personal grip pattern. The gun will immediately recognize a different grip pattern and won't function in the wrong hands. But what if a police officer has to borrow a colleague's gun? Then you have a similar pairing problem. A possible solution would be for them to hold each other's weapon, to allow the grip patterns to be compared in the same way as the pictures, and to produce a matching key. Apart from that, past CTIT research has explored using your personal picture to access your own PDA or mobile phone, as a standalone password. One research result was an excellent face recognition algorithm, but then we discovered that not every PDA 'speaks' the same language. By choosing a slightly different algorithm for our purpose, we managed to overcome this problem."

> 'How can you safely send confidential information in an environment that is inherently insecure?'

"We also did some research into what people think of this way of pairing devices. They actually find taking each other's picture rather funny! 'I wouldn't take a picture of my boss' they say. In a business context, people prefer something like a PIN code. But then you have the problems I mentioned earlier. I think it's largely a matter of getting used to the idea. And if face recognition isn't the right way, we could use fingerprints or voice recognition instead. Any kind of biometric information will do."