

Secure across borders

Charles Brookson, European Telecommunications Standards Institute (ETSI) Operational Coordination Group OCG Security Chairman, talks to Intercomms about the standards body's role in enabling secure architectures



Charles Brookson CEng FIEE FRSA
Chairman of ETSI OCG Security

Charles Brookson works in the Department of Business, Enterprise and Regulatory Reform and is a Professional Electronic Engineer. He previously was Head of Security for one2one (now T-Mobile UK), and worked within British Telecom for twenty years before. He has worked in many security areas over the last 30 years.

He has been Chairman on the GSM Association Security Group. He has been working the GSM and 3GPP security standards, first chairing the Algorithm Expert Group way back in 1986. He is Chairman of the NISSG, a group that was set up to co-ordinate security standards amongst the three European Security Standards Organisations and other bodies outside Europe. He is also Chairman of ETSI OCG Security, which is responsible for security within ETSI. He is also on the Permanent

Stakeholders group of ENISA, The European Network and Information Security Agency.

Q: Could you describe the current state of play with regards to ETSI's work with encryption and security?

A: Various initiatives have moved along over the past twelve months. Now, there is much more interest in Near Field Communications or RFID. There is within ETSI itself for example an RFID Group being talked about, just to address that technology's security issues. ETSI also have a new Quantum Cryptography Group.

Q: What can Quantum cryptography offer?

A: Quantum cryptography is an unbreakable authentication system. In very simple terms, quantum cryptography sends information via photons. You need all of them in order to read the message. It's seen as the second secure system that has yet emerged. The first was the Vernam One Time Pad. There you have a completely random set of data with which you mix your original text. That does however suffer the disadvantage that the encrypting text is as long as the text that you are sending. It's quite inefficient, but it is unbreakable.

Q: Has the work on security thus far being paying dividends to the consumer?

A: All the hard work on securing mobiles, through various different fronts including the GSM association, ETSI and others does seem to have paid off. In the UK for example, there has been a drop the number of phones being stolen.

Q: What about interest in Near Field Communications?

A: There has been some interesting recent activity in the Netherlands in the Near Field Communications with MIFARE cards. Of course, that is just one chip, but clearly there are issues there relate to the wider security of protocols and attempts to standardise. There are also huge privacy issues on which the European Commission is working with ETSI and others. One suggestion has

been that RFID tags on clothes and goods should be erased when you leave the shop. That would prevent others from profiling customers as they walk around with multiple, active tags, for the purposes of marketing. The issue is complex because that same technology is also used for other items like passports and Oyster cards on the London Underground for example. Consequently, there are important privacy mechanisms that need looking at.

ETSI's work on Near Field Communications is tied in with other work such as M-Payments, which can be based on the same technology. There are also other solutions that could be used such as text messaging. That approach is used by Vodafone in Kenya to enable people without banks to pay one another electronically in countries without a developed banking systems or where people have too little money to even think about a bank. It could also be used to transfer money between one country to allow the local immigrant population remitting money back to their relatives.

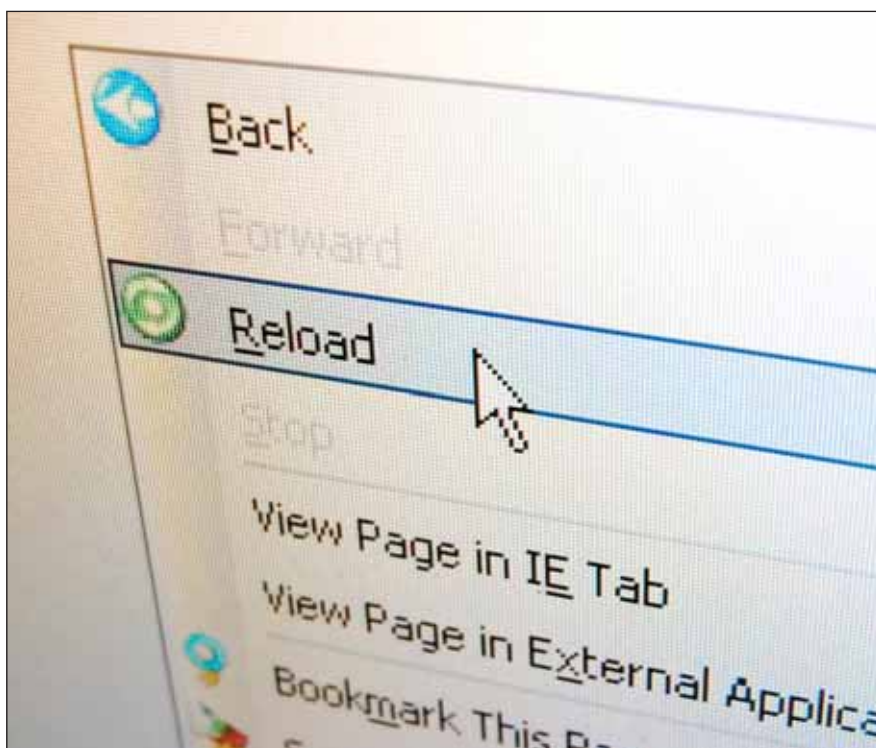
Q: Is there interest in seeing these types of approaches being adapted in the developed world?

A: In some countries they are already incredibly popular. Turkey for example has a well developed M-payments system. There you can text someone a code that they can then can punch into an ATM and get cash out.

However, it really depends on whether people adopt it. That seems to me a totally random process, much like how SMS has taken and even the first mobile phones too. When the take off of mobile phones began there were small 'explosions' of users in specific areas where people saw others using them and then bought one themselves.

Q: How does the advent of Next Generation Networks (NGN) affect the security picture?

A: NGNs are basically a huge IP-based multi-media infrastructures such as BT's 21C network and ETSI's Tispan group which builds upon the work already done



► by 3GPP on a harmonized IMS-centric core for both wireless and wireline networks. In addition, there are also interesting developments like the Femto cell, low power bases stations enabling you and I to run our own 3G network in our homes, much like a wireless router. There are all sorts of security issues around that.

Q: Does the speed of the throughput pose challenges for existing encryption systems?

A: High speed access systems such as 3GPP's Long Term Evolution have demonstrated that 70Mbps broadband on the move is possible in lab conditions. Existing security systems should run perfectly well on that. There is very little overhead in running encryption so the whole of the current 3G encryption will support that.

Security is layered in the sense that different people have different levels of control. If for example you are an operator running a communication system, then you put encryption on the communications itself. If you are a bank, using that communication system, then you will be running encryption end-to-end for the customer device to your bank and third parties.

Q: Trust brings in the issue of human factors. To what extent are improvements in security targeting the user rather than 'just' the technology?

A: Clearly there are tradeoffs. You don't want to ask people lots of question although, that has, to a certain extent worked up until now. At some level the operator has to make decisions for you. Many mobile phones now actually tell you whether encryption is turned on or off via an encryption indicator. Eventually, however as in Microsoft products you will still be asked lots of question as to whether you trust this or want to download that. That can be reduced but not eliminated.

Q: How are human factors being fed into the wider ETSI standards role?

A: There is a Human Factors Group at ETSI and some of the guidelines that they have issued are actually fed into other initiatives. It is recognised throughout ETSI that a system has to be acceptable to the user and the degree to which it relies on the user's intelligence, is a very important aspect of any design.

Q: What about the rise of Malware and Trojans within an all IP environment?

A: As terminals become smarter and more like PCs that is an issue we need to start thinking about. At the moment, it's not huge issue but clearly when devices are being used for payment systems, then it will start to attract attention. I know within the GSM Association for example, mobile malware has been addressed and discussions between manufacturers are taking place. Eventually, this will lead to things like better operating systems and there is work going on in regards to trusted modules for mobiles. At the moment every computer that is less than three years old actually has a trusted secure module inside it and there are standards being worked on now to extend that to mobiles.

Q: How is ETSI interacting and working with national governments and the Commission?

A: There is of course ENISA (European Network and Information Security Agency). That's the Commission organisation responsible for producing guidelines for businesses, SMEs and individuals. There is a big tie up between ENISA and ETSI and we have a co-operation agreement with them. They have been helping to co-operate on all the security standards, together with the ITU. We have a list of security standards available from all the standards organisations, which as far as we can, we keep up to date. There is certainly a significant emphasis on security, from the commission and its bodies.

In general, what we produce are generic standards. People then put together systems based on those standards. In the case of an electronic signature, people can sign their document, send it off to someone else and who can then countersign it. All this is done electronically. Behind those signatures however, there has to be a legal agreement within Europe and indeed there is a European electronic signature directive, where there is a legal acceptance of an electronic signature. Clearly with things like M-payments, the capability is already there within the devices. Then one can look at all the business relationship and systems on top of that based on those open standards. ETSI produces the standards that others will put together within a system.

For more information please visit:

www.etsi.org