Cyber-crime
New technologies

Everyday, unsuspecting people around the world are falling prey to cyber-criminals acting individually or in organised crime circles. These fraudsters specialise in deception, whether it be credit card fraud, identity theft, or 'phishing'.

The Internet has revolutionised how people do business, interact with government, learn and entertain themselves. But it is also a place where unscrupulous cyber-criminals armed with e-fraud tools and sophisticated 'crimeware' can steal your identity, either online or through mobile telecommunications networks. The potential for cyber-crime is almost as limitless as the boundaries of cyberspace. However, so is the potential for new technologies to foil such deception and protect consumers through identity management.

protect consumers

Credit card fraud used to mean someone stealing and using your card or number. Today, it could involve 'skimming', a high-tech device that collects your credit card information and makes it easy to produce a replica of your card. Identity theft used to mean someone rifling through your household bin to find bank statements, benefits information, calling card and personal identification numbers and using the information to pretend to be you. This still holds true, but today's sophisticated thief is likely to be armed with an arsenal of e-fraud tools that can steal your identity in cyberspace.

'Phishing' scams involve using email to link consumers to phoney websites that ask users to confirm their account information by entering personal data into an official-looking online form. It is on the rise in the USA, which means Europe cannot be far behind. Data confirms that in 2005, about 109 million US users received phishing e-mail attacks, a 100% increase from the previous year.

These are just a few examples of cyber-crime. While the definition of identity fraud is not black and white, it is like all frauds in that it involves an element of deception. This can involve:

Deception as to an individual's identity.

Deception as to that individual's entitlement or authority to receive funds.

Deception as to that individual's intention to provide goods or services.

In addition to the serious financial losses suffered by victims, insurance companies, banks and other institutions, there is the unquantifiable cost of consumers losing faith in the Internet and mobile telecommunications networks to deliver goods and services. The threat is invisible until it happens, which means concerns about privacy issues may often undermine support for better personal data protection measures.

Effectively fighting cyber-crime involves a multi-pronged approach. The right legislative framework is critical to fighting cyber-crime and enforcement measures must be in place. Equally critical is sophisticated technology to mitigate security risks and increased public awareness.

Building trust is key

Building trust in a world increasingly characterised by multi-layer vulnerability is a huge challenge. In the middle of this complex landscape is the consumer looking for the ultimate: unlimited online and mobile connectivity that is secure, seamless and simple.

A question often asked by government and industry is: How can the public and private sector work together to maintain the integrity of identities and payments and retain the confidence of consumers?

'Users do not want to bother about security issues. They want mobility and access to services, but are reluctant to give personal data that may be misused, particularly when services such as banking and others are being threatened,' says Heinz Brüggemann, director of EUREKA's CELTIC Cluster, an industry-led initiative dedicated to R&D in end-to-end telecommunications solutions.

'We must resolve this tension between user comfort and security requirements. We need to create an easy-to-use, invisible, secure environment that is trusted by the user and cannot be threatened,' he adds. 'We also need a standardised approach to provide a framework agreed upon by industry, public authorities and consumers.'

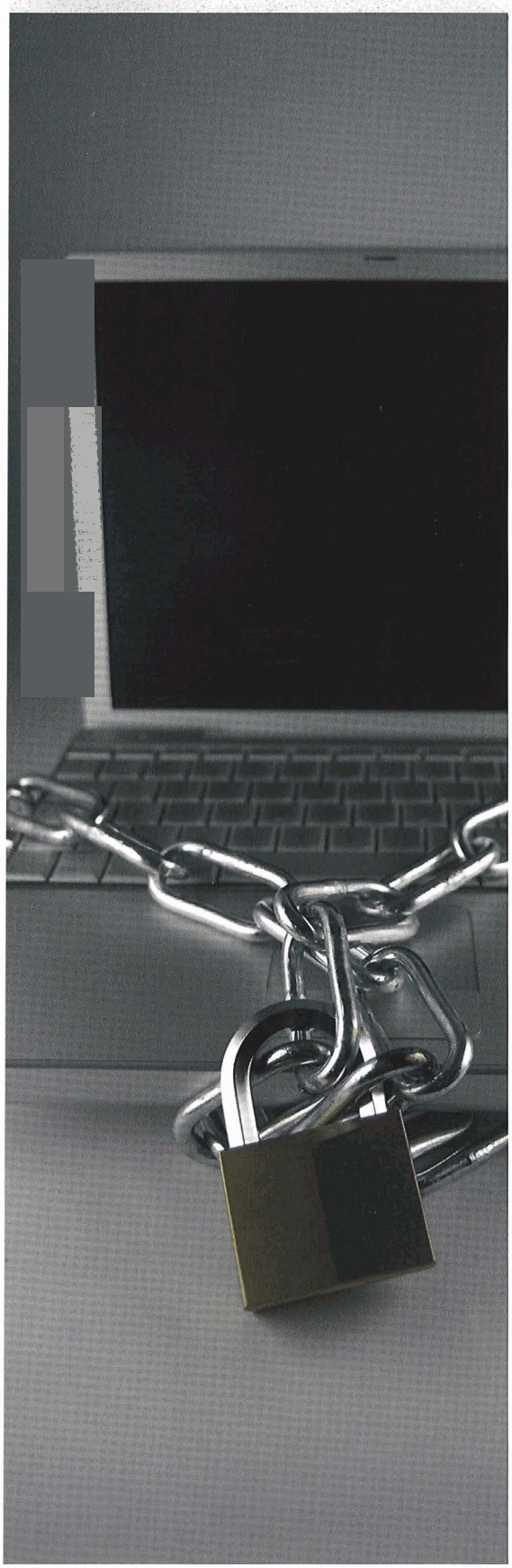
Identity management: a key enabler for tomorrow's Internet

Standardisation issues are being addressed in several forums, including the global Liberty Alliance, which brings together technology, business and policy experts to address security in areas such as healthcare, e-government, payments and identity theft. EUREKA's CELTIC project, FIDELITY (CP2-013 Federated Identity Management based on Liberty) tested the technical, economical and legal viability of Liberty's approach to identity management in a pan-European context through seven close-to-market scenarios.

FIDELITY implemented Liberty ID-FF1.1 and ID-WSF1.2. ID-FF is based on SAML1.1 (Security Assertion Markup Language) which is an XML (extensible mark-up language) standard for exchanging authentication and authorisation data between security domains, that is, between an identity provider and a service provider. ID-FF addresses this critical issue, known as the web single sign-on problem, and ID-WSF is about sharing the user's attributes.

The project, which ended in December 2006, focused on Federated Identity Management (FIM), a system that allows individuals to use the same user name, password or other personal identification to sign onto the networks of more than one enterprise – or service provider – to conduct transactions.

→



Partners in a FIM system depend on each other to authenticate their respective users and vouch for their access to services. In this way, authentication becomes interoperable and secure among various providers. For users, it is both simple and seamless.

FIDELITY used the project results to create a business model for identity management in which a telecommunications network operator acts as an identity provider. Project coordinator Guillaume Garnier de Falletans, from France Télécom R&D, says the results reinforced consortium partners' conviction that identity management is a key enabler for tomorrow's Internet. 'Telecommunications providers, thanks to the trust relationship they already have with their customers, can play a very important role,' he says.

FIDELITY developed a mergence of 'circles of trust' interconnecting identity providers. 'By interconnecting them, the advantage to the user is seamless and simple as they change from one circle of trust to another without having to authenticate each time,' Garnier de Falletans explains. France Télécom is taking project results further to develop *My Civil Service*, a platform allowing citizens to access government services using the Internet.

An ongoing CELTIC Cluster project, SEIMONET (CP2-023, Secure Interworking of Mobile & Wireless Networks), is developing a new architecture for secure billing and authentication across heterogeneous networks. It is focusing on providing a mechanism to enable seamless mobility of the user between WLAN and GSM environments.

Smart cards deliver security

The potential for smart cards in this field is limitless. Early EUREKA projects focused on developing common standards for EU citizenship cards based on an IAS (Internet Authentication Service) common platform. Projects under EUREKA's MEDEA+ Cluster, which supports advanced R&D in the microelectronics sector, are delivering results.

Small microprocessor chips embedded in smart cards that can hold and process data, enable them to address identity security issues. Before the breakthroughs achieved by the Esp@ss-is (Project A302) consortium, a smart card chip could hold and transmit just 424 KB of data per second through contactless technology. In a contactless smart card, the chip communicates with the card reader through RFID (radio frequency identity) technology. The project developed a chip able to hold and transmit 1.7 Mb of data, which is ample to perform transactions requiring high security, such as paying bills, when connected to the Internet through a wireless interface.

'The core architecture we developed within the project is based on contactless technology with large storage capabilities,' explains project partner Andreas Raschmeier STMicroelectronics smartcard division. 'The core architecture can also be used for mobile connectivity to secure transactions over the Internet.'

Laurent Sourgen also of STMicroelectronics smartcard division, describes a situation where a foreign traveller can use a bank card in a system that recognises the card does not have the right access application. The system authenticates the identity of the user, gets authorisation to unload from the user's bank, uploads to the local electronic purse and delivers cash. Another application is downloading music to mobile phones while respecting digital intellectual property rights.

Most users are unaware that behind a smart card lies a labyrinthine network of systems, servers and software that manages identity and authentication. In this territory, the issue of interoperability is critical in providing security.

'This issue was addressed by working in a consortium under the EUREKA MEDEA+ Cluster. STMicroelectronics developed the integrated circuit and each partner contributed technology that built the system, including readers, software, background systems and computers,'

Sourgen says. 'When designing a chip, we need a clear understanding of the whole system before we can develop the right product. High-end products cost millions to develop. By working this way, we share the risk and avoid failure.'

The project ended in 2004, but laid the foundation for quantum leaps in the field. For example, an ongoing MEDEA+ project, Onom@Topic+ (2A302), is focusing on developing complete hardware and embedded software platforms to support a new generation of universal subscriber identity module (USIM) cards for pay services.

End-to-end security is paramount

The end-to-end security of electronic telecommunications networks is paramount as mobile, Internet and multimedia technologies converge. At the same time, governments and public authorities are facing huge challenges in the area of protecting the identity and privacy of consumers who use such technologies. Data protection is a key – and controversial – policy area for both national and EU authorities, as is protection of telecommunications networks.

The European Commission has recognised that identity theft and online fraud are major issues. It is taking a global approach and developing a general policy for the fight against cyber-crime, which should be released sometime in 2007. The Commission is looking to reinforce EU-wide coordination and cooperation, as well as to formulate a policy on international and public-private cooperation.

The European Network and Information Security Agency (ENISA), was created by the EU in 2005 to advise and assist EU member states and the business community on how to ensure a high and effective level of network and information security. Among other activities, ENISA has launched a pan-European discussion on a common authentication language to enable more effective identity management. The SAML standard, among others, is part of this important dialogue.

Spokesman Ulf Bergstrom says the future of Europe's economy depends on the establishment, maintenance and increase in security of transactions, which is in the interest of both consumers and business.

'Everyday, millions of consumers in Europe buy books, tickets, DVDs and perform e-transactions, including digital banking,' he says. 'For them, the secure transfer of data is paramount for the confidence, trust and development of e-commerce. European citizens must feel confidence in the protection of their privacy, just as they want to have full trust that their purchases and transactions are done in a secure way.'

The numbers tell the story

EU-wide statistics on payment frauds are unavailable, however, estimates on card fraud alone run into well above 1 billion euro per year. An upcoming Eurobarometer survey reports six out of 10 European citizens think identity fraud is widespread in their countries. About half of Europeans polled regard national measures against identity fraud to be insufficient and consider that tackling this issue at EU level rather national level would be more effective.

Alarming statistics estimate the total cost of identity fraud to the UK economy in 2006 at £1.72 billion, or 2.55 billion euros. APACS, the UK payments association, reports losses of £504.8 million (749.2 million euros) resulting from plastic cards being used by criminals pretending to be the rightful owner or by criminals using a fictitious identity.

In 2006, the Better Business Bureau reported the number of U.S. adult victims of identity fraud was 8.9 million in 2006. It estimates that losses due to fraud rose from US$ 53.2 billion in 2003 and US$ 54.4 billion (41.1 billion euros) in 2005 to US$ 56.6 billion (42.7 billion euros) in 2006.