

## Technical Appendix to Annex 4 Designing Out E-Crime: Removing vulnerabilities and reducing temptations

### 1 Has the time come to apply crime reduction principles to on-line malpractice?

The House of Lords report [www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf](http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf) on Personal Internet Safety called for a review of responsibilities and liabilities to encourage those wishing their customers go on-line to do more to help protect them, including by working together to improve the security of products and services. Debate has moved on since 2004 when such ideas were taboo and the EURIM-IPPR study on Partnership Policing found no consensus for even discussing this approach in its paper on Reducing Opportunities for E-Crime. [www.eurim.org.uk/activities/ecrime/reducingops.pdf](http://www.eurim.org.uk/activities/ecrime/reducingops.pdf)

The Lords Report has recommendations to improve the security facilities currently on offer (including intelligibility, interoperability, ease of use etc.) and to encourage co-operation in removing the underlying vulnerabilities which they seek to remedy. Work for the DTI-supported Foresight Programme into Cyberbersecurity (subsequently published as *Superhighway Robbery: Preventing e-commerce crime* by Graeme R.Newman and Ronald V.Clark) identified a need to apply “crime science” principles to the criminogenic (i.e. attractive to criminals) features of information systems, the Internet and E-commerce. The aims, as with physical crime reduction programmes, should include reducing the opportunities and temptations available when the goods and services “on offer” are CRAVED: concealable, removable, available, valuable, enjoyable and disposable.

They summarised the features that make the Internet so attractive to criminals as SCAREM:

- opportunities for **stealth**;
- an intellectual climate of **challenge**;
- ability to remain **anonymous**;
- automated tools for **reconnaissance**;
- tools and routines not only to **escape** but to cover one's tracks;
- the opportunity to automate and organise **multiple** crimes.

### 2 Are the obstacles to addressing these features technical or economic?

The “Internet” has no “security” or “authentication” layer but there has been much work on the use of encryption technologies to “authenticate” traffic before it is transmitted so that this can subsequently be checked by recipients. The systems already available require the use of common security processes by senders and receivers and/or their Internet Service providers and are used mainly for traffic to service business supply chains or trading markets. They rely on “transport layer security” implemented by standards such as SSL (HTTPS) or VPN. These require the authentication of one or both parties prior to the establishment of a secure “tunnel” over which data is exchanged. Such techniques are not currently promoted to mass-market end-users. Instead companies such as Symantec offer products and services to business and consumers to provide multi-layered defences for the systems they connect to the “Internet”.

Paragraph 2.1 of the Lords report makes an important distinction between

- the “Internet” (initial capital letter), defined as the global network of interconnected networks that transmit and exchange data by means of the Internet Protocol (IP);  
and
- “internets” (no capital letter), defined as sets of interconnected computer networks. These are often based on the same IP standards but have connection restricted to authorised users. They may also be known as extranets).

The hardware and software are often the same but the business models for providing “secure internets” to those willing to pay for security, (for example the US Department of Defence, the world’s stock exchanges or SWIFT [www.swift.com](http://www.swift.com) for authenticated funds transfer), are very different to those for supplying cheap access to millions of teenagers gossiping and swapping multi-media content over the “Public Internet”.

Moreover, those business models may be about to undergo fundamental change at the same time as the current protocols (IPV4) run out of addresses (faster than expected) and we see an accelerating transition to products and services developed, designed and built around the Pacific rim to use a new generation of protocols (IPV6). On the 29<sup>th</sup> June the ICANN board [www.icann.org/minutes/resolutions-29jun07.htm#n](http://www.icann.org/minutes/resolutions-29jun07.htm#n) agreed to support the regional registries in making this transition: i.e. an acceptance that will not be driven from the US. The implications, including for a multi-tier, multi-speed Internet, perhaps with different levels of authentication and security, appear profound – especially given that over 80% is owned and operated in the private sector with control distributed to avoid “single points of failure”.

What is “practical” is a matter of economics, intellectual property rights and cultural values, as much as of software engineering. The security features common to most of the servers and routers that underpin the current Internet are routinely switched off by those providing fast response or low cost services to researchers (who need raw power/speed) or consumers (wanting fast response multi-media).

Much effort is instead spent on encouraging consumers and small firms to install software that will identify traffic carrying known or suspected malware (a kaleidoscope of automated spam and phishing carrying worms, viruses, Trojans and spyware to facilitate an equally wide variety of malpractice) or attempts to visit websites believed to carry illegal/undesirable content or otherwise used to support criminal activity.

This is the equivalent of encouraging householders and storekeepers to fit better locks and grills on a crime-ridden housing estate and its vandalised shopping mall: a vital defensive activity but not one that will attract new residents or business to help regenerate the neighbourhood.

Those who inhabit “cybercommunities” also need:

- easy ways of establishing how secure their systems are, the threats they face and the balance of risk, facilities, ease-of-use and speed appropriate to their applications: leisure, learning, business etc..
- schemes (from basic consumer information packs through to more detailed information for technicians and professionals) that indicate clearly what security facilities are built into which products and services and to which security profiles/standards they conform
- security facilities that are pre-installed and configured to the security levels required by the average user (i.e. average for the market into which the systems is being sold) with clear information on what this means and how to customise the balance of facilities, performance and security.

Many suppliers claim to already provide such material and/or default settings, but the documentation is usually drafted for security professionals and does not follow common formats or use shared definitions and standards.

Those who come from a traditional crime prevention or security background also see a widespread need to make the systems and services of large organisations (especially banks, e-commerce players and central and local government) more resistant to misuse by those using them as part of their daily life (including employees and contractors) as well as by those not authorised to access them.

However, their employers do not always share this view, take a more risk-based approach and are keen to ensure their systems do not become harder to use. They also question how they can prevent phishing and similar attacks, beyond helping to educate their users. The traditional security professionals therefore see a need to promote better risk management at every level, underpinned by three basic principles:

1. Security should be easier for the user than insecurity.
2. Security should be cheaper for the user than insecurity.
3. Security should be a community issue.

These principles do not, however, have universal acceptance within the ICT and business communities, where there is a common view that security should be appropriate to the application - not “generic”. Moreover the application of these principles requires forethought. Unless done early in the planning and design process, it can lead to significant extra cost.

The Internet community was focussed until recently on ease of use and facilities. Security is therefore commonly seen as an add-on: something that will necessarily cost users additional time and money and will also provide suppliers with new business opportunities and/or competitive advantage. The software mass-market has similarly focussed on marketing-driven upgrades, with new facilities (and vulnerabilities) rather than adopt “secure by design” systems engineering principles. Government has shown similar priorities by omitting improved security and reduced vulnerability from both its initial planning criteria for non-classified systems and from subsequent procurement requirements.

### **3 Who really wants to win the current “arms race”?**

We consequently have a very expensive (for users) “arms race” between the developers of malware and the providers of security tools. There appear to be stronger economic incentives for software and service suppliers to compete in the provision of security add-ons rather than to co-operate in disrupting the malware development chain or in removing systemic vulnerabilities. Many users will indeed have to protect legacy systems that will never be retrofitted with, or replaced by “secure by design” systems - but others would willingly switch off features they do not currently use, in order to improve security.

This is an area of much debate and the Security Economics [www.cl.cam.ac.uk/~rja14/econsec.html](http://www.cl.cam.ac.uk/~rja14/econsec.html) website (an excellent source of material on research and debates in this space) begins by questioning whether we are spending our security budgets on the right things and whether our failures are due less to lack of resource than to perverse incentives.

The House of Lords enquiry found that “Even if fundamental redesign of the Internet is not feasible, it may still be the case that specific security issues are best addressed at the network level”. It also commented that the “*end to end principle* has become more than a practical or technological description of how the network is built”. It has become “a battle cry for Internet freedom ... to buttress arguments about the ideological impropriety of filtering Internet traffic.”

A number of its recommendations are then about encouraging the development and use of filtering software for child protection and extending this approach to cover other areas. The Law Commission, however, commented in 2002 that “notice and take-down” regimes give ISPs no incentive to check the validity of complaints. Thus a company, cult or individual which does not like a comment on a blog or website may retain lawyers who will allege that it is a breach of copyright, or defamatory and threaten legal action if it is not taken down. It is alleged that even well known ISPs will then remove material without investigating the validity of the complaint.

### **4 Filtering and Authentication**

It is also said that large scale monitoring and filtering, while very profitable to suppliers of hardware (because of the processing demands), could be more destabilising than the wider use of existing traffic authentication technologies. For nearly a decade many of the major suppliers have been researching a variety of approaches to authentication. Some of these are now widely deployed, but nearly always to serve the needs of those who will pay for them, on secure internets, with limited access from the public Internet.

Papers For The EURIM Session: Tackling Crime and Achieving Confidence in the On-Line World  
Parliament and the Internet Conference: 18 October 2007

From its very inception the Internet was a hybrid: a set of evolving protocols capable of embracing both open access academic networks and secure defence networks “designed to survive World War 3”. One consequence is not only that we have always had a multi-track and multi-tier Internet, despite the “any-to-any” image. Another is that different sub-sets of “the Internet community” have different, sometimes incompatible, views as to what is practical, let alone what is desirable. Arguments that change is impossible can be as fallacious as those which attempt to impose change on a network that is so large and complex that no-one understands how it really functions, only (at best) “their” part(s) of it.

The House of Lords concluded that “well-targeted incentives are more likely to yield results in such a dynamic industry than formal regulation”. Their consequent recommendations with regard to, for example, giving the Banks responsibility for securing on-line transactions akin to those they have for off-line (under the Bills of Exchange Act 1882), merit serious consideration - especially since current confidence appears to be based mainly on the Banks’ willingness to underwrite transactions on a voluntary basis and it is the Banks who are, in any case, driving most of the current investment in improved security.

The arguments for such an approach are rehearsed in detail in papers like “Electronic Commerce: Who Carries the Risk of Fraud?” [www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000\\_3/bohm/](http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/). It is less clear whether results will be achieved by causing the banks to issue two factor authentication to their customers, (e.g. the card readers now being issued by RBS/NatWest and others), by causing them to demand more robust browsers (like the Microsoft CardSpace project), by demanding that many more ISPs help authentic the traffic they accept from/deliver to their customers, or because “following and retrieving the money” is the best way of removing the main incentive behind criminal behaviour.

Banks have an incentive to spend money on security to prevent direct losses through fraud, protect their reputations and prevent loss of customer confidence. The last is, however, the main current driver because the cost of customers reverting to branch banking would dwarf current losses from on-line fraud. Banks have the technical ability to take on a wider role but it is unclear why they should do so, unless they understood the risks and liability involved and have a business case.

There is also “robust” debate between those who believe Internet Service Providers should be “encouraged” to provide more secure services, perhaps seeking to collect or deliver only authenticated or “clean” traffic - i.e. either scanning and authentication before acceptance from customers to put into the “Internet” and/or filtering before final delivery. ISPs are increasingly offering bundled virus and spam filtering in their offerings, but routines designed to handle e-mail could well present serious bottlenecks when faced with unlimited volumes of multi-media entertainment exchanged over peer-to-peer social networks.

The House of Lords found the positions of many players to be inconsistent. They are - but for good reasons.

It is one thing to provide authentication services for organisations willing to sign up to the protocols of IdenTrust [www.identrust.com](http://www.identrust.com) (for transactions underwritten by banks), secure transaction services like those provided by VocaLink [www.vocalink.com](http://www.vocalink.com) (for business payments) or those proposed by TWIST [www.twiststandards.org](http://www.twiststandards.org) (for supply chain transactions) or otherwise underpinned by the contractual acceptance of liability as well as responsibility, by all concerned. It is something very different to try to provide such services to those claiming crown immunity or consumer protection rights to avoid responsibility, whether for their own actions or for that which is genuinely outside their control. Moreover, the traffic transmissions of the former produce many fewer packets of data than those of the latter.

Therefore many believe it is “impossible” to move from a situation where malpractitioners can pretend to be who they wish, including by using the failure of many ISPs to authenticate the traffic they accept from their “customers”, or by abusing the “free trial” routines of the domain name registration authorities to migrate illegal or pirate websites faster than anyone can locate them and take legal action.

If that is correct, we will almost certainly see the current polarisation between secure internets and the public “Internet” continue: at least until economic forces and the research they stimulate tip the balance of argument, or the current system collapses under peaks of malware transmissions that are even higher than

the 500 times legitimate traffic envisaged by one witness to the House of Lords. It may even be that polarisation, despite (or because) of the arguments over “net neutrality” is the only practical way forward.

Meanwhile the main technology suppliers are developing new generations of encryption-based security “solutions” (including for “Identity Management” and “traffic authentication”) to sell to major users and a growing variety of malware filtering and monitoring tools to sell to ISPs and consumers.

In parallel, the growth of always on wireless based systems, from RFID chips tagged to children or patients through domestic or town centre WiFi to regional WiMax, adds a whole new dimension of risk. Is this going to be addressed at the design stage? Or will it have to be the subject of expensive systems re-engineering in ten years time, the electronic equivalent of tearing down a crime-ridden 1970s housing estate?

## **5 Current Filtering Initiatives**

There are many different types of filtering initiative using current hardware and software technologies.

At one end of the spectrum, the Internet Watch Foundation provides a dynamic list of URLs for websites containing potentially illegal child sexual abuse content to companies such as mobile and internet service providers, filtering companies and search providers that have voluntarily committed to implement a solution to block access to these URLs.

Then there is a wide range of services using automatic filters to remove traffic to or from blacklisted sources (such as the IWF list) or containing key words or patterns or according to content ratings.

There are also services which involve active monitoring by panels of volunteers (e.g. silver surfers under law enforcement supervision looking for sites and “conversations” that are illegal under US law), contractors looking for breach of copyright or court order and censors looking for that of which the local government or content regulator does not approve.

Yet more, using new techniques and technologies, are under development.

It is said that filtering is best done at the lowest possible level, ideally before traffic enters the “Internet” and that anything later is an expensive second best. That does, however, require co-operation between independent players operating under different jurisdictions around the world. Progress will not be easy save in the context of a polarisation of services that is being vigorously opposed in the name of “net neutrality”.

## **6 Current Authentication Initiatives**

### **6.1 Financial Services: Chip, Pin and other On-line Authentication Devices and Services**

“Chip and PIN” is the biggest change to the way Britons pay since decimalisation but the £1.1 billion pound UK programme is only part of a global exercise. Since 14<sup>th</sup> February 2006, those with chip and PIN cards are required to use the PIN rather than use their signature. The result is credited with halving face-to-face card fraud in the UK over the past two years, but this reduction has been balanced by the rise in card-not-present frauds, which now make up half of all card fraud, 73% of which are committed online. This has led to a dramatic increase not only in the levels of fraud online, up to £154.5m in 2006, but also the proportion, with three times as much lost online (one in £200 spent against one in 600).

A number of banks will shortly require their on-line banking customer to insert their chip and PIN card into a hand-held card-reader and key in their PIN (two factor authentication). The device will then produce a one-time-only passcode to authorise the transaction. While no technology is fool proof and “fake web-sites” can, in theory, be used in the same way as false ATM fronts to help “man-in-middle” attacks on the transaction supply chain, this is expected to tackle online banking fraud losses effectively.

Meanwhile the secure payment systems introduced by Visa [www.visaeurope.com/verified](http://www.visaeurope.com/verified) and Mastercard [www.mastercard.com/uk/securecode](http://www.mastercard.com/uk/securecode) allow cardholders to register a password for use when shopping online at participating retailers. These help address “card-not-present fraud but are vulnerable to phishing attacks to gather the necessary password details. Moreover, even security experts are unclear, after reading the small print, whether liability shifts from the bank or card operator to the individual who signs up for such a scheme. Even if this is not so, the confusion may hamper take-up.

## 6.2 General Purpose Identity Management Services

There are a great many ID management schemes competing to provide “answers” to the problems of on-line impersonation. Some of these are linked to the extension of the registers of “residents” and issue of low security “ID cards” that are common to central and local government across the world. Others are linked to national security concerns, frequent flier programmes or the facilitation of authenticated on-line transactions. Some governments, as in the UK, are attempting to link these together in common frameworks.

For the past decade the financial services industry has been transitioning the international systems that have evolved over the past millennium to the on-line world, including to do instantaneously that which previously took minutes, hours, days, months or years. But they have been trying to do so using traditional concepts of trust, dating from when The Knight Templar, who accompanied a group of pilgrims on their way from London to Jerusalem, combined the services of travel courier, American Express Card and representative of Den Norsk Veritas, removing the need to carry cash or valuables and giving personal authority for transactions with people he had never met on the basis of “shared secrets”.

The governments of today are as loath to give such power to the “private sector” as were the Kings and Popes of the Middle Ages. Hence their proposals to create a new generation of identity management services which they will expect the private sector to use and help fund: as with the National Identity Register in the UK. Given that the government services will also have to cover those unlikely ever to be conventionally credit-worthy (e.g. the homeless and socially excluded), it is debatable whether these services can ever compete on cost or efficiency with those of the private sector: where players like Experian could probably provide 90% cover, to a higher standard of performance and reliability for 10% of the cost. The other 90% of spend to reach the final 10% would, however, have to borne by government on grounds of social inclusion. At this point there are arguments as to whether spending that to support traditional channels and human intermediaries might not be more efficient.

## 6.3 Global Trust Services

The trust and transaction systems of the financial services industries have grown over recent years to embrace many/most of those willing/able to accept contractual responsibility for their actions. Thus IdenTrust (originally created to enable cross-border electronic commerce) and SWIFT (originally created to service correspondence banking), now enjoy a symbiotic relationship with each other and with organisations like VocaLink [www.vocalink.com](http://www.vocalink.com), owned collectively by the main UK banks, which not only handles the payment clearing service, including salaries, direct debits and the cash terminals on every high street, but also provides a growing range of national and international services for securely transmitting other forms of transaction information. In parallel we have alliances of the technology suppliers, like the Liberty Alliance [www.projectliberty.org/](http://www.projectliberty.org/) to provide interoperable “federated” identity standards management at the product and service level.

## 7 Information Assurance Initiatives

We hear much in the UK and Europe about the need to improve data protection and information security in the private sector, but the US President’s Identity Task Force [www.idtheft.gov/reports/StrategicPlan.pdf](http://www.idtheft.gov/reports/StrategicPlan.pdf) strategic plan begins with the need to keep **public sector** information out of the hands of criminals.

Recent revelations as to the scale and nature of tax credit and benefits fraud show that the UK public sector has similar problems to those in the US.

The challenge is summarised by the Independent Review of Government Information Assurance: see [www.cabinetoffice.gov.uk/csia/documents/ia\\_strategy/ia\\_review.pdf](http://www.cabinetoffice.gov.uk/csia/documents/ia_strategy/ia_review.pdf) for a synopsis. The UK response includes [www.cabinetoffice.gov.uk/csia/documents/ia\\_strategy/nia\\_strategy.pdf](http://www.cabinetoffice.gov.uk/csia/documents/ia_strategy/nia_strategy.pdf) "A National Information Assurance Strategy for the UK". This is owned by "The Officials Committee on Security" (Chief Information Security Officers), the "Information Assurance Policy and Programme Board" and the CIO Council. It will be driven forward by CSIA, CESG and CPNI with industry collaboration via groups such as the Crypto Developments Forum and the Information Assurance Collaboration Group.

The US strategy also includes actions with regard to keeping private sector data out of criminal hands, making it harder to misuse that data, helping victims to repair their lives and prosecuting and punishing identity thieves. A major driving force behind the private sector initiatives is the "evolution" of liability for action in the US. For example, the latest California State Assembly Bill (779 [www.out-law.com/page-8476](http://www.out-law.com/page-8476)) extends the duties to report data breaches under the previous SB1316. Those who collect card payment data from their customers are now required to use encryption and security protocols, delete sensitive authentication information and add access controls to what is held. They are also liable to the owner or licensee of compromised information "for the reimbursement of all reasonable and actual costs of providing notice to consumers ... and for the reasonable and actual cost of card replacement ..."

If the Bill is signed by the Governor, said to be a formality because of the support it has, this will come into force on 1<sup>st</sup> July 2008 to give retailers the time necessary to implement the required security controls. Given that other states are likely to follow the Californian lead, this is likely to give a major fillip to attempts to greatly improve information assurance in the private sector.

In the light of the recommendations from the House of Lords, Intellect [www.intellectuk.org](http://www.intellectuk.org) is planning a working group to provide the UK government with "the industry's view" on "an effective Data Breach Notification requirement (from measuring the problem and improving security to centralised reporting structure)".

## **8 Where are the issues debated ?**

The Jill Dando Institute of Crime Science [www.jdi.ucl.ac.uk](http://www.jdi.ucl.ac.uk) claims to be the world's first organisation devoted specifically to crime reduction. It does this through teaching, research, public policy analysis and by the dissemination of evidence-based information on crime reduction. It has a formidable network of contacts throughout the world but has left e-Crime to the Cybersecurity Knowledge Transfer Network [www.ktn.qinetiq-tim.net](http://www.ktn.qinetiq-tim.net). This claims to be "a single focal point for UK Cyber Security Expertise" and was created to follow up the Foresight Cyber Security Programme, helping target UK research and development by identifying the needs of the future and ensuring that these were addressed and the results were transferred to the benefit of the UK economy as whole. To do this, it uses advisory panels drawn from public and private sector users, suppliers and law enforcement. It is also in the process of upgrading its consultation and dissemination networks.

The "Light Blue Touchpaper" [www.lightbluetouchpaper.org](http://www.lightbluetouchpaper.org) blog and seminar series of the Cambridge University Computer Laboratory's Security Group and the Cambridge-based global Security Economics group [www.cl.cam.ac.uk/~rja14/econsec.html](http://www.cl.cam.ac.uk/~rja14/econsec.html) are among the other forums for wide ranging policy debate as opposed to research networking (or which there are many more). Then there are the many groups addressing specific issues such as Identity Management and Authentication technologies and standards, Information Assurance (variously defined), Data Protection, Encryption technologies and policies and so on.