The Foundation for Information Policy Research

Consultation response on

Personal Internet Security

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

Background

The hard information security problems nowadays mostly span technology and policy. Security failures are often due to misplaced incentives; when the people guarding a system are not the people who suffer when it fails, then one may expect less than the socially optimum level of diligence. There are many relevant examples.

1. Mass-market software vendors have so far managed to disclaim almost all liability for security vulnerabilities; thus whenever a trade-off has to be made between security and ease of use, or between security and easy programmability, security tends to be neglected. So far they have got away with telling their customers to 'buy a firewall' or 'buy antivirus software'.
2. People whose PCs become badly infected with viruses or spyware often just buy a new PC, rather than having the old one cleaned up. This may make shops less eager to sell PCs with up-to-date software and prudent defaults; aftermarket sales of antivirus products give them a further perverse incentive. Software vendors benefit too when users upgrade or replace systems early.
3. The security of electronic payment systems depends critically on the banks who set standards and police merchants. The banking industry takes a large slice of the value of Internet business via their charges to merchants; yet UK banks are finding many ways to dump fraud risk on merchants and customers.

Globalisation matters. The Internet enables UK consumers to transact with merchants in countries with inadequate law enforcement. Such protection as they have comes through the credit card system; they can charge back goods paid for but not satisfactorily delivered. Yet the technical mechanisms – from online banking through auctions to shopping websites – evolved mainly for US markets, where consumers have significantly higher protection than in the UK. If the UK drifts too far away from US norms, then the resulting 'trust gap' may create serious disadvantages for Britain's online businesses. Parliament should bring UK consumer protection up to US levels – and this means financial services as well as PCs and software.

Since FIPR was founded in 1998, we have been bringing technologists together with lawyers and economists to think about these issues. The collaboration between economists and information security experts has been particularly fruitful, leading to the birth of a new discipline of 'Information Security Economics,' which now has perhaps a hundred active researchers. We refer committee members to the online proceedings of the Workshop on the Economics of Information Security (WEIS), which has been held annually since 2002, and to the Economics and Security Resource Page maintained by Ross Anderson, the chair of FIPR[1].

Collaborative work between technologists and lawyers is also important; just as economics can help analyse the theoretical allocation of risks, so law deals with their practical allocation. An early study by members of FIPR's Advisory Council showed that when introducing online banking to the UK, many financial institutions designed their terms and conditions so that the customer became liable for fraud[2].

It is timely for Parliament to consider this topic. While ten years ago both security and policy people dealt in terms of what might go wrong with the Internet, enough people have been using it for long enough that we are starting to have good data on what actually does go wrong. Also, thanks to the last few years' research in security economics, we have some practical ideas on what policymakers could do about it.

Answers to specific questions

Defining the problem

• What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

As people rely on the Internet for more, so the exposure will increase. When it was only used for personal and professional communication (say in 1990) the risk was low, being largely limited to defamation, embarrassment and perhaps plagiarism. Now that most people use it for shopping and banking, fraud is a growing problem. Once people start to rely on it for safety-critical services (e.g. remotely-hosted medical-records systems), failures will be able to threaten human life directly.

The last five years have seen a shift from 'nuisance' threats such as computer viruses written by teenagers to show off, to fraud and other exploits designed to make money. Virus writers nowadays do not attempt to crash millions of machines, but rather to install spyware on a few hundred thousand, or to take over a few thousand for sending spam. The criminals are now specializing – rather than one-man crime operations, we see malware writers, money launderers, phishermen and so on trading with each other.

---

[1] See http://www.cl.cam.ac.uk/~rja14/econsec.html

[2] 'Electronic Commerce: Who Carries the Risk of Fraud?' N Bohm, I Brown, B Gladman, Journal of Information, Law and Technology 2000 (3), at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/

• What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

Reporting and measurement are a serious problem in the UK. Many US states, starting with California, have introduced security breach disclosure laws, whereby a company suffering a security failure must notify all potentially affected data subjects. In the UK, however, a company whose systems have been compromised has every incentive to keep quiet about it, and will probably receive legal advice against notifying affected individuals. Even in egregious cases – such as when a bank discovers a 'skimmer' attached to an ATM – the potentially affected customers are not directly notified. In less clear-cut cases, such as when a webserver that was carelessly designed to retain customer credit-card data might (or might not) have been hacked, there is no prospect of notification. Thus security breaches affecting the individual are typically detected when the individual complains of fraud. Such complaints are often met with hostility or denial by financial institutions, or with a demand that the customer explain how the dispute might have arisen. Without breach notification, this can be an unmeetable burden of proof. As a side-effect, we have no really dependable statistics.

• How well do users understand the nature of the threat?

Their understanding appears to be variable: short-term risks such as fraudulent transactions are understood better than long-term privacy risks.

Tackling the problem

• What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

The UK government can make one or two specific interventions; for example, it might require new PCs to be sold with a 'best before' date indicating the update status of the installed software. However, the main thing government can do is to align the incentives better. Here the most important single change would be an upgrade to banking regulation to bring the UK into line with the US 'Regulation E' which governs electronic banking. This would unambiguously place the liability for fraudulent transactions back with the banks, as it has been from time immemorial: the common-law rule, codified in S24 of the Bills of Exchange Act 1882, was that a forged manuscript signature on a cheque was null and void – a rule that could not be altered by the bank's terms and conditions.

• What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

We would caution the committee against endorsing the industry line that 'user education' is the solution to Internet security problems. For an industry to produce insecure products, and then expect government not merely to excuse them from liability but to spend public funds advising citizens to buy anti-virus software, is breathtaking. It

combines liability dumping by the platform vendors with free advertising for the antivirus firms. Instead, Parliament should enact a security breach disclosure law as in California.

• What factors may prevent private individuals from following appropriate security practices?

The typical computer user can do little to identify or mitigate technical risks. He buys a computer as a consumer electronic appliance, plugs it in and uses it; attempts to turn up the 'security level' of his browser will cause some web sites to not work; he has no way of telling good security software from bad; and many of the problems are completely outside the control of even technically sophisticated users. Much of the advice on offer to the naïve user is also dubious. For example, users are often advised to turn on encryption on their home wireless LANs; yet when this issue was polled at WEIS 2006, a majority of delegates (and a large majority of technical security experts) publicly indicated that they do not use encryption. Experts also disregard the universal advice to change passwords frequently, as this leads to weak passwords.

• What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

In markets with network externalities, companies generally design products with too little security at first so as to build market share by appealing to complementers. If they succeed in becoming the dominant firm in their market, they may then add excessive security in an attempt to lock in their customers more tightly. In competitive markets, especially with complex value chains, firms typically try to dump risks – for example by telling their customers to buy third-party security products such as firewalls.

• Who should be responsible for ensuring effective protection from current and emerging threats?

As with risk management in general, there is a role for the state via criminal law, and a role for private action via tort litigation and insurance markets – where the state acts as rulemaker, regulator and operator of the court system. A critical difference is the speed with which online behaviour is still evolving; there are significant changes year-on-year in patterns of fraud and abuse, which create problems for Parliament with its much slower legislative cycle. Micromanagement by government will be impractical – another reason why Parliament should focus on getting the broad incentives right.

• What is the standing of UK research in this area?

About half the research in information security, and most of the work in information security economics, is done in the USA. However there is a strong research team at Cambridge, which does security engineering and helped found the discipline of information security economics; there are also research groups at Oxford (theory and protocols), Royal Holloway (mathematics of codes and ciphers), Newcastle (dependability and security usability) and the LSE (security management).

Governance and regulation

• How effective are initiatives on IT governance in reducing security threats?

Government initiatives have mostly been ineffective – the security agencies have if anything exacerbated the problem, as their institutional incentives lead them to focus on the offensive rather than the defensive side of information warfare. Private initiatives can have some effect, in that well-managed companies are generally at lower risk of information security compromise.

• How far do improvements in governance and regulation depend on international co-operation?

So far the main improvements have come about from action by ISPs. Countries that were a disproportionate source of spam have in the past had their email traffic blocked. Any international agreement that prevented this (as the Nairobi convention would in the case of voice telephony) could have serious effects.

• Is the regulatory framework for Internet services adequate?

It has been barely adequate up till now – although there have been many tussles over telecoms regulation, law enforcement access and so on. Unfortunately the direction of government policymaking post-9/11 appears to be drifting in the direction of more censorship and surveillance, rather than doing things that might be useful to users.

• What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

These are mostly economic rather than technical. The biggest single standards issue is the anticompetitive behaviour associated with the 'Trusted Computing' initiative. If the liability lay unequivocally with the parties in control of system design, much more progress would be made. Some is being made; after all, banks can only dump some of their fraud risk on customers. For example, one online bank is introducing a one-day delay plus SMS notification whenever a customer appears to order a payment to a new beneficiary. But this is not rocket science; payee nomination was a feature of the UK's first electronic banking service, introduced by the Bank of Scotland in the early 1980s.

Crime prevention

• How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

Computer crime has always been poorly handled by the police in Britain: current targets make it a low operational priority, and the routine rotation of officers through specialist units has made it hard for local forces to build and maintain a capability. More recently,

the absorption of the NHTCU into SOCA has left a gap in the coverage of level 2 computer crime (which is most of it), and the proposed mainstreaming of computer offences may dump us back to where we were before the NHTCU was set up. Mainstreaming is good in principle, as most white-collar crimes have a computer component nowadays – a technophobic detective will soon be as disadvantaged as a detective who cannot drive. However there are significant resource / priority issues, both at the sharp end of operational training and at the back end of computer forensics. Overall, we would expect better performance if the Government were to give police forces a public set of priorities, rather than trying to micromanage them using targets.

- Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

More or less – the issue is not so much the law as its enforcement. Even level 2 crimes are not anybody's priority at present, and no real effort at all is being made on the spam and spyware that cost users (and industry) many billions in wasted time and resources. Even a small push here might have dramatic results. We suggest making it clear that companies who use spam or spyware as a marketing tool are breaking the law, and cannot just blame the marketing agencies they employ. A single prosecution of a blue-chip company CEO could have a massively beneficial effect on the digital ecology.

- How effectively does the UK participate in international actions on cyber-crime?

These are not very effective at present. The UK is weak on security disclosure and consumer rights, while the US is erratic on enforcement. About half of all child porn websites seem to be hosted in the USA; most spyware appears to be operated on behalf of US companies; and US plans to interfere with credit-card payments to online gaming sites may unleash unregulated payment mechanisms on the world – an online rerun of Prohibition. We should try to get the best of both worlds, rather than the worst of both.

Conclusion

UK citizens suffer significant harm as a result of Internet security failures, which are largely due to misaligned incentives. At present the harm is largely limited to online fraud, but as more and more devices become programmable and acquire the ability to communicate, the potential for harm will spread. As more safety-critical systems come to rely on the Internet, security vulnerabilities are starting to turn into hazards.

Government cannot micromanage the information security business, most of which is in any case outside the UK. What it can do, and should do, is to ensure that people and companies have the necessary incentives to take responsibility for the consequences of their actions, online as well as offline.

Ross Anderson
Cambridge, 23 October 2006