SCRIPT-ed

*Volume 4, Issue 1, March 2007*

# The internet and security: do we need a man with a red flag walking in front of every computer?

*Lilian Edwards*[1]

Internet security is big news. According to the latest National Opinion Poll, as of January 2007, almost half of UK citizens still harbour a "deep mistrust" of the Internet due to security concerns[2]. The House of Lords Select Committee on Science and Technology, meanwhile, is currently orchestrating a major enquiry into personal Internet security[3]. Their Lordships observed wisely that "*With the ever growing use of home computers, the spread of broadband, and the rise in internet banking and commerce the importance of proper internet security measures has never been greater*.**"** Issues highlighted include:

- What is the nature of the security threat to private individuals and what is the scale of the problem?
- How well do the public understand the nature of the threat they face?

---

[1] Professor of Internet Law, University of Southampton; Director, *iLAWs*; Associate Director, AHRC Centre for Research into Intellectual Property and Technology.
[2] <*http://www.vnunet.com/vnunet/news/2169264/uk-adults-harbour-deep-mistrust*>
[3] Announced on July 2006 – see press release at <*http://www.parliament.uk/parliamentary_committees/lords_press_notices/pn280706st.cfm*>

- What can be done to provide greater personal internet security? How much does this depend on software and hardware manufacturers?
- Is the regulatory framework for internet services adequate?
- How well equipped is Government to combat cyber crime? Is the legislative framework in UK criminal law adequate to meet this growing challenge?

Response to the consultation has been extensive[4], and the Lords Select Committee has been hearing evidence since consultation closed in October 2006, from parties as varied as the Internet Service Providers Association, Richard Clayton of the Cambridge Security Lab, John Carr of the Children's Charities' Coalition on Internet Safety, Jonathan Zittrain of the Oxford Internet Institute and many speakers from commercial bodies such as eBay, as well as the ICO, OFT and DTI. It will be very interesting to see what emerges, as advertised, in early summer 2007.

Meanwhile the EC has been more concerned with the public aspects of cyber security. In the last few years we have seen a rash of communications from them on topics such as information system security, critical infrastructure protection and denial of service attacks. ENISA, the European information Security Agency established in 2004[5] is becoming increasingly active. The 2006 "Strategy for a Secure Information Society"[6] highlighted a number of key challenges:

- Attacks on information systems were increasingly motivated by profit not for "kicks"
- Increasing use of mobile communications had opened new widespread areas of insecurity
- Ambient intelligence e.g. RFID or "the Internet of things" created significant new privacy and insecurity risks
- The ICT sector was becoming more and more crucial to the EU economy and therefore more and more vulnerably tempting to attack, and the more crippling if attacks were mounted
- Non ICT critical infrastructure – e.g. transport, energy, hospitals - was increasingly dependent on ICT connectivity
- Despite all this, the threat posed by cyber-insecurity was still not taken seriously by most businesses and citizens in Europe.

Unsurprisingly, this damning summary was followed quickly by a Programme and a Draft Directive on Critical Infrastructure Protection announced at the end of 2006[7]. Apocalyptically, the EU opined that,

---

[4] Evidence, oral and written can be viewed at <*http://www.parliament.uk/parliamentary_committees/lords_s_t_select/Evidence1.cfm*>

[5] See Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency <*http://enisa.europa.eu/pages/01_05.htm*>

[6] A strategy for a secure information society – "Dialogue, partnership and empowerment," Brussels COM (2006) 251.

[7] <*http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0787en01.pdf* >

> *The security and economy of the European Union as well as the well-being of its citizens depends on certain infrastructure and the services they provide. The destruction or disruption of infrastructure providing key services could entail the loss of lives, the loss of property, a collapse of public confidence and moral in the EU.*[8]

At root here, of course, is the fear not of simple hacking by domestic criminals or bored teens, nor even of blackmail by gangs of Estonian extortionists, but, in the post 9/11 world, of serious terrorist activity directed at nuclear plants, hospitals, automated transport, air traffic control, banking systems and domain name servers: the catalogue of possible targets is endless. Accordingly, the Draft Directive proposes the designation of a European Critical Infrastructure which will receive special protection and attention. The Appendix blandly designates "The Internet" in its entirety as part of this ECI. When and if the Directive passes, it will be fascinating to see how the fairly onerous responsibilities of the Directive – e.g. the creation and implementation of an Operator Security Plan - can be applied to every part of the Internet, including small one man ISPs and universities, etc. – but that is a problem for later.

For now, the point of this editorial is that, in the realm of Internet security, the personal is also the public (an adaptation of the old feminist adage that the personal is political?) and that the two cannot, and should not, be separated if we are to attain the nirvana of a safe and secure critical infrastructure and Internet. Nor can consideration of personal security and privacy *threats* to consumers, usefully be separated from the home security *practices* of those same individuals. In previous work on spam and denial of service[9], I have pointed out that most mal-doing on the Internet is now orchestrated via unknowing networks of thousands if not millions of "zombie" or "bot" computers. Such computers are typically home consumer machines, attached to "always on" broadband facilities, which have been infected by viruses or other types of software so that unknown to their legitimate owner, and usually without degradation of their ordinary capabilities, they perform the bidding of a "zombie master". (Since the UK is in the forefront of consumer broadband uptake, impressively we lead the world in having the highest zombie population per capita.) Hacking, denial of service, virus dissemination, theft of personal data, spamming, key-logging, click fraud, ID fraud and other cyber exploits are all now almost wholly orchestrated via such zombie networks.

Why? A number of reasons. For exploits such as denial of service, superior fire power is needed to knock down the servers of (say) a bank or a major corporation – hence DoS becomes *distributed* denial of service. The activity of zombies is almost untraceable back to the actual criminal masterminds, the zombie masters (or their paymasters). Criminal activity can be handled remotely by botnets while the zombie masters stay safely at home in safe havens like parts of the Former Soviet Union. And making or acquiring zombies is child's play nowadays: botnets can be bought for

---

[8] See press release at <*http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/477&format=HTML&aged=0&language=EN&guiLanguage=en*>

[99] L Edwards, "Dawn of the Death of Distributed Denial of Service: How to Kill Zombies" (2006) 24 *Cardozo Arts & Entertainment Law Journal* 1 23.

remarkably low prices, and zombie-making virus kits are readily available on the net. Technical knowledge is thus no longer necessary, and zombie networks are simply becoming another tool of the international criminal and gangster (and terrorist?) fraternity. In the networked, broadband world we live in, in the UK in 2007, it is hard to believe, but probably accurate, that around half of the computers of people we know and like have been co-opted as zombies to do cyber-wrongs.

What are we to do about this? Grand plans to safeguard Critical Infrastructure are clearly important, but they are, to some extent, a case of safeguarding the stable after the horses have become zombies. Would it not be better to plan to make a more secure Internet from now on, as well as to put resources into fortifying our airports and power plants from attacks from the insecure Internet we have currently created? Criminal law is also a rather blunt and expensive tool with which to attack this threat. Criminal cross-border investigations may catch a few zombie masters and international hackers, but the resources needed are vast and the rewards few. Arguably, updating and enforcing cyber-criminal law (one goal specifically mentioned by the HL enquiry above) is something of a red herring; an administrative, regulatory or technical solution might work better to produce a safer Net first, and then we can worry about catching and punishing the actual wrongdoers, safe behind territorial and technical anonymity, later.

In my work on denial of service published in 2006[10], I argued that "security was for everyone, not just for Christmas". What does this mean? Catching and prosecuting zombie masters is the hardest and least useful part of the puzzle to solve. Instead, we can more helpfully look elsewhere for aid. For a start, we could ask the software writers to write better software, with fewer vulnerabilities, and therefore less need for frequent patching and updating to plug exploitable holes. (A tall order, says the software industry, but one that needs tackled sooner rather than later.) We could ask industry and the public sector to make sure their machines run up to date, patched software, and perhaps that they show a preference for open source software which is often more secure and less prone to attack than some ubiquitous proprietary software. We could ask ISPs to scan the data traffic going to and from computers attached to their networks for unusual patterns of traffic, and then to cut those likely zombies off from the Internet until they can be de-zombified. We could even ask then to take on remote patching and updating of the operating systems and software on consumer machines, though this has multiple problems, of cost, liability, autonomy and consumer choice. It would however get round the problem of consumer ignorance and inertia as to computer security. We could alternately, as the EU and the government have both repeatedly suggested, try to educate consumers in "safe software": to use virus checkers, adware and spyware blockers, and firewalls conscientiously. But will we succeed? At least two generations of Internet users still exist in the UK alone to whom a computer is as much an inscrutable black box as their car or their TV. (And, it should be remembered, computers get more complex every day, while TVs have arguably become relatively simple, at least in interface). They do not want to fiddle with their PCs and Macs, to take the back off, or to get under the hood. They do not have the knowledge, the skills or, usually the incentive (zombified machines work fine, the threat posed is to others) and in some cases, they are actively scared of getting their "hands dirty". (I always cite my own mother here, who thinks she can single-handedly break the Internet.) Until the computer-savvy twenty-something

[10] Id.

generation rules the world, we may have to think again about an interim solution to cope with domestic machines, zombies and computer insecurity.

Let us think about cars. When automobiles arrived on the scene, they were clearly inherently dangerous objects. They went too fast, were driven badly by ignorant, uneducated owners and scared the horses. Naturally a man was instructed to walk in front of them with a red flag and they were restricted to an anecdotal 5 mph.

Today cars go far, far faster (but are, admittedly, a lot lot safer) but are still inherently dangerous objects. They are driven by people who, just as in the 19th century, largely do not understand how their car works, and have no idea how to maintain it in a state of safety. How do we as a society manage the risks of dangerous cars and consumer ignorance?

Well, in several ways. There is of course the criminal law; we know we are not allowed to drink and drive, or to drive dangerously without possibility of penalty. But this is not really the main way in which "car insecurity" is controlled. There are instead a number of regulatory and administrative means, far more effective than criminal law, which keep our roads, to a reasonably large extent, safe. You cannot, for a start, drive a car without a license. That implies a certain degree of education and knowledge of the rules of the road. You cannot drive without insurance. That means that if you do cause damage to someone else due to your insecurity they are at least always compensated. Both the license and the insurance systems are enforced, cleverly, not (in the main) by resource intensive police checks, but by the requirement that both be displayed to obtain a tax disc: and the tax disc system combined with a national car registration database allows for effective checking of who is properly "secured" by an automated computer system. Policing such a system then becomes relatively trivial.

Can we learn from this for computer insecurity, with reference to consumers and zombies? Perhaps, perhaps not. It is clearly impossible, practically, politically and ethically, to require every consumer – including the ignorant, the poor and my mum – to be legally responsible for keeping their computer in a state of reasonable security. We can try and educate them but we probably cannot impose a "computer driving license". But perhaps we can allow them to offload that responsibility, as we do with cars. Cars in the UK are safe in part because after a certain age they have to be checked over by a responsible garage and certified as fit for the road. Without such an "MOT", again, a tax disc cannot be obtained. Again, we cannot probably reasonably demand that home owners have their computers checked over as safe by a travelling "computer MOT man" – the issues of invasion of privacy, surveillance and inertia are too great, and, anyway, one day after the MOT man had been round the computer would be hit by a new virus. But we could present a number of alternatives.

Suppose a basic obligation is placed on every networked computer owner to keep that computer reasonably secure. This obligation could be met by:

- *Self vigilance*. This is fine for the commercial and public sector where resources such as IT departments exist to keep computers safe. It is also fine for home computer owners who feel capable of keeping their own machines secure ("geeks" as they are known in the trade). Alternately, for the vast majority of individuals (and small businesses?) who do not have computer skills, another option would be:

- *Subscribing to an ISP who undertakes security measures for you.* Such services are already beginning to be available on the market at reasonable rates. Nildram[11] e.g., offer a range of industry level secure ISP services to consumers. A legal obligation of security on consumers which could be met by signing up to an accredited secure ISP service would quickly inspire a competitive market of "safe ISPs". Exactly what the ISP would have to offer would have to be worked out and supervised – patching, updating, scanning, closing of ports, remote operation of virus checkers and firewalls? Model "safe ISP" contracts could perhaps be drafted, drawn up in collaboration between the ISP and the DTI, and then kitemarked. The strength of this suggestion is that ISPs are being asked to provide a business service at market rates; not to take on a role as guardians of the Internet for free, which there is no reasonable case for imposing on them.
- *Insurance.* In this system, every consumer should also be asked to take on cybersecurity insurance. Currently this is a very fledgling market, but a legal obligation would immediately create a competitive market. If an individual breached their obligation of reasonable security – e.g. by choosing option 1 of self vigilance and failing to keep their computer adequately patched – then at least insurance would be available to pay towards damage caused to third parties. This should also provide an incentive not to choose option 1 out of inertia as the result of calling on cyber-insurance would be that the cost of the next premium should rise considerably. (Problems might arise with causality and share of blame – if a network of 10,000 bots attacks IBM, what is the responsibility of one zombie? -but these could be overcome if insurance pay-outs were made into a general pot out of which compensation was paid to victims. Clearly, there is a lot of detail to be filled in here.)

This is just one back of an envelope scheme, which seeks to use (primarily) administrative rather than criminal law to regulate cyber-insecurity; there could be others. But the underlying message is to ask both the Select Committee and the EC to think about ways of securing home user computers as well as critical infrastructure; to try to create a safer Internet *ab initio*, not just try to deal with the consequences of an unsafe one. To reshape slightly another old aphorism, in this domain, security really does begin at home.

DOI: 10.2966/scrip.040107.1



[11] <*http://www.nildram.net/*>