“Security Economics” and “Network Security”

E-Crime and Opportunities

E-COPP 2008

20th November 2008, Loughborough, UK.

Richard Clayton

richard.clayton@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Economics and Security

- Over the last six years or so, we have started to apply an economic analysis to information security issues, creating the new field of “Security Economics”
- Economic analysis often addresses the underlying causes of security failures within a system, whereas a technical analysis will merely identify the mechanism!
- Tackling the problems in economic terms can lead to valuable insights as to how to create permanent fixes
- Meanwhile, the trend is for information security mechanisms (such as cryptographic protocols) to be used to support business models rather than to manage risk

“Security Economics and European Policy”

- ENISA commissioned a report from us (Prof. Ross Anderson, Rainer Böhme, Dr Richard Clayton, Dr Tyler Moore) “analysing barriers and incentives” for security in “the internal market for e-communication”. It was published in February 2008
  - 114 pages, 139 references, 15 recommendations
  - This audience should read the whole thing! It contains much about security economics & valuable discussions of topics that did not merit a recommendation (such as “cyber-insurance”)
  - If time-challenged there’s an executive summary! or a 62 page version published at WEIS 2008 (less literature review since that audience would know it); or a 20 page version at ISSE
- Much favourable comment thereafter
- The recommendations are for policy initiatives that require harmonisation (or at least EU-wide coordination)

What Data do we Need ?

- Individual crime victims often have difficulty finding out who's to blame and getting redress
  - people who use ATMs fitted with skimmers are notified directly in the USA but via the media in the EU (if at all)
  - if you don't know you were attacked how can you take precautions?
- US security-breach notification laws now widespread
  - studies say no apparent impact on ID theft, but can impact share prices, and (anecdotally) increases profile of Chief Security Officer
- **RECOMMENDATION #1** Enact an EU-wide comprehensive security-breach notification law
- **RECOMMENDATION #2** We recommend that the Commission (or the European Central Bank) regulate to ensure the publication of robust loss statistics for electronic crime

How Can We Clean Up the Internet ?

- Botnets distributing malware, sending spam, and hosting phishing web pages pervade the Internet
- Some ISPs are better at detecting and cleaning up abuse than others. Badly run big ISPs are a particular (and common) issue (e.g. small ISPs find their email blocked out of hand; this is more uncommon for large ISPs because of network effects)
- Internet security is increasingly down to the “weakest link”, as attackers target the least responsive ISPs’ customers
- This is well-known in the industry, but we need the numbers
- **RECOMMENDATION #3** We recommend that ENISA collect and publish data about the quantity of spam and other bad traffic emitted by European ISPs

Data Collection is Not Enough

- Publishing reliable data on bad traffic emanating from ISPs is only a first step – it doesn't actually fix anything
- Internet security also suffers from negative externalities
- Modern malware harms others far more than its host: botnet machines send spam and do all the other bad things, but the malware doesn't usually trash the disk and may try to avoid over-use of bandwidth or processing cycles
- ISPs find quarantine and clean-up expensive (an interaction between customer and helpdesk costs more than the profit from that customer for months to come)
- ISPs are not harmed much by insecure customers since it's just a bit more traffic and a handful of complaints to process

Options for Overcoming Externalities

#1 Self-regulation, reputation etc (hasn’t worked so far)

#2 Tax on “digital pollution” (likely to be vehemently opposed)

#3 Cap-and-trade system (dirty ISPs would purchase “emission permits” from clean ones)

#4 Joint legal liability of ISP with user

#5 Fixed-penalty scheme (cf EU rules on overbooked aircraft)

- **RECOMMENDATION #4** We recommend that the EU introduce a statutory scale of against ISPs that do not respond promptly to requests for the removal of infected machines, coupled with a right for users to have disconnected machines reconnected by assuming full liability
- It’s controversial! but what should be done instead?

Liability Misallocation

- Software vendors use contracts to disclaim all possible liability
  - Many calls for this to change, as civilization ever more dependent on software; e.g. House of Lords suggested punishing negligence
  - Clearly not a policy that can be adopted in a single member state
- Intervention may be necessary to deal with market failures such as monopolies, and for ensuring consumer protection
  - consider example of using a GPS navigator and getting stuck on a country lane: is the map or the routeing algorithm at fault? Is what has failed a product or a service? Is it a consumer or a business?
- Too hard to do in one go! So need a long-term vision:
  - leave standalone embedded systems to safety legislation, product liability and consumer regulation
  - with networked systems, start by preventing harm to others
  - relentlessly reallocate slices of liability to promote best practice

Beginning to Tackle Software Liability

- **RECOMMENDATION #5** We recommend that the EU develop and enforce standards for network-connected equipment to be secure by default
- **RECOMMENDATION #6** We recommend that the EU adopt a combination of early responsible vulnerability disclosure and vendor liability for unpatched software to speed the patch-development cycle
- **RECOMMENDATION #7** We recommend security patches be offered for free, and that patches be kept separate from feature updates

Consumer Liability Issues

- Network insecurity causes privacy failures and service failures but the main effect on consumers is financial
- There is wide variation in the handling of customer complaints of fraudulent eBanking transactions (UK, DE the worst)
- eCommerce depends on financial intermediaries managing risk, but individual banks will try to externalize this
- The Payment Services Directive fudged the issue – and so this needs to be revisited
- **RECOMMENDATION #8** The European Union should harmonize procedures for the resolution of disputes between customers and payment services providers over electronic transactions

Abusive Online Practices

- Spyware violates many EU laws, yet continues to proliferate
- Going after the advertisers may work
  - c.f. UK’s “Marine Broadcasting Offences Act 1967”
- EU Directive on Privacy and Electronic Communications (2002) included an optional business exemption for spam, which has undermined its enforcement
- **RECOMMENDATION #9** The European Commission should prepare a proposal for a Directive establishing a coherent regime of proportionate and effective sanctions against abusive online marketers

Consumer Protection

- Consumers can buy goods in any EU country, so although jeans can cost less in Sofia than London, entrepreneurs can ship them to London and make a buck. However, it gets messy when one considers trade-marks, and messier still – challenging the Single Market principle itself – when considering the bundling of physical goods and online services
- It’s hard to open a bank-account in another country (because of the way credit-referencing is bundled up to sell to banks). This means you can’t put pressure on uncompetitive banks by switching your business abroad
- **RECOMMENDATION #10** ENISA should conduct research, coordinated with affected stakeholders and the European Commission, to study what changes are needed to consumer-protection law as commerce moves online

Lack of Diversity

- Failure to have logical diversity makes physical diversity irrelevant – attacks work “everywhere”. This affects risk (and has a big impact on insurance as a solution)
- Unfortunately all the economic pressures are towards dominant suppliers, but at the very least Governments should be avoiding making things any worse
- **RECOMMENDATION 11:** ENISA should advise the competition authorities whenever diversity has security implications
- **RECOMMENDATION 12:** ENISA should sponsor research to better understand the effects of IXP failures. We also recommend they work with telecomms regulators to insist on best practice in IXP peering resilience
  - NB: IXPs have been rather critical of what they think this says!

Criminal Law

- Most crimes on the Internet don’t need special laws (death threats, extortion &c) “If it’s illegal offline, it’s illegal online”
- But have had to extend “trespass” to deal with computer hacking; and useful to have special laws for computer “viruses”
- Advent of the Internet means need for laws on denial of service (where network is the target) and possessing/distributing attack tools (“without right” – since most are dual use)
- Approach has been to try and harmonise laws (and penalties)
- BUT real problem isn’t laws but enforcement across borders
  - c.f. bank robbers who fled across US state lines, dealt with by making bank robbery (etc) into Federal offences – but this only worked because of the existence of the FBI

Fragmented Laws & Policing

- **RECOMMENDATION 13:** We recommend that the European Commission put immediate pressure on the 15 Member States that have yet to ratify the Cybercrime Convention
- **RECOMMENDATION 14:** We recommend the establishment of a EU-wide body charged with facilitating international cooperation on cyber-crime, using NATO as a model

… and finally, a slightly self-interested recommendation, noting problematic legislation on crypto products and dual-use tools:

- **RECOMMENDATION 15:** We recommend that ENISA champion the interests of the information security sector within the Commission to ensure that regulations introduced for other purposes do not inadvertently harm researchers and firms

More..

ENISA Report (and comments)

http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm

Economics and Security Resource Page

http://www.cl.cam.ac.uk/~rja14/econsec.html

Cambridge Security Group Blog

http://www.lightbluetouchpaper.org

UNIVERSITY OF CAMBRIDGE
Computer Laboratory