

# “Security Economics” and “Network Security”

Richard Clayton

`richard.clayton@cl.cam.ac.uk`

LSEC Information Security Economics 2008  
Leuven, Belgium, 8th September 2008



**UNIVERSITY OF  
CAMBRIDGE**  
Computer Laboratory

# Outline

---

- Security economics
  - A powerful way of looking at overall system security
  - New uses of security mechanisms
  - IT economics
- ENISA Report: “Security Economics and European Policy”
  - Information asymmetry
  - Externalities
  - Liability regimes
  - The role of ISPs and IXPs
  - Consumer protection
  - Diversity
  - Policing

# Economics and Security

---

- Over the last six years or so, we have started to apply an economic analysis to information security issues
- Economic analysis often addresses the underlying causes of security failures within a system, whereas a technical analysis will merely identify the mechanism!
- Tackling the problem in economic terms can lead to valuable insights as to how to create permanent fixes
- Clearly shows that consumers need access to better information so they can make informed decisions about security
- Meanwhile, the trend is for information security mechanisms (such as cryptographic protocols) to be used to support business models rather than to manage risk

# Traditional View of Information Security

---

- People used to think that the reason that the Internet was insecure because of lack of features or that there was not enough crypto / authentication / filtering
- If only people had a proper checklist of security issues to tackle then we would all be more secure
- So engineers worked on providing better, cheaper, (and even occasionally easy-to-use) security features – developing secure building blocks such as SHA-1, AES, PKI, firewalls...
- About 1999, we started to realize that this is not enough

# Using Economics to Explain Security

---

- Electronic banking: UK banks were less liable for fraud than US banks, so they got careless and ended up suffering more fraud and error. The economists call this a “moral hazard”
- Distributed denial of service: viruses no longer attack the infected machine but they use it to attack others. Why should customers spend \$20 on anti-virus software when it isn't their data that is trashed? Economists call this an “externality”
- Health records: hospitals, not patients, buy IT systems, so they protect the hospitals' interests rather than patient privacy. These are “incentive” and “liability” failures

and

- Why is Microsoft software so insecure, despite its market dominance? The economists can explain this as well!

# New Uses of Security Mechanisms

---

- Xerox started using authentication in ink cartridges to tie them to the printer
  - followed by HP, Lexmark. . . and Lexmark's case against SCC
  - note that the profit is in the consumables – purchasers compare ticket price rather than total cost of ownership
- Accessory control now spreading to more and more industries
  - games, mobile phones, cars...
- Digital rights management (TPMs): Apple grabs control of music downloads, Microsoft accused of trying to control distribution of HD video content...
- Encryption is being used to tackle the obvious contradiction between the decentralization of network intelligence and the operators desire to retain control

# The New View of Information Security

---

- Systems are commonly insecure because the people who could fix them have a limited incentive to do so
  - bank customers suffer when poorly-designed bank systems make fraud and phishing easier
  - patients suffer when hospital systems put administrators' convenience before patient privacy
  - casino websites suffer when infected PCs attack them
- In these scenarios security has become what economists call an "externality" – just like environmental pollution
- This can sometimes be fixed by "the market" but will often require regulatory (Government) intervention

# IT Economics

---

- Economic “rules” for the IT industry are different
- Network effects
  - value of a network grows super-linearly to its size (Metcalfe’s Law says  $n^2$ , Briscoe/Odlyzko/Tilly suggest  $n \log n$ )
  - this drives monopolies, and is why we have just one Internet
- High fixed and low marginal costs
  - competition drives price down to marginal costs of production; but in IT industries this is usually (near as makes no difference) zero
  - hence copyright, patents &c needed to recover capital investment
- Switching costs determine value
  - switching from one IT product or service is usually expensive
  - Shapiro-Varian theorem: net present value of a software company is the total switching costs
  - once you have 1000 songs on your iPod, you're locked into iPods

# IT Economics and Security

---

- The high fixed and low marginal costs, the network effects and switching costs are all powerful drivers towards dominant-firm markets with a big “first-mover” advantage
- Hence the “time-to-market” is critical
- Paying attention to security rarely assists scheduling
- Thus the Microsoft philosophy of “we’ll ship it Tuesday and get it right by version 3” is not perverse behaviour by Bill Gates or a moral failing, but absolutely rational behaviour
- If Microsoft had not acted this way, then almost any other company which took the same approach would now be the dominant player in the PC operating system business (and/or in the office productivity tools business)

# Key Problem of the Information Society

---

- More and more goods contain software so more and more industries are starting to become like the software industry
- The Good
  - flexibility, rapid response
- The Bad
  - Complexity, frustration, bugs
- The Ugly
  - attacks, frauds, monopolies
- How will regulation evolve to cope with this?

# ENISA

---

- European Network and Information Security Agency
  - established in 2004
  - based in Heraklion, Crete
- Motivation: network insecurity threatens the smooth operation of the EU's single market
- Duty: "giving advice and recommendations, data analysis, as well as supporting awareness raising and cooperation by the EU bodies and Member States"

# "Security Economics and European Policy"

---

- In September 2007, ENISA commissioned us (Ross Anderson, Rainer Böhme, Richard Clayton, Tyler Moore) to write a report "analysing barriers and incentives" for security in "the internal market for e-communication"
  - what are the big impediments to security?
  - what is the EU's role in fixing the problems?
  - what are the advances in security economics (often at the WEIS series of conferences) and how might they usefully be applied?
- Report published January 2008
- 15 comments published June 2008 (7 of these were from IXPs, of which more later on)
- Much favourable comment elsewhere

# What's in the Report?

---

- 114 pages, 139 references, 15 recommendations
- 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
- The recommendations are for policy initiatives that require harmonisation (or at least EU-wide coordination)
- Recommendation to this audience: read the whole thing!
  - much of the value is in the survey of the application of security economics to information security; and in the detailed discussion of policy initiatives – for example there's a discussion of cyber-insurance that proposes 5 policy options, but none makes it to a recommendation because the market is finding the best way forward – and the other recommendations will speed this along.

# Economic Barriers to Security

---

All the stuff I've been talking about so far:

- Information asymmetries
- Externalities
- Liability dumping
- Lack of diversity in platforms and networks
- Fragmentation of legislation and law enforcement

# Analyzing the Harm

---

- Type of harm
  - threats to nations
    - Critical National Infrastructure (CNI) : if it breaks, nation is in trouble
    - what if networks are attacked in times of tension ?
  - physical harm to individuals
    - consider the failure of online medical systems
  - financial harm, such as card fraud and phishing
  - harm to privacy, such as by unlawful disclosure of personal data
- Since 2004, online fraud has been industrialized with a diverse market of specialist criminals trading with each other
- We have one or two things to say about CNI and privacy, but the report focuses on financial losses
- To identify the market failures – where the EU can lift barriers and realign incentives – we must look at the fraud process

# Information Asymmetry

---

- We need better data on attacks. Available statistics are poor and often collected by parties who have a vested interest in under- or over-counting
- Different requirements for individuals, firms, security professionals (e.g. at ISPs and banks), academic researchers and policy-makers
- Variables to record include attack type, losses, geography, socio-economic indicators...
- Sources include ISPs, AV vendors, vulnerabilities / attacks disclosed, financial losses, black market monitoring ...

# What Statistics 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

# The Attack Lifecycle

---

- Flaw introduced, either in the design or the code
- The flaw is discovered and reported. Sometimes it is identified before an attack takes place; sometime it first comes to notice when used in a “0-day” attack (where everyone is vulnerable)
- A patch is shipped, but not everyone applies
- Patch is reverse-engineered and attacks occur – increasingly “drive-by” attacks : enticing the vulnerable to “bad” websites
- If the flaw allows control of the machine then it will be recruited as a “zombie” into a botnets where it will send spam, host phishing sites, serve more malware, send DDoS packets etc
- Compromised PCs are detected, taken offline and fixed
- Occasionally law enforcement will try to locate the attackers

# 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 (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 (and many service firms) disclaim all possible liability using contract terms
- There have been many calls for this to change, eg UK House of Lords suggested negligence should be punished
- Clearly not a policy that can be adopted in a single member state, and perhaps not even on a regional basis
- Of course governments should not interfere in business contracts without good reason! Nevertheless 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 routing algorithm at fault? Is what has failed a product or a service? Is it a consumer or a business?

# Liability & Politics

---

- Tackling the “culture of impunity” in software is going to be absolutely essential as civilization comes to depend ever more upon software
- But it’s too hard to do in one go! So need a long-term vision
- Suggested strategy:
  - 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
- Need to robustly tackle the “open source” issues. Why should giving it away “for free” justify negligence or carelessness about security? Might a role develop for bundlers (Red Hat) and consortiums (Apache Foundation) to stand behind individuals?

# Vendor Liability Options

---

- #1 EU Directive that ensures that liability for defects can't be dumped by contract
- #2 Statutory right to sue vendors for damages. If ISPs are liable for "bad traffic" (see earlier recommendation) then can ensure they can recover charges and costs
- #3 Do nothing and rely on market pressure (make it a big deal that Sun and HP patch slower than Microsoft and Red Hat)
- #4 Insist upon "safety by default"  
you can't sell a car without a seatbelt, so why should you be allowed to sell an O/S without patching service?

# Dealing with Software

---

- **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
  - cf 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
- Policy options:
  - Promote open standards to facilitate market entry
  - promote diversity in procurement (and in eGovernment)
  - Provide advice when lack of diversity is a security threat
- **RECOMMENDATION 11:** ENISA should advise the competition authorities whenever diversity has security implications

# Internet Exchange Points

---

- The Internet is clearly part of the CNI, and in many countries IXPs handle most of the peering traffic. Clear pattern of dominant players in almost all member states
- Large networks achieve diversity by peering in multiple IXPs
- Smaller networks rely on the diversity within the IXP itself
  - this is continually under review by the largest and best-run IXPs
- **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
- A number of IXPs have objected to this recommendation on the basis that they don't believe there are monopolies, they already share best practice, and that they should not be regulated

# 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" so as 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)
- Real problem isn't laws but enforcement across borders
  - cf bank robbers who fled across US state lines, dealt with by making bank robbery (etc) into Federal offences
- Approach has been to try and harmonise laws (and penalties)
  - Convention on Cybercrime, Framework Decision on attacks against information systems, Draft Communication on cybercrime...

# Law Enforcement Co-operation

---

- Police forces have to prioritise investigations
  - they consider impact on local citizens, and that's often low
  - also, international investigations are slow and expensive
  - hence very few cyber-criminals caught and prosecuted
  - perception of zero-risk makes attacks more attractive & prevalent
- Policy options:
  1. Increase funding for joint operations (many "joint" operations are lop-sided, with second country merely handling paperwork for an investigation run by another – more funding would mean that they are not done solely on quid pro quo basis)
  2. Mutual legal assistance treaties (generally too slow for cybercrime)
  3. Cyber-security co-operation using NATO as a model (or perhaps WWII SHAPE) Member states make their own political decision on budgets, but some of this funds liaison at a central command centre, that takes Europe-wide view on what to prioritise

# 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](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