An Introduction to Security Economics

Richard Clayton
richard.clayton@cl.cam.ac.uk

with acknowledgements to

Ross Anderson & Tyler Moore
ross.anderson@cl.cam.ac.uk **tmoore@seas.harvard.edu**

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Luxembourg
11th April 2011

NPL
National Physical Laboratory

Outline

- Security economics
  - a powerful new way of looking at overall system security
- Some of the basic ideas from economics
  - Incentives
  - Asymmetric information
  - Externalities
- Applying this ideas to real situations
- ENISA Report: “Security Economics and European Policy”
- Conflict theory: models of attack and defence
- Fixing the Internet for consumers

Traditional View of Information Security

- People used to think that the reason that the Internet was insecure because of a lack of features, or that there was not enough crypto / authentication / filtering
- Also, `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…
- Others worked on lists of things to check upon, or policies that ought to be adopted…
- About 1999, we started to realize that this is not enough…

The ‘New School’ of Information Security

- For the last decade, 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

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, games consoles almost given away and money is made from licensing deals to allow games to be played...
- Cryptography is being used to tackle the obvious contradiction between the decentralization of network intelligence and the operators desire to retain control

Using Economics to Explain Security

- Electronic banking: UK banks were less liable for fraud then 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 $50 on anti-virus software when it isn’t their data that is trashed? Economist 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!

Security Economics Research

- Key early work by Anderson, Odzlyko & Schneier
- Security Economics has grown to 100+ active researchers
- Workshop on the Economics of Information Security (WEIS), held annually in major research centers in US and UK
- Topics range from econometrics of online crime through DRM policy to return on security investment and how to manage the patching cycle
- Anderson maintains an ‘Economics and Security Resource Page’

  http://www.cl.cam.ac.uk/~rja14/econsec.html
- Note also various survey papers by Anderson & Moore, the latest of which is:

  ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf

The Basics of the New Analysis

- Incentives: failures are more likely when the person responsible for protecting a system is not the one who suffers harm
  - so it’s of concern if a bank can dump ‘phishing’ losses onto customers; or if hospital systems put administrator convenience before patient privacy
- Asymmetric information
  - vendors claim that their software is secure, but the buyers have no means of judging this; so they refuse to pay a premium for quality
- Externalities (‘side effects’)
  - a larger network is more valuable to each of its members, so there is a trend towards dominance (Microsoft/Facebook/iTunes)
  - ‘negative externalities’ arise where the damage is done to someone else; malware may not do much local damage, but botnet membership means that everyone else is being damaged

IT Economics and Security I

- 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
- Hence 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 another company which took this approach would now be the dominant player in the PC operating system business (and/or in the office productivity tools business)

IT Economics and Security II

- When building a network monopoly, it is critical to appeal to the vendors of complementary products
  - remember the old mantra of “find the software product then ask which machine and operating system to buy”…
  - … Microsoft spent huge amounts assisting developers
  - we can see the same pattern with PC v Apple; Symbian v WinCE, WMP v RealPlayer, not to mention the console games market
- The lack of security in earlier versions of Windows made it significantly easier to develop applications
- It’s also easy for vendors to choose security technologies that dump support costs onto the users (SSL not SET, PKI, . . .)
- SSH succeeded because the switching cost was low (Telnet++) and there`s benefit to early adopters; hence BGPSEC, DNSSEC and various email protection schemes struggle

The Economics ‘Rules’ for the IT Industry

- 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 etc. needed to recover capital investment
- Switching costs determine value
  - switching from an IT product or service is usually expensive
  - once you have 1000 songs on your iPod, you’re locked into iPods
  - Shapiro-Varian theorem: net present value of a software company is the total switching costs of its customers

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

- When markets fail, one way of dealing with this is to regulate, so how will regulation evolve to cope with this?

Adverse Selection & Moral Hazard

- Suppose you sell insurance to smokers and non-smokers. Smokers are more likely to die earlier, so they get better value from insurance than non-smokers, so as a group they buy more insurance – so the insured are a worse risk. From the point of view of the insurance company the higher mortality by those who ‘select’ insurance is ‘adverse’.
  - fix is to require medicals, or use questionnaires to set rates
- Some central bankers did not want to bail out the failing banks because of the ‘moral hazard’ (the removal of the incentive to be prudent in future)
- Why do Volvo drivers have more accidents? Adverse selection can lead to bad drivers choosing Volvos and moral hazard may mean that people drive more badly because they feel safe

Adverse Selection in Security Software

- George Akerlof’s ‘market for lemons’ (Nobel Prize 2001)
  - considered the trade in second-hand cars as a metaphor for a market with asymmetric information: if there are 50 cars worth $2K and 50 cars worth $1K, then what is the equilibrium price?
  - buyers cannot determine car quality, so they are unwilling to pay a premium for a quality car
  - sellers know this, so market is dominated by low-quality goods
- Software market is a market for lemons (Anderson 2001)
  - vendors may believe their software is secure, but buyers have no reason to accept that this is correct
  - so buyers refuse to pay a premium for secure software, and vendors refuse to devote resources to make it secure
- How can we reduce this asymmetry of information?

Markets for Vulnerabilities

- Need a way to easily measure a system's security
  - stock markets dip after breach, but only a bit & soon forgotten
- One possible approach: establish a market price for an undiscovered vulnerability (Schechter 2002)
  - reward software testers (hackers) for identifying new vulnerability
  - products with higher outstanding rewards are more secure
- Not simply academic fantasy
  - iDefense, Tipping Point have created quasi-markets for vulnerabilities (& now WabiSabiLabi has an auction site)
  - however, their business models have been shown to be socially sub-optimal (e.g., they provide disclosure information only to subscribers and they have an incentive to disclose vulnerabilities to harm non-subscribers)
  - limited public information (at present) on pricing

Adverse Selection in Seals and Adverts

- Ben Edelman (WEIS 2006) used data from SiteAdvisor to identify ‘bad’ sites distributing spam and malware
  - 2.5% of all sites were found to be ‘bad’
- But ‘bad’ companies are more likely to be TRUSTe-certified:
  - 5.4% of TRUSTe-certified sites are ‘bad’
  - However, sites with the BBBOnLine seal are slightly more trustworthy than random sites (but their process is very slow and there were only 631 certificates issued)
- Similarly, untrustworthy sites are over-represented in paid advertisement links compared to the organic search results
  - 2 to 3% of organic results are ‘bad’ (0% for top hit at Yahoo!)
  - 5 to 8% of advertising links are ‘bad’

Tackling Adverse Selection by Regulation

- When the market fails you regulate!

- Options:
  - require certification authorities and search engines to devote more resources to policing content
  - assign liability to certification entities if certifications are granted without proper vetting
  - alternatively, regulate enforcement actions by requiring complaints to be published
  - search engine operators could be required to exercise ‘reasonable diligence’ before agreeing to accept an advertisement

- But so far, we’re just tolerating/ignoring the problem

Privacy

- Most people say they value privacy, but act otherwise. Most privacy ventures have failed
- So why is there this privacy gap?
- Hirshleifer – privacy is a means of social organization, a legacy of territoriality
- Odlyzko – technology makes price discrimination both easier and more attractive
- Acquisti – people care about privacy when buying clothes, but not cameras (phone viruses worse for image than PC viruses?)
- Leads in to research in behavioural economics (the interface between economics and psychology)

“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 (February) 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 ENISA 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, and more:

- 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
  - 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
- We have one or two things to say about CNI and privacy, but the report focuses on financial losses
- Since 2004, online fraud has been industrialized with a diverse market of specialist criminals trading with each other
- To identify the market failures – where the EU can lift barriers and realign incentives – we must look at the fraud process

Conflict Theory

- Does the defence of a country or a system depend on the least effort, on the best effort, or on the sum of efforts?
- Hirshleifer (1983) discussed the island of Anarchia
  - Flood defences built by individual families, so effectiveness depends on the weakest link (the lowest wall, the laziest family)
  - But defence against incoming missiles would depend on who was the best shot
  - Varian (2004) added `sum of efforts’ to this
  - Sum-of-efforts is optimal; least-effort is really awful
- Software is a mix: it depends on the worst effort of the least careful programmer, the best effort of the security architect, and the sum of efforts of the testers
- Moral: hire fewer better programmers, hire more testers, and always use the top architects

Modelling Attacks

- Danezis and Anderson (2005): peer-to-peer systems more resilient when people care about the material they are hosting
- Fultz and Grossklags (2008): study Varian`s security games but model the interaction between attacker and defender (with trade-offs such as the cost of attack, likelihood of detection and value of attack).
- Böhme and Moore (2009) considered iterated games. Defender fixes a hole, attacker exploits another weakness.
  - In the static case (the defender chooses defence at the start) increasing uncertainty causes more assets to be protected, but if uncertainty too high then nothing will be protected.
  - In the dynamic case, the defender can wait and see what is attacked and then defend whatever fails.

Attack and Defence may be Intertwined

- Suppose you are the head of the NSA and discover have a nice new hack on Windows 7 (or even XP), do you tell Microsoft?
  - Tell – protect 300m Americans
  - Don’t tell – be able to hack 400m Europeans, 1000m Chinese…
  - If the Chinese hack US systems, they’ll keep quiet. If you hack their systems, you can brag about it to the President
  - So offence can be favoured over defence
- BTW: investing in finding bugs is probably worthless
  - Windows may well contain tens of thousands of bugs
  - The attacker needs to find just one
  - You have to find thousands before it becomes likely that you find the same one as the attacker

How Much to Spend?

- How much should the average company spend on information security?
- Governments, vendors say: much, much more than at present
- But they’ve been saying this for 20+ years!
- Measurements of security return-on-investment suggest about 20% p.a. overall is in the right ballpark
- Big firms spend more than small; governments spend way more than the private sector
- So the total expenditure may be about right, but individual firms may be getting it wrong. Are there any better metrics?

Skewed Incentives

- Why do large companies spend too much on security and small companies too little?
  - Research shows an adverse selection effect!
  - corporate security managers tend to be risk-averse people, often from accounting / finance
  - more risk-loving people may become sales or engineering staff, or small-firm entrepreneurs
- Investment also affected by:
  - due-diligence (reasonable community standards)
  - government regulation (or initiatives such as PCI)
  - insurance (cyber insurance remains rare, not least because of a fear of correlation between claims when `everyone' attacked at once)
  - auditors (threatening to qualify accounts if their lists not ticked)

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 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

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 botnet 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 (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?

Open versus Closed?

- Are open-source systems more dependable?
  - it is easier for the attackers to find vulnerabilities
  - it is easier for the defenders to find and fix them
- Anderson (2002): openness helps both equally if bugs are random and standard dependability model assumptions apply
- Milk or Wine? bugs are correlated in several real systems
- Big debate on patching at WEIS 2004!
  - Rescorla: patching doesn`t improve systems much, so failures are dominated by patching failures
  - Arora *et al*: without disclosure, vendors won`t improve. Optimal to disclose after a delay
- Emerging consensus: CERT-type rules (responsible disclosure) plus breach disclosure laws for data loss

Liability Misallocation

- Software vendors (and many service firms) disclaim all possible liability using contract terms
- There have been many calls for this to change, e.g. 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 routeing 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 operating system (or a browser plugin, or an iPhone App) without a 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
  - 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
- 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
- Note: 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)
- Approach has been to try and harmonise laws (and penalties)
  - Convention on Cybercrime, Framework Decision on attacks against information systems, Communication on cybercrime...
- 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 and (crucially) thereby allowing the FBI to act

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:
  - increase funding for joint operations (many ‘joint’ operations are lop-sided, with one country merely handling paperwork for another; more funding would move away from just quid pro quo)
  - mutual legal assistance treaties (generally too slow for cybercrime)
  - cyber-security co-operation using NATO as a model (or perhaps WWII SHAEF). Member states make their own political decision on budgets, but fund liaison at a central command centre, that develops strategy & 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 an 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

Takedown times: Moore/Clayton WEIS 08

- Defamation – believed to be quick (days)
- Copyright violation – also prompt(ish)
  - experimentally ‘days’ (with prompting, so perseverance matters)
- Fake escrow agents
  - average 9 days, median 1 day
  - note that AA419 aware of around 25% of sites
- Mule recruitment sites (Sydney Car Center etc.)
  - average 13 days, median 8 days
  - doesn’t attack any particular bank, so they ignore the issue
  - slower than escrow sites (vigilantes more motivated ?)
- Fake pharmacies
  - no `vigilante groups’ – so lifetime is ~2 months

The Research Agenda

- The online world and the physical world are merging, and this will cause major dislocation for many years
- Security economics gives us some of the tools we need to understand what's going on
- Sociology gives some cool and useful stuff too
- And `security psychology' is not just about usability and preventing phishing. It might bring us fundamental insights, particularly in improving our understanding of why security fails for some individuals – just as security economics has given us insight into why it can fail for the crowd

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

NPL
National Physical Laboratory