An Introduction to Security Economics

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

with acknowledgements to

Ross Anderson & Tyler Moore
ross.anderson AT cl.cam.ac.uk **tyler-moore AT utulsa.edu**

Part II: Security
29th January 2016

Outline

- Security economics
  - a powerful new way of looking at overall system security
- Some of the key basic ideas from economics
  - incentives
  - asymmetric information
  - externalities
  - adverse selection
- Security economics research examples
  - malware on the Internet
  - website takedown times
  - HTTPS certificates
  - the cost of cybercrime

Traditional View of Information Security

- People used to think that the reason that the Internet was insecure was because of a lack of features, there was not enough crypto / authentication / filtering
- Plus, 'if only' people had a really good checklist of security issues to get right, 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 long lists of things to check up on, or policies that ought to be adopted…
- About 1999, we started to realize that this is not enough…

The 'New School' of Information Security

- Since the start of the century, we have started to apply an economic analysis to information security issues
- This 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
- It 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 authenticated 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 (Technical Protection Measures):
  - has allowed Apple to grab control of music downloads
  - games consoles are 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 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 (DDoS): spoofed source UDP packets (NTP, SSDP, DNS etc.) are amplified and the result is significant flows to the victims. Why should hosting companies fix their filters or reflectors update their software when they are not the ones being hit ? 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!

Security Economics Research

- Key early work by Anderson, Odlzyko & 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 Europe
- Topics range from econometrics of online crime through DRM policy, to determining the return on security investment and how best 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 is 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

- Why was Microsoft software so insecure in the early 2000s, despite its market dominance?
- 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 and only 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; Android v iOS, 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 is also easy for vendors to choose security technologies that dump support costs onto the users (SSL not SET, PKI, . . .)
- SSH succeeded because of a low switching cost (Telnet++) and there's benefit to early adopters; this is not so for BGPSEC, DNSSEC & various email protection schemes: and they struggle!

The Economics 'Rules' for the IT Industry

- Network effects
  - the 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 in 2008 because of the 'moral hazard' (the removal of the incentive to be prudent in future)
- It's claimed that Volvo drivers have more accidents. Perhaps adverse selection leads to bad drivers choosing Volvos and/or moral hazard could mean that Volvo drivers are less careful because they feel safe (the "risk thermostat")

Adverse Selection in Security Software

- George Akerlof's 'market for lemons' (Nobel Prize 2001)
  - he 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?
  - car sellers use 3rd party inspection reports (and give guarantees)

Malware on the Internet

- Internet security 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
- Should the Government have a role here (c.f. the way in which we tackle illness by public health initiatives)
  - the debate on this tells you more about participants' political views than whether this is a valuable suggestion

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
- Phishing
  - 4 hours if bank aware, 4 days if not
- 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

Security Economics of HTTPS I

- Paper by Asghari et al. at WEIS 2013
- Websites decide whether or not to offer services over HTTPS
  - used as a signal of security / trustworthiness / competence
  - or, in the case of payments, for reasons of compliance
- HTTPS certificates issued by Certificate Authorities
- Browsers decide which CAs are to be trusted
  - once money sufficed, now a complex assessment system
- Any CA can issue a cert for any domain & browser will accept
- High profile breaches have led to problems:
  - Diginotar (2011) : 531 certs issued by an Iranian (?)
  - Comodo (2011) : handful of certs for high value domains
  - intermediate cert issues with CA Trustwave (2012) & CINIC (2015)

Security Economics of HTTPS II

- Diginotar was delisted & went bankrupt
  - eventually… had to sort out NL Government websites first
- However Comodo (& Verizon, 2010) 'too big to fail'
- WEIS paper looks at market share and finds high price certificates have significant market share
  - certificates perfectly substitutable, so expect prices to drop
    - DV: pay $0 to $249, mean = $81 EV: pay $100 to $1522, mean = $622
  - note that 'weakest link' means you're not buying 'better security'
- So why no evidence of a 'race to the bottom' ?
  - some attempt at signalling (seals on web pages), malware scans &c
  - it may be that "too big to fail" is of practical importance
  - a key issue appears to be enterprise cert-management tools
  - viz: what is really being sold is a subscription service

Measuring Cybercrime

- 2009 McAfee: cybercrime costs $1000bn ($1 trillion) worldwide
- 2011 Detica (part of BAE plc): estimated cost of cybercrime to the UK economy was $43 billion / annum (~ 1.8% of GDP)
- Florencio and Herley "Sex, Lies and Cybercrime Surveys"
  - this WEIS 2011 paper points out how outliers affect results (single loss of $50K in a 1000 person survey becomes $10bn scaled up)
- We (multiple expert authors) assessed data for WEIS 2012:
  - created framework, and gave best estimates for each category
  - traditional frauds cost citizens a few hundred dollars per year
  - transitional frauds cost citizens a few tens of dollars per year
  - new cybercrimes net criminals tens of pence per citizen per year
- BUT the indirect costs and defence costs (& especially clean-up costs) for new crimes are more than 10x the criminal revenue

The Security Economics Research Agenda

- The online world and the physical world are merging, and this will cause major dislocation for many years to come
- Security economics gives us some of the tools we need to understand what's going on
  - we're a lot less puzzled than we were in 2000!
- Sociology gives some cool and useful stuff too
- But "privacy" issues still inadequately explained
  - people say they value privacy, but give it away for almost nothing
- A recent focus on '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..

Economics and Security Resource Page:

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

Richard Clayton:

http://www.cl.cam.ac.uk/~rnc1/publications.html

Cambridge Security Group Blog:

http://www.lightbluetouchpaper.org