An Introduction to Security Economics

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

with acknowledgements to

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

Tyler Moore

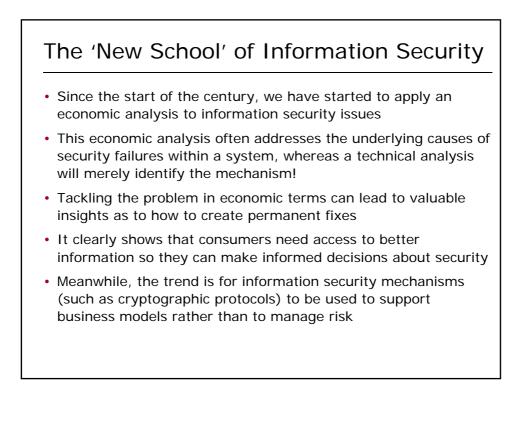


Part II: Security 29th January 2016

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

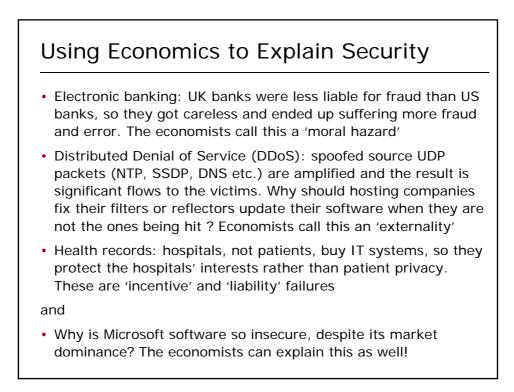
Traditional View of Information Security

- 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...



New Uses of Security Mechanisms

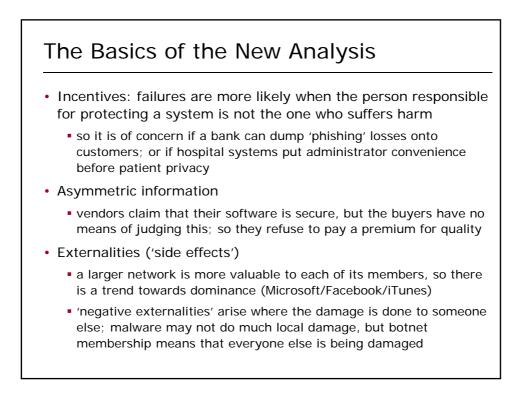
- Xerox authenticated ink cartridges to tie them to the printer
 - followed by HP, Lexmark. . . and Lexmark's case against SCC
 - note that the profit is in the consumables purchasers compare ticket price, rather than total cost of ownership
- Accessory control now spreading to more and more industries
 - 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



Security Economics Research

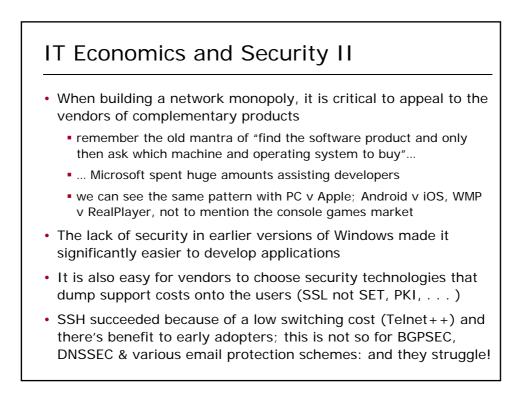
- · Key early work by Anderson, Odlzyko & Schneier
- Security Economics has grown to 100+ active researchers
- Workshop on the Economics of Information Security (WEIS), held annually in major research centers in US and Europe
- Topics range from econometrics of online crime through DRM policy, to determining 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



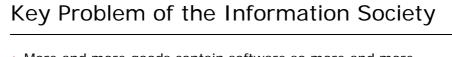
IT Economics and Security I

- 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)



The Economics 'Rules' for the IT Industry

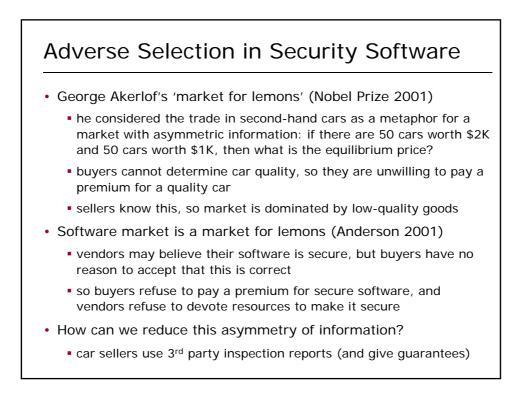
- Network effects
 - the value of a network grows super-linearly to its size (Metcalfe's Law says n², Briscoe/Odlyzko/Tilly suggest n log n)
 - this drives monopolies, and is why we have just one Internet
- High fixed and low marginal costs
 - competition drives price down to marginal costs of production; 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



- 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?

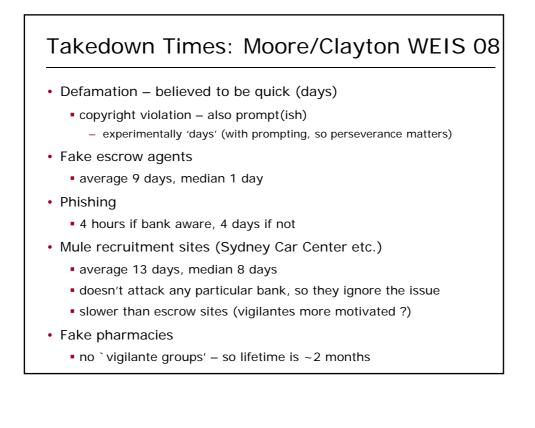
Adverse Selection & Moral Hazard

- 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")



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

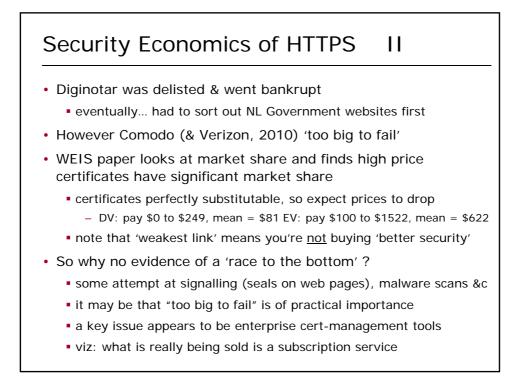


Security Economics of HTTPS

- Paper by Asghari et al. at WEIS 2013
- Websites decide whether or not to offer services over HTTPS

I

- 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)



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 <u>pence</u> 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

