Economics of Information Security

Robert Sloan, based significantly on Ross Anderson’s Crypto 2007 Keynote slides
Traditional View of Infosec

- People used to think that the Internet was insecure because of lack of features – crypto, authentication, filtering
- So worked on providing better, cheaper security features – AES, PKI, firewalls ...
- About 1994–2000, some prominent players started to realize that this is not enough
People, Law, Economics Trump!

* Bruce Schnier,
  * 2000, *Secrets and Lies*: “I have written this book partly to correct a mistake. Seven years ago I wrote another book ... The weak pints had nothing to do with [cryptography].”

* 1970s, Diffie & Hellman invent public-key crypto; 1998, Diffie & Landau publish *Privacy on the Line: The politics of Wiretapping and encryption*
Then came Economics

- 1994: Anderson publishes about U.K. banks’ economic incentives
- 2000 lots of stuff
- 2001–: Econ of Security annual conference
Economics and Security

- Since c. 2000, started applying economic analysis to IT security and dependability
- It often explains failure better!
- Electronic banking: UK banks were less liable for fraud, so ended up suffering more internal fraud and more errors
- Distributed denial of service: viruses now don’t attack the infected machine so much as using it to attack others
- Why is Microsoft software so insecure, despite market dominance?
Flip side: which economics

- The freshman Intro Microeconomics course’s supply and demand curves from 1950s for Ag. products don’t really explain IT.

- Need some cool parts of Intermediate Micro, results of 1970s–1990s. Monopoly effects, network effects, etc.
New View of Infosec

- Systems are often insecure because the people who guard them, or who could fix them, have insufficient incentives
  - Bank customers suffer when poorly-designed bank systems make fraud and phishing easier
  - Casino websites suffer when infected PCs run DDoS attacks on them

- Insecurity is often what economists call an ‘externality’ – a side-effect, like environmental pollution
New Uses of Infosec

* Xerox started using authentication in ink cartridges to tie them to the printer – and its competitors soon followed

* Carmakers make engine modding harder, and plan to authenticate major components
Economic Analysis Informs

- Hal Varian (then at Berkeley and NY Times columnist, now Google chief economist): linking two industries benefits the one that is more concentrated.

- January 2005: Claims recording industry will be unhappy if DRM goes in, because only 3 players in DRM with one (Apple) very powerful, music industry bigger.

- Indeed, industry did not like 99 cent tracks.
The first distinguishing characteristic of many IT product and service markets is network effects:

- Metcalfe’s law – the value of a network is the square of the number of users:
- Real networks – phones, fax, email
- Virtual networks – PC architecture versus MAC, or Skype.
- Network effects tend to lead to dominant firm markets where the winner takes all
Second common feature of IT product and service markets is high fixed costs and low marginal costs.

Competition can drive down prices to marginal cost of production.

Further, information is experience good every time.

This can make it hard to recover capital investment, unless stopped by patent, brand, compatibility …

These effects can also lead to dominant-firm market structures.
Third common feature of IT markets is that switching from one product or service to another is expensive.

E.g. switching from Windows to Linux means retraining staff, rewriting apps.

This lock-in is major part of value of SW companies.

So major effort goes into managing switching costs – once you have $3000 worth of songs on a $300 iPod, you’re locked into iPods.
IT Economics and Security

- High fixed/low marginal costs, network effects and switching costs all tend to lead to dominant-firm markets with big first-mover advantage
- So time-to-market is critical
- Microsoft philosophy of ‘we’ll ship it Tuesday and get it right by version 3’ is not perverse behavior by Bill Gates & Steve Ballmer but quite rational
- Whichever company had won in the PC OS business would have done the same
When building a network monopoly, you must appeal to vendors of complementary products. That's application software developers in the case of PC versus Apple, and perhaps today with mobile phone OS's. Lack of security in earlier versions of Windows made it easier to develop applications. So did the choice of security technologies that dump costs on the user (SSL, not SET c. 1998). Once you've a monopoly, lock it all down!

Suppose a town has 100 used cars for sale: 50 good ones worth $2000 and 50 lemons worth $1000.

What is the equilibrium price of used cars? Should it be midway point at $1500?
Why are so many security products so ineffective?

- If $1500, no good cars will be offered for sale ...
- Akerlof’s work Started the study of asymmetric information
- Security products are often a ‘lemons market’
Adverse Selection

- Undesirable situation in markets where due to information asymmetries, “bad” product or customer more likely to be selected
- E.g., Smokers more likely to buy health, life insurance, if insurance companies can’t distinguish smokers from non-smokers
Moral Hazard

- You act differently because you are (or believe you are) insulated from risk
- Less careful with insured risk
- Subprime mortgage mess?
- Anderson’s explanation of lazy UK Bank staff
- Software design and implementation staff that know they won’t be held accountable
Products worse than useless

- Adverse selection and moral hazard matter (why do Volvo drivers have more accidents?)
- Application to trust: Ben Edelman, ‘Adverse selection on online trust certifications’ (WEIS 06)
  - Websites with a TRUSTe certification are more than twice as likely to be malicious
  - The top Google ad is about twice as likely as the top free search result to be malicious (other search engines worse ...)
  - Conclusion: ‘Don’t click on ads’
Privacy economic issues

- People have less than perfect information
- People have limited computational ability
- Behavioral economics: even given those limits, people behave in (systematic, predictable) irrational ways.
Privacy

• Most people say they value privacy, but act otherwise. Most privacy ventures failed

• Why is there this privacy gap?

• Hirshleifer – privacy is a means of social organization, a legacy of territoriality

• Varian – you can maybe fix privacy by giving people property rights in personal information

• Odlyzko – technology makes price discrimination both easier and more attractive

• Acquisti – Experimental work. One result: overdiscounting—too willing to trade short-term benefit for long-term risk.
Conflict theory

* Does the defense of a country or a system depend on the least effort, on the best effort, or on the sum of efforts?

* The last is optimal; the first 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, more testers, top architects
Open versus Closed?

- Are open-source systems more dependable? It’s easier for the attackers to find vulnerabilities, but also easier for the defenders to find and fix them.
- Theorem: openness helps both equally if bugs are random and standard dependability model assumptions apply.
- Statistics: bugs are correlated in a number of real systems (‘Milk or Wine?’).
- Trade-off: the gains from this, versus the risks to systems whose owners don’t patch.
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% per annum overall
* So the total expenditure may be about right. Are there any better metrics?
Security metrics

- Insurance markets – can be dysfunctional because of correlated risk
- Vulnerability markets – in theory can elicit information about cost of attack
- iDefense, Tipping Point, ...
- Further: derivatives, bug auctions, ...
- Stock markets – in theory can elicit information about costs of compromise
- Stock prices drop a few percent after a breach disclosure
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
- There’s also due-diligence, government regulation, and insurance to think of
Skewed Incentives (2)

* If you are DirNSA and have a nice new hack on XP and Vista, do you tell Bill & Steve?
  
  Tell—protect 300 million Americans

  Don’t tell—be able to hack 400 million Europeans, 1.3 billion Chinese,…

  If the Chinese hack US systems, they keep quiet. If you hack their systems, you can brag about it to the President

  So offense can be favored over defense
Psychology and Security

- Phishing only started in 2004, by 2006 already there were significant phishing losses.
- Banks initially react to phishing by ‘blame and train’ efforts towards customers – but we know from the safety-critical world that this doesn’t work.
- We really need to know a lot more about the interaction between security and psychology.
Psychology and Security (2)

- Security usability research just beginning
- Most products don’t work well or at all!
- Train people to keep on clicking ‘OK’ until they can get their work done
- Systems designed by geeks for geeks discriminate against women, the elderly and the less educated
Psychology and Security (3)

- Social psychology has long studied obedience!
  - Solomon Asch showed most people would deny the evidence of their eyes to conform to a group
  - Stanley Milgram showed that 60% of people will do downright immoral things if ordered to
  - Philip Zimbardo’s Stanford Prisoner Experiment showed roles and group dynamics were enough

- The disturbing case of ‘Officer Scott’
- How can systems resist abuse of authority?
Risk perception, terrorism, & security

- Actual security different from feeling of security
- Food poisoning: 5,000 US deaths/year
- Autos: 40,000 US deaths/year
- 9/11 2,973 deaths once
- Risk perception biases plus "Availability heuristic" in human’s probability estimation: easy to imagine = probable
Psychology and Security (4)

- Evolutionary psychology may eventually explain cognitive biases. It is based on the massive modularity hypothesis and the use of FMRI to track brain function.
- ‘Theory of mind’ module central to empathy for others’ mental states.
- This is how we differ from the great apes.
- It helps us lie, and to detect lies told by others.
- So are we really homo sapiens sapiens – or homo sapiens deceptor?
Conclusion?

- 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.