THE UNIVERSITY OF BRITISH COLUMBIA

Economics of Information Security

EECE 412

(Adopted from the material by Ross Anderson and Richard Clayton, Univ. of Cambridge)

Outline

- Security economics
  - a powerful new way of looking at overall system security
- Key ideas for security economics
  - incentives
  - asymmetric information
  - externalities
  - network effects
  - low marginal costs
  - high switching costs
- Other issues

THE UNIVERSITY OF BRITISH COLUMBIA

Security Economics

Traditional View of Infosec

- People used to think that the Internet was insecure because of lack of features – crypto, authentication, filtering
- So engineers worked on providing better security features – AES, PKI, broadcast encryption, anti-virus scanners and firewalls …
- Others worked on long lists of things to check up on, or policies that ought to be adopted …

Is this really enough?

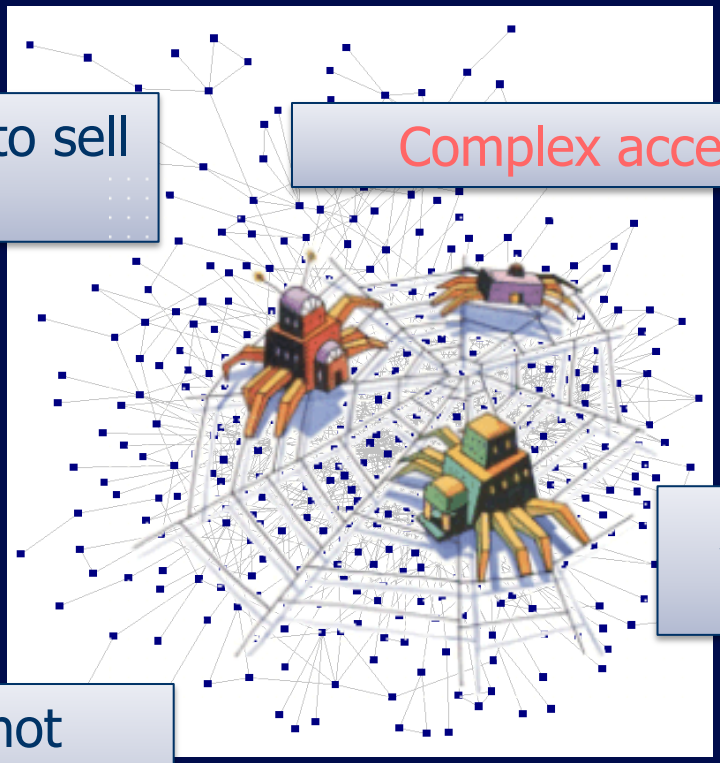
But, we started to realize
that this is not enough.

Economics and Security

- Since 2000, we have started to apply 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
- Meanwhile, the trend is for information security mechanisms (such as cryptographic protocols) to be used to support business models rather than to manage risk

An Example of Facebook

facebook wants to sell user data



Complex access controls

Users cannot measure their risks

Attackers' costs are very low

Over 90% of users never change defaults.

Economics

- What is Economics?
  - Economics is defined as the social science that studies the production, distribution, and consumption of goods and services (from Wikipedia)
  - Economics is also defined as the science which studies human behavior as a relationship between ends and scarce means which have alternative uses (by Lionel Robbins)
- Why should we study economics for information security?
  - The actions for information security demand resources
  - There exist multiple players (attackers and defenders)
  - We want to make better decisions regarding security

(1) Using Economics to Understand Security Industry

- Electronic banking: UK banks were less liable for fraud compared with US banks, so ended up suffering more internal fraud and more errors. The economists call this a 'moral hazard'
- Distributed denial of service: viruses now don't 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
- Why is Microsoft software so insecure, despite market dominance? The economists can explain this as well.

(2) New Uses of Security Mechanisms to Make Money

- Xerox started using authentication in ink cartridges to tie them to the printer – and its competitors (HP, Lexmark …) soon followed
- Accessory control now spreading to more and more industries
  - games, mobile phones, cars
- DRM: Apple used DRM to control the distribution of music contents, MS accused of making a play to control distribution of HD video content – money is made from licensing deals to allow contents to be used

THE UNIVERSITY OF BRITISH COLUMBIA

Key Ideas to Understand Security Economics

1. Incentives

- Incentive: motivating agents to take action
- 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
  - Patients suffer when hospital systems break privacy
  - Users suffer when poorly-protected web services' password database is leaked
- How can we fix this?
  - The regulation by government

2. Asymmetric information

- One party knows more than another, hence the bad drives out the good
- George Akerlof wrote a paper "The Market for Lemons"
  - A used car market includes both good (peach) and bad (lemon) cars. The seller only knows which is better, but the buyer can't tell the difference
  - Suppose there are 50 good ones ($2000) and 50 lemons ($1000)
  - What is the equilibrium price of used cars?
  - If $1500, no good cars will be offered for sale …

A Security Market for Lemons

- In a market where the seller has more information about the product than the buyer, bad products can drive the good ones out of the market
- Security products (e.g. firewall) are often a 'lemons market' – 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, and vendors refuse to devote resources to make it secure
- How can we fix this?
  - Providing information for consumers
  - Providing warranty to guarantee the quality of products
  - Government regulation
  - Self-regulation to produce credible product information

3. Externalities

- Externality is a cost or benefit that is not transmitted through prices
- 'Negative externalities' (a side-effect, like environmental pollution) arise when an individual or firm making a decision does not have to pay the full cost of the decision
  - malware may not do much local damage, but it can damage others
  - rooting mobile phones may incur significant losses in the contents and service providers instead of phone manufacturers
- How can we fix this?
  - The regulation by government
  - Market-based solutions to reduce the externality, by exploiting the price mechanism

4. Network Effects

- A distinguishing characteristic of many IT product and service markets is network effects
- A larger network is more valuable to each of its members, so there is a trend towards dominance (Microsoft/Facebook/iTunes)
  - Network effects tend to lead to dominant firm markets where the winner takes all
  - Metcalfe's law – the value of a network is the square of the number of users
- How can we fix this?
  - Use open standard to minimize vendor lock-in

5. Low Marginal Costs

- Marginal cost: change in cost due to one unit change in production
- A 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
- Hence copyright, patent, brand and compatibility are needed to recover capital investment

6. High Switching Costs

- A 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
- Shapiro-Varian theorem: the value of software company is the total switching costs
- So major effort goes into managing switching costs – once you have $3000 worth of songs on a $300 iPod, you're locked into iPods

First-Mover Advantages

- 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 (rather than building secure software)
- Microsoft philosophy of "we will ship it Tuesday and get it right by version 3" is not perverse behaviour but quite rational
- Whichever company had won in the PC OS business would have done the same

Why are so many security products ineffective?

- `Incentives', `asymmetric information' and `first mover advantages' explain this well.
- How can we solve this issue?
  - When the market fails, we might try to regulate!
  - Develop a way to easily measure a system's security

How to Evaluate Security

- Stock markets – can elicit information about costs of compromise. Stock prices drop a few percent after a breach disclosure, but only a bit & soon forgotten
- One possible approach: establish a market price for an undiscovered vulnerability
  - reward software testers (hackers) for identifying new vulnerability
  - products with higher outstanding rewards are more secure
  - iDefense, Tipping Point have created quasi-markets for vulnerabilities

Other Issues

Privacy

- Most people say they value privacy, but act otherwise. Most privacy ventures failed
- Why is there this privacy gap?
- We discussed relevant research in behavioural economics (the interface between economics and psychology) including
  - Acquisti – people care about privacy when buying clothes, but not cameras (data relating to body or image are more privacy sensitive)

Open versus Closed?

- Are open-source systems more dependable?
  - it's easier for the attackers to find vulnerabilities
  - it's easier for the defenders to find and fix them
- Theorem: openness helps both equally if bugs are random and standard dependability model assumptions apply
  - Protocol: open might be better than closed
  - OS (with many bugs): closed might be better than open
- "Milk or Wine?": bugs are correlated in a number of real systems; so openness might be helpful
- 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!
- How do we measure the cost of security? Are there any reasonable metrics?

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
- Security psychology is also vital
- The research agenda isn't just about designing better crypto protocols; it's about understanding dependability in complex socio-technical systems

More …

- See the chapter 7 in the text book of "security engineering"
- See Economics and Security Resource Page – www.cl.cam.ac.uk/~rja14/econsec.html (or follow link from my home page
- See www.ross-anderson.com for survey articles, papers (e.g., measuring the cost of cybercrime), and ENISA report
- Attend WEIS – Workshop on Economics and Information Security