System Security Group | Lancaster University

Economics of Security

Aims

- Provide a new tool set to understand security issues
- Help us to understand broader ranges of risks to security outside of the technical

Why Are We Not More Secure?

- We know how to build secure systems!
- Wrong incentives
    - Guards don't suffer
    - Security shift liability
- The Internet, millions of independent principles interacting
    - Reasonable global outcomes from selfish local actions
- Incentives drive security design and policy

Is Network insecurity the Same as Air Pollution?

- Insecure machines connected to the Internet have costs for all
    - Who should bear al the cost?
        - Individuals, vendors, regulators, authorities?
- Security Economics can be used to help understand
    - Security issues: Privacy, Spam, Phishing etc
    - System Dependability: optimum ratio of dev to test
    - Analysis of Policy Problems: DRM

Public Good

- Same quantity of good regardless of desire
  - Air Quality
- Properties:
  - Non-rivalrous: my use does not deplete yours
  - Non-excludable: inefficient to stop people from using them, lighthouse
- Public good supply
  - Directly from governments: national defence
  - Patents and Copyright: temporary monopoly

Security and Public Good

- Many aspects of security are public goods
  - Air defence is not an individual action
- Strong externalities
  - Cost borne by others
  - One insecure system connected to the Internet affects all
    - Air pollution, toxic dumping
- Is IT security air defence or air pollution
  - Spam used to be a large number of small groups
  - Spam now a small group of powerful teams
  - Is it a national defence issue?

The Price of a Good

- Jerons and Menger: the price of a good in equilibrium is the marginal cost of production
- A good cost £10 to produce, not every producer sells at £10, only marginal ones
    - Those producers just stay in business
    - If price goes down marginal producers close
    - If price goes up marginal producers open

The Price of Information

- In a competitive market price should be its marginal cost
  - Information has high fixed costs
  - Information re-production is free
  - Reason for so much free info, zero is a fair price
- If you can produce at 0 cost then the incentive is to cut without limit to undercut competitors
- Encyclopaedias
  - Britannica $1600, Encarta $49.95, Wikipedia $0

Business Models

- Linux is free, support is not
- Snort is free, rules are not
- Open source devs contribute for free, but gain CV experience
- Information Goods and Services Characteristics
    - High fixed costs, low production = service or advertising model
    - Dominated by network effects
    - Technical lock in
    - Tend to lead to dominate firms and monopolies

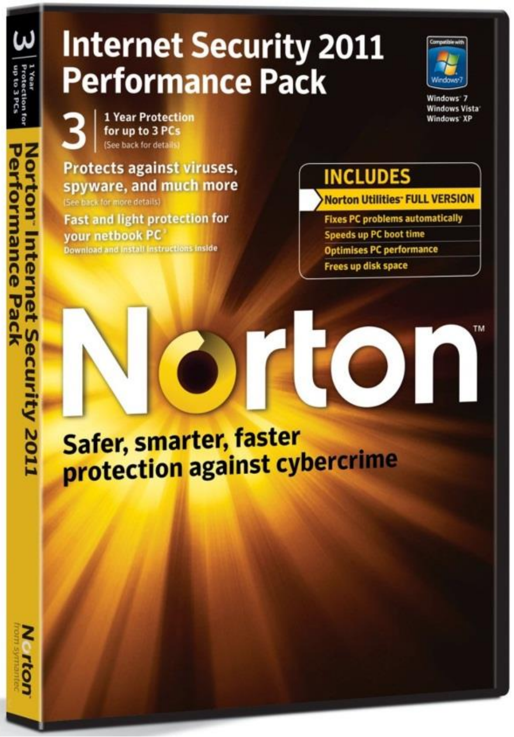
The Value of Lock In

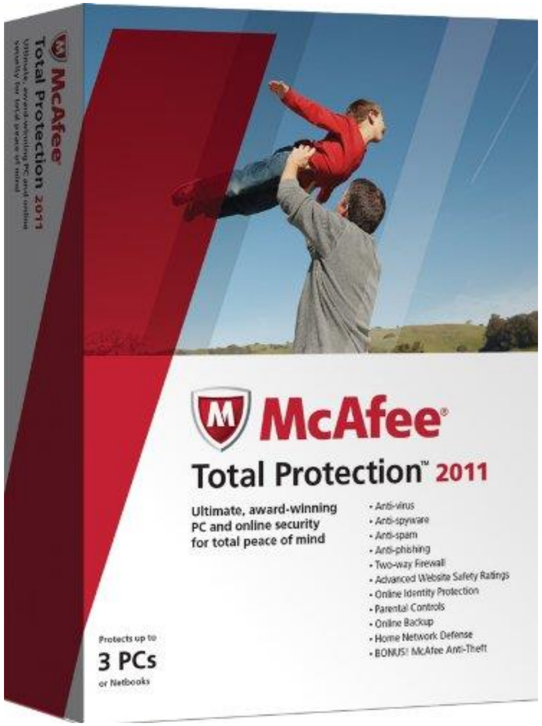
- Shapiro and Varian: The value of a company is the total lock in cost
- Consider a company with 100 staff with Office @ £500 a pop
  - Company switch to Open Office save £50000
  - If costs of change were less, they would switch
  - If they were more MS would put up price
- Consider Apple and Itunes

Information Asymmetry

- George Akerlof - “Market for Lemons” – 1970
  - Some know more than others
- Example
  - 100 used cars, 50 good £2000, 50 bad £1000
  - Sellers know which is which, buyers don’t
  - What is the market price of the used car?
  - At £1500 no good cars will be offered, so price will be closer to £1000.

Can You Decide?


Internet Security 2011
Performance Pack
3 1 Year Protection for up to 3 PCs
Protects against viruses, spyware, and much more
Fast and light protection for your netbook PC
INCLUDES
Norton Utilities FULL VERSION
Fixes PC problems automatically
Speeds up PC boot time
Optimises PC performance
Frees up disk space
Norton
Safer, smarter, faster protection against cybercrime
Norton Internet Security 2011 Performance Pack



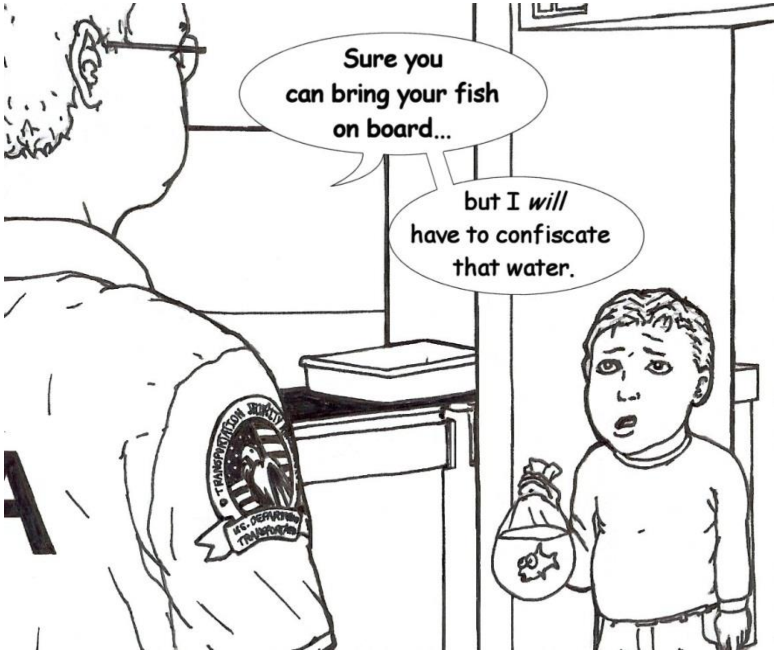
- Poor security products dominate when users can’t tell the difference
  - Race to the bottom on price

What about you? Why do you get insurance?

- Hidden information – adverse selection
- Hidden action – moral hazard
- Volvos are safe cars but have higher accident rates
  - Do bad drivers buy them? – AS
  - Do you drive badly because you think you are safer? – MH
- Consider AV products?
  - Do they make you feel safer – act riskier
  - Get the best AV because you are risky
- What about in private browsing?

Why does security fail?

- Those guarding have no incentives to protect what we think is important.
  - Guards don't suffer a point of failure
  - Risks are dumped on others
- Security is a power relationship
  - Principles control security meaning to advance power


Sure you can bring your fish on board...
but I *will* have to confiscate that water.
TRANSPORTATION SECURITY
U.S. DEPARTMENT OF TRANSPORTATION

What is the best Strategy?

- Jack Hirshleifer founded conflict theory
- Consider the country of Anarchia
  - Flood defence managed by everyone on the coast
    - As good as the weakest link
    - The more defenders the greater the number of weaknesses
  - Missile defence is based on best shot
    - Best effort

System Reliability and Freeriding

- Hal Varian work applying previous theory to effort applied in securing systems.
- **Total effort.** Reliability depends on the sum of the efforts exerted by the individuals.
- **Weakest link.** Reliability depends on the minimum effort.
- **Best shot.** Reliability depends on the maximum effort.

How should you structure your dev team?

How should you structure your dev team?

- Program correctness can depend on minimum effort
  - Most careless programmer
- Software vulnerability testing may depend on sum of all testers efforts
- Security depends on best effort
  - Actions taken by individual champion, architect/designer
- More agents
  - Less reliability in min. effort case
  - More reliability in total effort case

Whys is Windows insecure?

- Why are there still so many bugs when Windows is so dominant?
- Why no comparable effort in commodity platforms compared to defence or healthcare?
- Technically we know how to build good systems, so why don’t we?
- Product insecure at first then improve, why?
  - Symbian, IBM
  - Win95->Win98->WinXP->Vista->Win7->Win10

What is the software market like?

- Low marginal but high fixed costs
- Network effects
- Technical lock-in
- Race to dominate, the dominant firm gets all the money
- MS 1990’s philosophy *“ship it Tuesday and get it right by V3”* is rational
- You must appeal to complementers
  - Security gets in the way
  - Add security later, but make sure it helps lock in

DRM, is it a good thing?

- Varian, DRM is about tying, bundling and price discrimination
- Transfer of control from owner of contain to owner of file
  - Potential for lock in increases
  - Amazon Kindle 1984, Itunes DRM
- Oberholzer & Strumpf showed music shared was not bad backed up by Canadian government
  - Varian in early 2005 showed DRM helps system manufacturers not music industry
  - End of the year publishers protesting against Apple

Questions?