Economics and computer security

Hal R. Varian
UC Berkeley
http://www.sims.berkeley.edu/~hal
Outline

- Assignment of liability
- Role of insurance
- Efficiency and coordination costs
- Implications of weakest link technology
Assignment of liability

• Want to reduce expected cost of accidents
  – Parties can affect the probability of accidents happening
  – Want to set up incentives to get the right parties invest effort in reducing expected costs of accidents
  – Liability: who has to pay and how much if accident occurs. Sets incentives to reduce expected costs.

• Basic principles
  – Least cost avoider: assign liability to the party that is best positioned to reduce expected costs
  – Due care standard: set a due care standard, no liability if you meet the due care standard, otherwise pay accident cost
Least cost avoider

- \( ECost = \text{Prob}(e1+e2)A - c1e1 - c2e2 \)
  - \( ECost \) = expected cost
  - \( \text{Prob}(e1+e2) \) = prob accident occurs
  - \( A \) = cost of accident/event
  - \( e1, e2 \) = effort to reduce prob of accident
  - \( c1, c2 \) = cost of effort

- Observe: you want the party with the lowest effort cost to exert all the effort

- This drives the other party’s effort to zero, but that’s OK \textit{in this case}
Due care standard

- \( EC = \text{Prob}(e1,e2) A - c1 e1 - c2 e2 \)
  - Find efforts that minimize expected costs, \((e1^*,e2^*)\)
  - Set due care standards equal to this effort level
  - No liability if you meet due care standard
  - Otherwise, pay fine equal to cost \( A \) if accident occurs
  - See Steven Shavell, *Economic Analysis of Accident Law*
Computer security

- Sometimes the effort cost is so extreme (e.g., technical knowledge) that liability goes to one party
- Other times due care standard is plausible
  - Due care standard determined by courts, but guided by industry practices
  - Could be very important role for security community
  - Better to be proactive than just let these standards evolve
  - Should there be a FASB-like board?


**Example: ATM machines**

- Ross Anderson: “Why cryptosystems fail”
- Suppose there is a dispute between you and your bank about your ATM usage
  - England: bank is right unless you can prove them wrong
  - US: you are right unless the bank can prove you wrong
- Two different default assignments of liability
Result of ATM liability assignment

• US: banks invest in risk reduction technology
• England: banks typically do not invest in such technology
• Credit card and phone card risk management
• Role of competition: debit cards
Role of insurance

• Two major risk management institutions
  – Stock market
  – Insurance market

• Why do corporations buy insurance?
  – Value of shares depend on portfolio value
  – Shareholders can diversify risk themselves
  – Particularly good question in case of computer security
Why do corporations buy insurance?

• Answer: risk management services
• Insurance companies are well placed to
  – recommend actions
  – require compliance
  – disseminate best practices
  – insurance contract is incentive compatible!
• Especially valuable services for rare events
Examples

• Expert certification
  – Year 2000 problem

• Could do more
  – CERT patches requirement for insurance
  – SATAN test

• Prediction
  – insurance companies will move into computer security (supplemented by expert advisors)
Insurance: moral hazard

- Want the insured to bear some risk
  - full insurance has bad incentives
  - deductible/co-pay is much better

- Want to structure incentives to reduce risk
  - liability assignments – as discussed
  - deductible – moral hazard
Adverse selection

- Those who need insurance most buy it
- Pool that *purchases* insurance is not representative of entire population
- Adverse selection can destroy market
  - argument for social insurance
  - e.g., infrastructure protection above and beyond that covered by private incentives
Infrastructure as public good

• Private good v public good
  – excludability
  – rivalry

• Public good aspect to security
  – national defense; police services

• How to pay for security?
  – individual or social choice?
Private or public?

- Gated communities or private walls?
Costs

- Production costs
  - economies of scale in protection?

- Countervailing effects
  - decision costs: social v private decisions
  - coordination/complexity management costs
  - effectiveness of measures
  - clarity of who is responsible
  - genetic diversity
Total effort v weakest link

• Public goods usually involve total effort
• Security often has weakest-link character
  – makes public good more costly
  – private incentives
    • leadership is critical
    • coordination is critical
Why systems fail?

• Ross Anderson paper “Why cryptosystems fail”
  – http://www.cl.cam.ac.uk/~rja14

• What to do about human failure?
  – get incentives right (e.g., liability assignments)
  – outside monitors and auditors (insurance)
  – follow procedures (banking)
  – standards setting role of military (e.g., aviation)