Background

- Anderson: "Why Cryptosystems Fail"
  - mostly due to implementation and management errors
  - better system security depends on improving human dimensions
  - what can economics contribute?

Economic analysis

- Incentives
  - to create and maintain secure systems
  - to make cost-effective choices
  - to manage risks appropriately
  - to disseminate information
  - Economics: socially optimal and private incentives may well differ
    - but can be aligned

Liability and incentives

- ATM machines
  - In the event of dispute
    - US: customer is right
    - UK: bank is right
  - Investment in risk management
    - high in US
    - low in UK

Credit cards

- Liability is normally with bank
  - consumers, merchant have due care standard
  - fee to credit card agency depends on circumstances
  - banks have incentive to invest in profiling and other risk management techniques
  - Debit cards have adopted similar liability rules
Uniform Commercial Code

- UCC Section 2A (or 4A)
  - made liability for electronic transfer explicit
  - resulted in tighter security

Economics of liability

- Assign liability to party who has most influence over expected costs
  - ATM: bank
  - Credit cards:
    - bank
    - merchant
    - consumer
  - Electronic transfers: ?

Research plan

- Examine systems, identify weaknesses
- Identify who can correct weaknesses
- Assign liability appropriately
- Comments
  - has to be done at a fairly general level
  - hope for broad principles

Simple model

- \( P(e_1, e_2) = \text{probability of not failing} \)
- \( v_1 = \text{value if success} \)
- \( c_i = \text{cost of effort to avoid failure} \)
- Social objective
  - \( P(e_1, e_2)(v_1 + v_2) - c_1 e_1 - c_2 e_2 \)
- Private objective
  - \( P(e_1, e_2)v_1 - c_1 e_1 \)

Total effort model

- Assume \( P(e_1, e_2) = P(e_1 + e_2) \)
  - pure public goods model
  - social optimum: party with least cost of effort does all the work
  - private equilibrium: one party does all the work
    - “right party” does the work
    - but puts in too little effort

Liability and incentives

- Make party with least cost bear costs incurred by other party in case of failure:
  - \( P(e_1 + e_2)v_1 - c_1 e_1 - (1 - P(e_1 + e_2))v_2 \)
  - may want to compensate this party if there is a participation constraint
  - only need liability “on the margin”
Weakest link

- Weakest link analysis
  - maybe technology should be $P(\min(e_1, e_2))$
  - Hirschleifer (19??)
- General results
  - socially want less security in weakest link case (because it is more costly)
  - Private equilibrium is closer to social optimum as number of agents increases

Weakest link, continued

- Always a (0,0) equilibrium
- Nice ranking of social optimum and private equilibrium in total effort compared to weakest link
- Can also examine “best shot”, where $P(\max(e_1, e_2))$
  - several defenses, only strongest matters

Probability of detection

- Detection
  - counterfeiting
  - Pachinko parlor smart cards
  - intellectual property piracy
- Fundamental negative feedback
  - the more the criminal does, the more likely he is to get caught

Model

- Notation
  - $x$=level of activity
  - $\pi(x)$=probability of detection
  - $px$ = revenue
  - $F$=fine if caught
  - $K$=fixed costs of production

Analysis

Max $[1-\pi(x)] px - \pi(x) F - K$
  - rearranged: $px - \pi(x)[px+F] - K$
  - behaves like $px - c(x) - K$
  - AC=MC determines MES, equilibrium price
  - looks just like intermediate micro
  - can examine comparative statics wrt
    - $K$, $F$, $\pi(x)$
    - which policy variables are most effective?

Dissemination of practice

- Anderson: comparison to airlines and safety engineering to security
- Public v private incentives
  - disclosure
    - Y2K liability act
  - role of insurance companies
  - public role such as CERT
  - combination of public and private
Public vs private security

- Police or bodyguards?
  - Bodyguards = better incentives
  - Policy = more cost effective
- Build wall around each house or around the city?
  - Military and civilian concerns
  - Criminal activity, terrorism, war

Conclusion

- More baking needs to be done!
- Interesting theory
- Security analysis
  - Identify, classify weaknesses
  - Also should determine responsibility/liability