Countering Hidden-Action Attacks on Networked Systems

Tyler Moore

University of Cambridge

Workshop on the Economics of Information Security, 2005

Outline

UNIVERSITY OF CAMBRIDGE

Motivation

- Asymmetric information inspires a class of hidden-action attacks: actions made attractive by a lack of observation
- Classic economics example: insurance companies cannot easily monitor their customer's behaviour so many behave recklessly
- Hidden-action in computer networks
  - Routers dropping selected packets
  - Nodes redirecting traffic to eavesdrop on conversations
  - Users in a file-sharing system "free-riding"

UNIVERSITY OF CAMBRIDGE

Available Countermeasures

So what can be done to address hidden-action attacks?

- In economics, contracts are devised to compensate agents capable of hidden-action
  - Distributed algorithmic mechanism design
  - Side-payments often burdensome to implement
  - Accepts system attributes as unchangeable
- We instead turn to social capital theory to undermine the potential for hidden-action
  - Node interactions
  - Network topology
  - Enforcement mechanisms

UNIVERSITY OF CAMBRIDGE

Contributions

- Define hidden-action attack category
- Identify hidden-action attacks in computer networks
- Demonstrate a contradiction between the environmental assumptions of peer-to-peer networks and the requirements for viable reputation systems
- Leverage results from social capital theory to improve network topology design and node interaction

UNIVERSITY OF CAMBRIDGE

Why Social Capital?

Social capital analyses how human societies build institutions for facilitating credible transactions between mutually suspicious parties

1. Threat of punishment to deter misbehaviour
   - External or mutual enforcement
2. Resource allocation mechanism
   - Markets or communitarian institutions

Some institutions better suited to address hidden-action attacks

Increasing relevance to computer network design

- Nodes control behaviour but depend on interactions
- Computer scientists must build the institutions that define node interaction

UNIVERSITY OF CAMBRIDGE

Enforcement Mechanisms

- External enforcement
  - Transactions translated into an independently verifiable contract
  - Enforcer does not participate in any transactions
  - Requires access to trusted, centralised mediator
- Mutual Enforcement
  - In many societies, members cannot rely upon an impartial third party
  - Transacting members punish misbehaviour
  - Scalable, decentralised approach—effective when environmental assumptions are met

UNIVERSITY OF CAMBRIDGE

Market Failures and Communitarian Institutions

- Market institutions
  - Accommodates large populations with diverse interests
  - Low anticipation of future interactions
  - Repeated interaction with external enforcer, not each other, facilitate trust
  - Hidden-information during node selection
  - Hidden-action during node interaction
- Communitarian institutions
  - Grameen banks in Bangladesh
  - Small group size ensures repeated interactions
  - Low cost to monitor for (and punish) any misbehaviour
  - Undermines hidden-action attacks with mutual observation

UNIVERSITY OF CAMBRIDGE

Hidden-Action Attacks Defined

Agent engaging in a transaction

- Can abide by (A) or break (B) the agreement
- Compare two operating environments
  - m: observation is difficult (e.g., market mechanism backed by external enforcement)
  - c: observation is easy (e.g., communitarian institution mutually enforced)

Expected utility for the agent

$$u_A = v_A - d_A$$

$$u_B = v_B - d_B - P(\text{detection}|B) * \text{penalty}$$

$$v : \text{value of action}, d : \text{disutility of action}$$

- Assume more costly to cooperate ($d_A > d_B$)
- More valuable individually to deviate ($v_B > v_A$)

Hidden-Action Attacks Defined (ctd.)

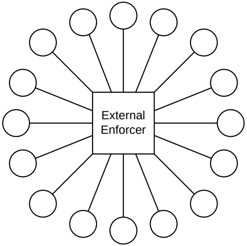
Definition An action B is considered a *hidden-action attack* whenever its benefits and costs to an agent satisfy the following inequalities:

$$P_m(\text{detect}|B) * \text{penalty}_m < (v_B - d_B) - (v_A - d_A) < P_c(\text{detect}|B) * \text{penalty}_c$$

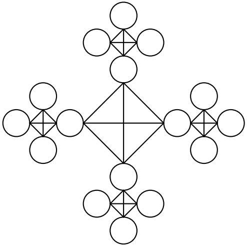
- Hidden-action attacks may occur whenever the *net utility gain from deviating* lies between the expected penalty enforced when observation is unlikely and the penalty enforced when observation is likely
- Definition suggests that increasing observation along with a credible threat of punishment can obviate hidden-action attacks

UNIVERSITY OF CAMBRIDGE

Exploiting Social Capital to Increase Observation



Market-style Institutions



Communitarian Institutions

- Network topology design
  - Small, densely-connected subgroups
  - Constrained connectivity
  - Fosters repeated interactions
  - Supports efficient observation
  - Comes at price of allocative inefficiency

Hidden-Action in Computer Networks

- Network interconnection enables hidden-action
  - Across the Internet, global interconnection is unavoidable
  - More specialised applications, however, are capable of constraining relevant attributes
- Attacks
  - Faked information aggregation in sensor networks
  - Selective forwarding in routing protocols
  - Redirecting traffic for eavesdropping
  - P2P free-riding

UNIVERSITY OF CAMBRIDGE

Hidden-Action in Peer-to-Peer Systems

- Environmental assumptions of P2P file-sharing systems
  - Large member populations
  - Universal addressability
  - High turnover
  - Inexpensive/costless identities
- Proposed free-riding solutions use mutual enforcement
  - Direct contradiction of social capital research!
  - Mutual enforcement mechanisms require:
    1. Repeated interactions
    2. Far-sighted nodes
    3. Sufficient capability to punish deviation
  - Presently, P2P systems meet none of these requirements
  - Changes to network topology and interaction required

Countermeasures for Hidden-Action Attacks

- Resources available to the security engineer
  - Create monitoring threat
  - Change network structure and operation
- Build locality into network topology
  - Place interacting nodes in close proximity whenever possible
  - Arrange nodes in restricted neighbourhoods
- Incorporate mutual dependence between nodes to complete tasks

UNIVERSITY OF CAMBRIDGE

Towards a Communitarian Institution for Enforcing Network Behaviour

- Neighbourhood topology
  - In many existing systems, node neighbours are selected based on random discovery (e.g., Gnutella) or random distribution (e.g., Chord)
  - Neighbour selection should connect nodes with similar interests
  - Critical for establishing repeated interactions and efficient observation
- Some requirements and open challenges
  - Node discovery mechanism
  - Network addressability restrictions
  - Efficient monitoring techniques
  - Effective punishment strategies

Discussion

- System attributes for mutual enforcement
  - Diversity vs. Solidarity of Interests
  - Instrumental vs. Expressive Actions
- Negative implications of communitarian institutions
  - Inefficient resource allocation
  - Tendency towards risk correlation
  - Privacy concerns
- Security maintenance costs often high in decentralised networks
  - Reputation systems and accounting mechanisms introduce high overhead
  - Minimising these costs is a fundamental challenge
  - Constructing network topologies and interactions to minimise hidden-action may reduce overhead

UNIVERSITY OF CAMBRIDGE

Open questions

- Is mutual enforcement the only viable mechanism for deterring misbehaviour in decentralised networks?
- Can external enforcement be deployed without resorting to centralisation?
- How and when can network topologies be constrained without burdening or limiting users?

UNIVERSITY OF CAMBRIDGE

Conclusions

- We have defined an economic category of hidden-action attacks
- We have turned to results from social capital theory to align incentives instead of relying on side payments
- We have found that many existing systems must change node topology and interactions for self-enforcement to work

UNIVERSITY OF CAMBRIDGE