Network Economics and Security Engineering

Tyler Moore
(joint with Ross Anderson and Shishir Nagaraja)

Computer Laboratory
University of Cambridge

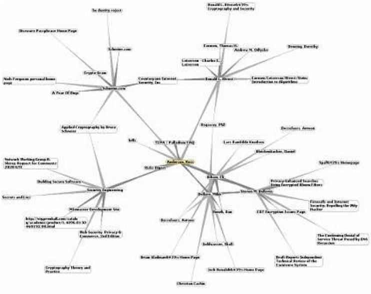
DIMACS
January 18, 2007

Outline

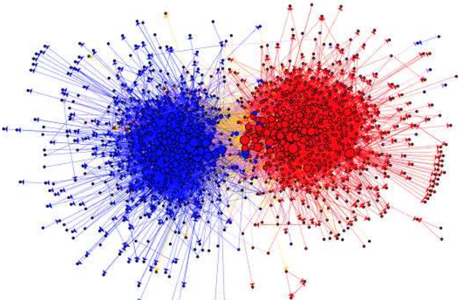
Motivation

- Many computing applications are network-based
  - World-wide web
  - Internet backbone
  - Peer-to-peer networks
  - Wireless sensor networks
  - Social networks
- Network externalities matter: the decisions of others impact a user's best response
- Interactions on these networks can be modeled as repeated games with evolving strategies
- Network properties influence dominant strategy outcomes

How do we represent a network?



http://www.cl.cam.ac.uk/~rja14/

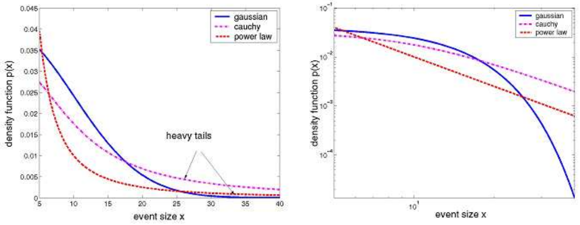


Community structure of political blogs, 2004 US presidential elections (Adamic and Glance 2005)

Relevant network properties

- Network topology
- Network dynamics
- Adversarial model
  - Different attacker goals
  - Different attacker capabilities

Network topology



- Fully-connected graph
- Lattice
- Random graph (Erdős-Rényi)
- Geometric random graph
- Scale-free degree distribution
- Small-world topology

Network dynamics

- Node mobility
  - Lessens likelihood of repeated interaction
  - Allows malicious nodes to maximize attack
- Churn
  - Lessens likelihood of repeated interaction
  - Makes punishment by exclusion difficult
  - Makes Sybil attacks likely
- Intermittent connectivity
  - Makes fair resource contribution difficult to establish
- Each of the above dynamics creates an informational asymmetry

Attacker goals

- Network partition
  - Good strategy for a communications network, maybe not for a file-sharing network with built-in redundancy
- Disrupt operations of ‘normal’ protocols (e.g., message routing)
- Avoid detection and punishment
- Maximize eavesdropping capability

Attacker capabilities

- Global knowledge
  - Powerful adversary can identify central nodes
- Local knowledge
  - Random walk to infer network topology

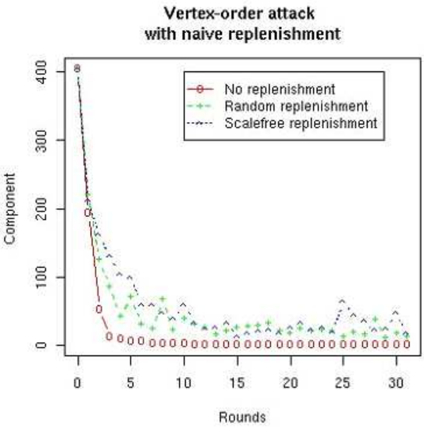
Topology of covert conflict

- Scale-free network
- No application-level network dynamics (mobility, churn, etc.)
- Attacker goal: network partition
- Defender goal: maximize connectivity
- Attacker has global knowledge of network topology, defender has local knowledge
- Goal: study interaction between dynamic attack and defense strategy

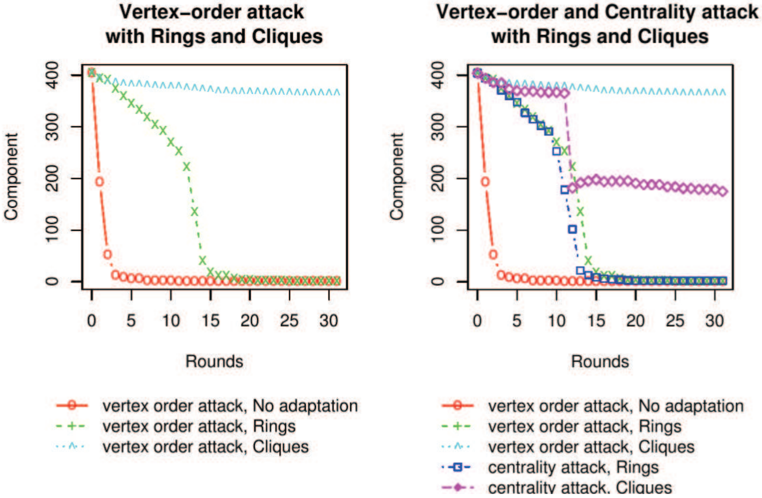
Attack and defense mechanisms

- Attack mechanisms
  - Remove nodes with high degree
  - Remove nodes with high betweenness centrality
- Defense mechanisms
  - Naive replenishment
  - Localized rings
  - Localized cliques

Attack under naive replenishment



Attack and ring/clique defenses



- We would like to apply a similar repeated game simulation framework to other network applications
  - Vary attacker models and goals
  - Vary network topology and dynamics to study effect on security mechanisms
  - Test viability of security mechanisms by varying strategies
- Promising applications
  - Communications surveillance by a limited adversary(Danezis and Wittneben, WEIS 2006)
  - Punishment mechanisms in decentralized computer networks

Punishment mechanisms in decentralized computer networks

- When devices misbehave, often there is no central authority available to identify and punish malicious behavior
- Solution: collective-decision mechanism
    - Reputation system
    - Blackballing with threshold voting
- Attacker goals
    - Avoid punishment while misbehaving
    - Abuse strategy to disconnect the network
- We have explored this space, and have proposed alternative mechanisms

Alternative mechanisms for addressing misbehavior

- Blackballing
  - Nodes cast accusatory votes upon observing misbehavior; once enough votes are cast against a node, it is removed
- Reelection
  - Devices cast positive votes affirming their friends; strangers only interact when they can demonstrate having a sufficient number of friends
- Suicide
  - Nodes unilaterally decide when to remove a malicious node, but must sacrifice itself to demonstrate its sincerity

Open questions in the strategy space

- For blackballing and reelection, nodes can individually set thresholds according to their risk attitude
- Network topology and dynamics determine which strategy works best
    - Scale-free degree distribution makes high-degree nodes immune to thresholds and low-degree nodes susceptible
    - Likewise, suicide can be used to target high-value nodes
- Which strategy, if any, will dominate?

Potential game frameworks

- Hiding attacker
  - Initially, half of nodes are assigned to each strategy
  - Small fraction of nodes set as malicious (attacker goal: avoid punishment)
  - Each round:
    1. Attack (some nodes misbehave)
    2. Defend (implement strategy)
    3. Adapt strategy if node identifies an unpunished neighbor
- Active attacker
  - Initially, half of nodes are assigned to each strategy
  - Small fraction of nodes set as malicious (attacker goal: remove as many honest nodes as possible)
  - Each round:
    1. Attack (malicious nodes falsely accuse honest nodes)
    2. Defend (honest nodes try to punish attackers)
    3. Probabilistically change strategy if node identifies unpunished neighbors

Conclusions

- The structure and dynamics of networks can vary greatly
- It is not well understood how differences in network composition impact secure operation
- Simulations using a repeated game framework looks promising
- Much more work to be done!

More. . .

- http://www.cl.cam.ac.uk/~twm29/