Security Decision Making in Interdependent Organizations

Presented by R. Ann Miura-Ko

Joint work with Benjamin Yolken, John Mitchell and Nicholas Bambos

Risk Management

- Security: not a technology issue alone
- Budgets and resources are limited
- Human error can lead to risk

- Should I invest in more user authentication?
  - Which kind is most effective?
- Do I worry more about a high probability, low loss event or a low probability, high loss event?

Risk Management

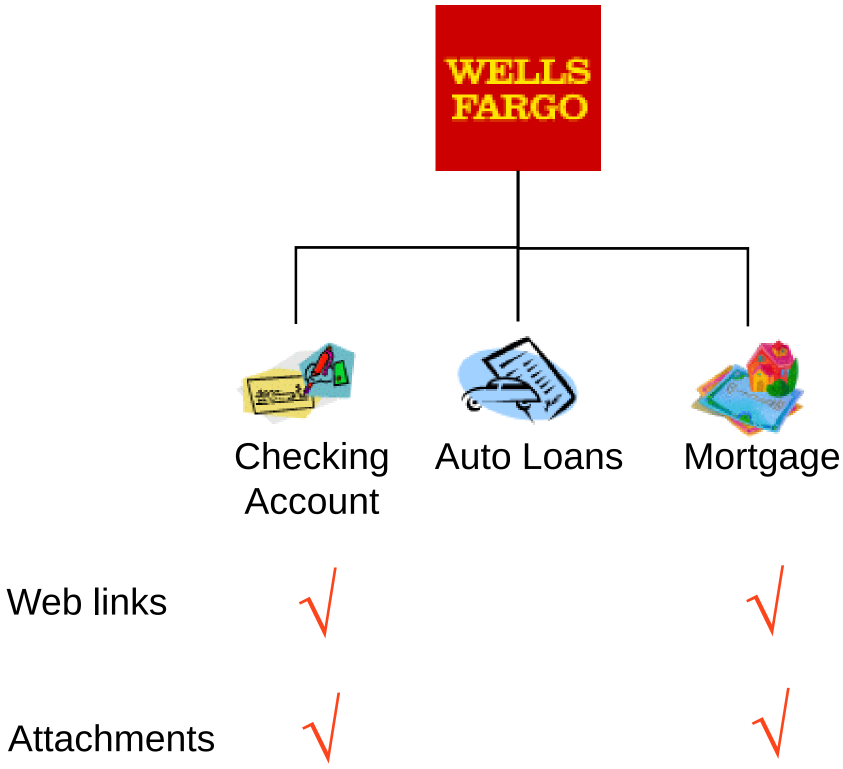
- Why is risk management of security hard?
  - Measurement is difficult
  - User incentives generally not aligned
- Security as an optimization problem
  - Dynamic resource allocation under constraints
  - Game played against an adversary

Model Fundamentals

- Companies make investments in security
- Your security depends on:
  - Own investments
  - Neighbors' investments
- Neighbors:
  - Relationship ties their security to yours
- Relationship:
  - Beneficial
  - Harmful

Customer Education Effort

- Customers receive email communications from multiple departments at a bank
- Each product group constructs own email policy
- Inconsistent messaging $\Rightarrow$ *shared risk*

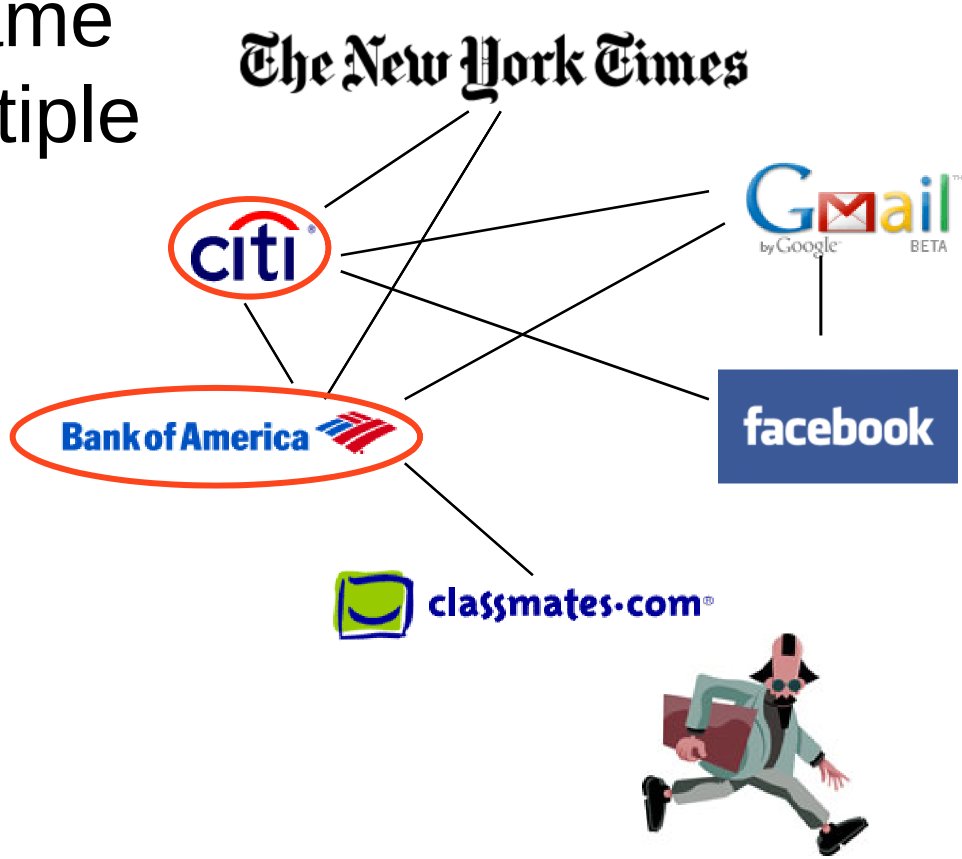


Anti-Spam

- Investment in email path verification
  - Sender ID
  - Sender Policy Framework
- Two types of companies:
  - Email service provider
  - Business / organization
- Email path verification can benefit or damage anti-spam efforts of neighbors
- *Will everyone implement?*

Web Authentication

- Same / similar username and password for multiple sites
- Security not equally important to all sites



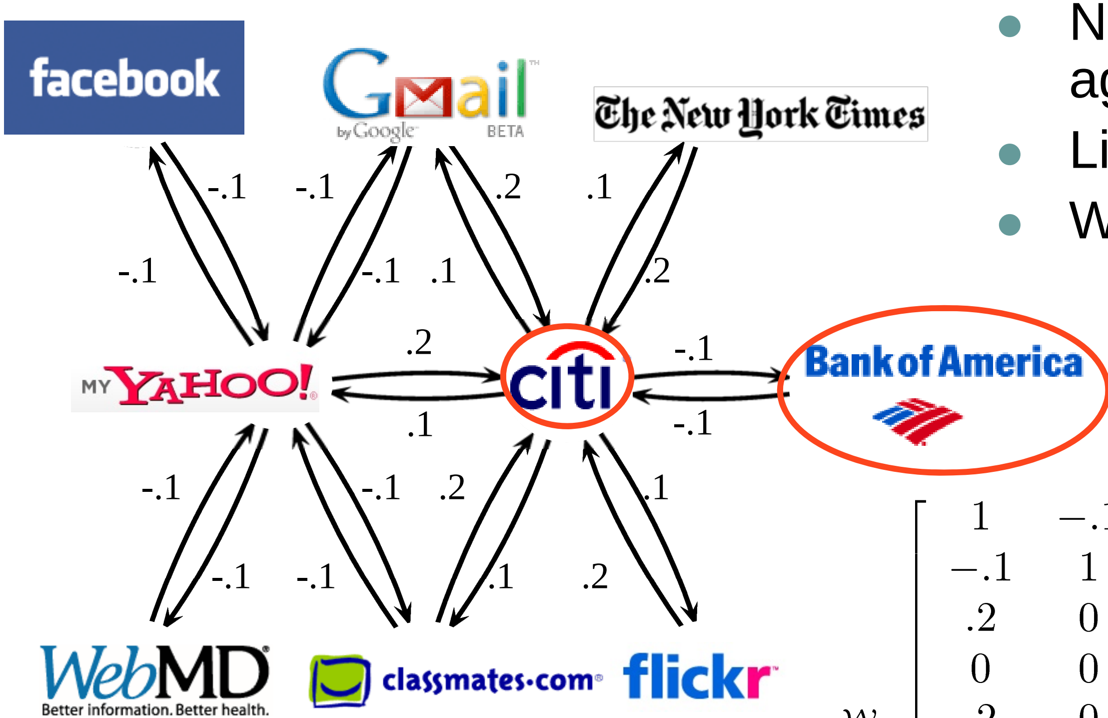
Shared risk for all

Motivation

- Many situations where this type of model makes sense
  - Peer-to-peer networks and security
  - Social networks and privacy
  - Health information sharing between hospitals
- Interactions can be beneficial as well as detrimental

- How much free riding occurs?
- Who invests and how much?

Network Model



- Network = Directed Graph
  - Nodes = Decision making agents
  - Links = influence / interaction
  - Weights = degree of influence

$$\mathbf{W} = \mathcal{W}^T$$

$$\mathcal{W} = \begin{bmatrix} 1 & -.1 & .1 & 0 & .1 & .1 & 0 & .1 & .1 \\ -.1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ .2 & 0 & 1 & -.1 & -.1 & 0 & -.1 & -.1 & 0 \\ 0 & 0 & -.1 & 1 & 0 & 0 & 0 & 0 & 0 \\ .2 & 0 & -.1 & 0 & 1 & 0 & 0 & 0 & 0 \\ .2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -.1 & 0 & 0 & 0 & 1 & 0 & 0 \\ .2 & 0 & -.1 & 0 & 0 & 0 & 0 & 1 & 0 \\ .2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Incentive Model

- Each agent, *i*, selects investment, x_i
- Security of *i* determined by total effective investment:

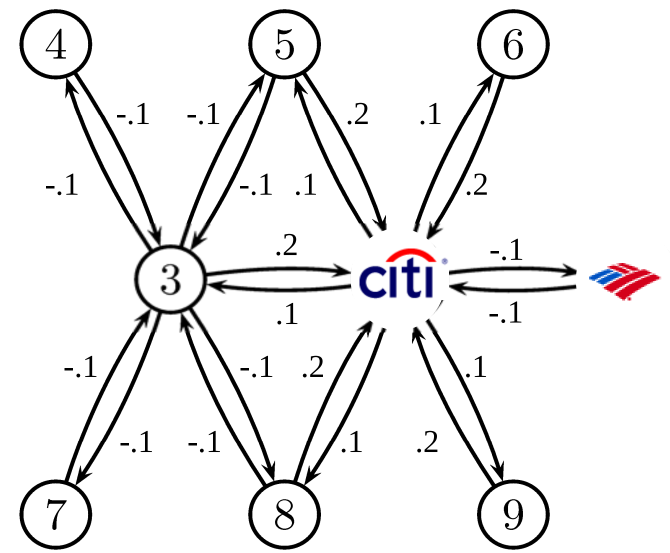
$$(\mathbf{Wx})_i = \sum_{j=1}^{N} w_{ij} x_j$$

- Benefit received by agent i:

$$V_i(\mathbf{Wx})_i$$

- Cost of investment: $c_i x_i$
- Net benefit:

$$U_i(\mathbf{x}) = V_i((\mathbf{Wx})_i) - c_i x_i$$



$$V_i(\mathbf{Wx})_i = \beta_i log((\mathbf{Wx})_i)$$

$$c_i = 1$$

$$\beta_i = 1$$

$$U_i(\mathbf{x}) = \beta_i log((\mathbf{Wx})_i) - x_i$$

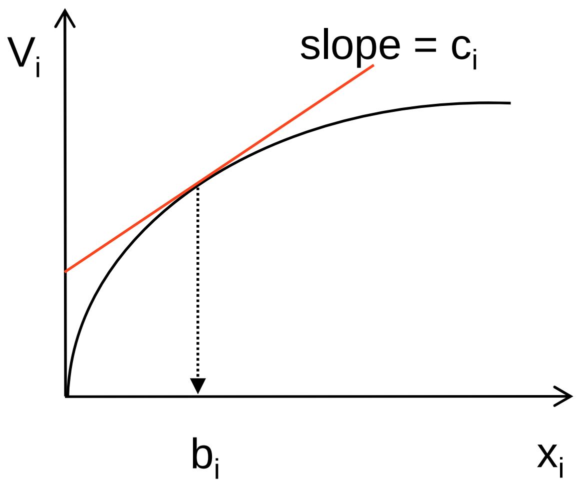
$$\beta_{citi} = \beta_{BofA} = 10$$

How will agents react?

- Single stage game
- All agents maximize their utility function:

$$U_i(\mathbf{x}) = V_i((\mathbf{W}\mathbf{x})_i) - c_i x_i$$
$$U_i'(\mathbf{x}) = 0 \Rightarrow V_i'(\bullet) = c_i$$

- b_i is where the marginal cost = marginal benefit for agent i
- If neighbor's contribution > b_i, x_i=0
- If neighbor's contribution < b_i, x_i = difference



How will agents react?

- All agents maximize their utility function:

$$U_i(\mathbf{x}) = \beta_i log((\mathbf{W}\mathbf{x})_i) - x_i$$

- b_i is where the marginal cost = marginal benefit for agent i

$$\beta_i \frac{1}{b_i} - 1 = 0 \Rightarrow b_i = \beta_i$$

- Each node seeks a level of b_i effective investment

$$b = [10\ 10\ 1\ 1\ 1\ 1\ 1\ 1\ 1]$$

What is an equilibrium?

- Nash Equilibrium
  - Stable point (vector of investments) at which no agent has incentive to change their current strategy

$$U_i(x_i, x_{-i}) \geq U_i(x_i', x_{-i}) \forall i, x_i \in [0, \infty)$$

  - This happens when:

$$(\mathbf{Wx})_i = b_i \text{ if } x_i > 0$$
$$(\mathbf{Wx})_i \geq b_i \text{ if } x_i = 0$$

  - Leverage Linear Complementarity literature

Analysis of the Model

- Diagonal Dominance:

$$\sum_{j \neq i} |w_{ij}| \leq |w_{ii}| = 1 \forall i$$

- Existence and uniqueness of Nash Equilibrium
- Convergence to the Nash Equilibrium in a distributed, asynchronous manner

Free Riding

- Since others are contributing to an agent's investment, some may choose not to invest at all
- Measure of contribution relative to what they need, *free riding index:*

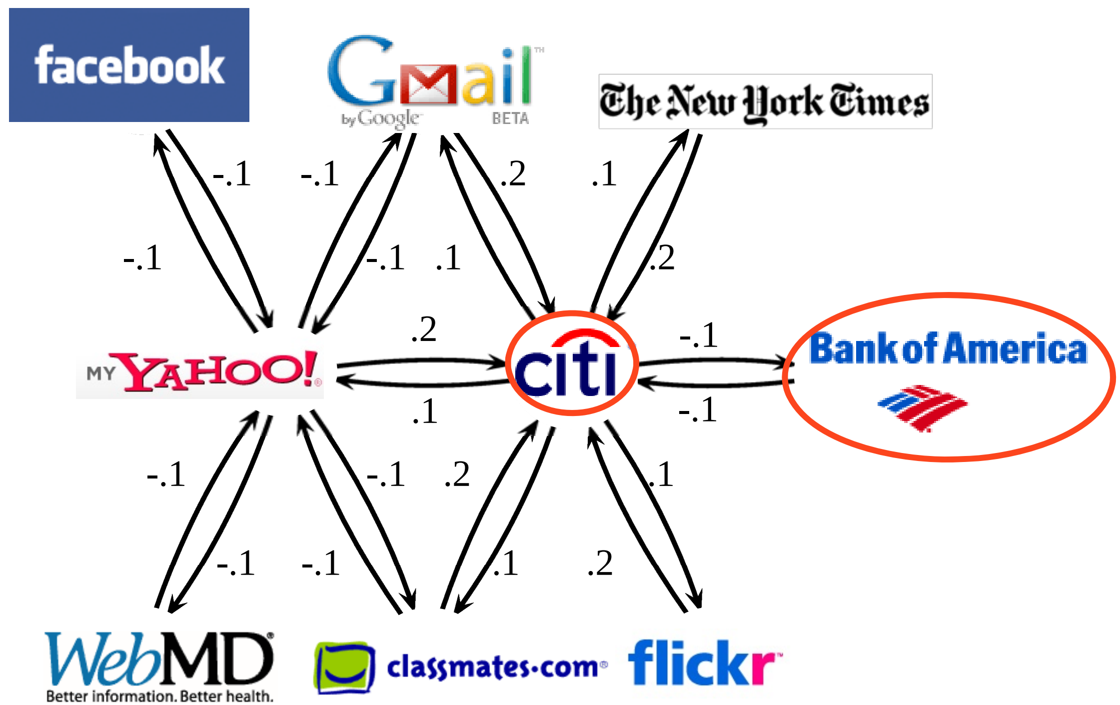
$$\gamma_i = \frac{(\mathbf{Wx})_i - x_i}{b_i}$$

Web Authentication

- Utility function:

$$U_i(\mathbf{x}) = \beta_i log(\mathbf{W}\mathbf{x}) - x_i$$

Firm	x_i	γ_i
1	11.09	-0.11
2	11.11	-0.11
3	0.09	0.91
4	1.01	-0.01
5	0	1.10
6	0	1.11
7	1.01	-0.01
8	0	1.10
9	0	1.11



Conclusion

- Application of risk management modeling to real scenarios in security

- Future direction:
  - Optimization to improve equilibria
  - Possible relaxations of diagonal dominance restriction