Cybersecurity and Financial Services

Anna Nagurney

Isenberg School of Management, University of Massachusetts
Amherst, Massachusetts 01003

INFORMS Conference on Business Analytics
& Operations Research, Boston, Massachusetts
March 30 - April 1, 2014

ISENBERG
SCHOOL OF MANAGEMENT

Funding for our project, *Cybersecurity Risk Analysis and Investment Optimization*, provided by:

with Co-PIs: W. Burleson, M. Sherman, S. Solak, and C. Misra, all at UMass Amherst.

This project aims to assess the vulnerability of financial networks with a focus on cybersecurity.

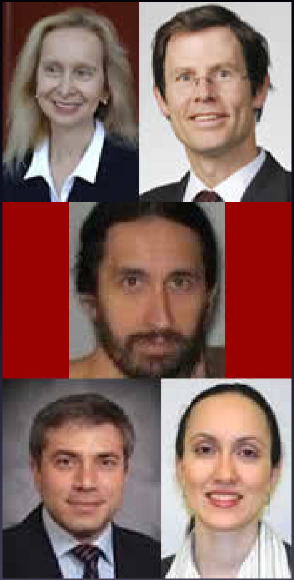
Also support for the project: *Collaborative Research: Network Innovation Through Choice*, which envisions a Future Internet Architecture, provided by:

with Co-PIs: T. Wolf of UMass, K. Calvert and J. Griffoen of U. of Kentucky, G. Rouskas and R. Dutta of NCState, and I. Baldine of RENCI is also gratefully acknowledged.

Outline

- Background and Motivation
- The Financial Network Model – A System Perspective
- Cyber Crime and Financial Services
- A Network Economic Model of Cyber Crime
- Envisioning a New Kind of Internet – ChoiceNet
- Summary and Conclusions

Background and Motivation



The vision of our ACSC project, *Cybersecurity Risk Analysis and Investment Optimization* was to develop:

- rigorous models for cybersecurity risk,
- models for costs and benefits of various cybersecurity technologies,
- techniques for integrating these models into higher level models that account for other risks and risk management expenditures.

University of Massachusetts Amherst Team:

- Wayne Burleson
- Anna Nagurney
- Mila Sherman
- Senay Solak
- Christopher Misra.

The Internet has transformed the ways in which individuals, groups, organizations communicate, obtain information, access entertainment, and conduct their economic and social activities.

70% of households and 94% of businesses with 10 or more employees are online with an immense growth in mobile devices and social media. In 2012, there were over 2.4 billion users.

Financial Services

Banks and other financial service providers depend on Internet technology for information dissemination and timely business transactions.

The advances in information technology and globalization have further shaped today's financial world into a complex network, which is characterized by distinct sectors, the proliferation of new financial instruments, and with increasing international diversification of portfolios.

It is crucial for decision-makers in financial systems (managers, executives, regulators, IT professionals and cybersecurity specialists) to be able to identify a financial network's vulnerable components in order to protect the functionality of the network.

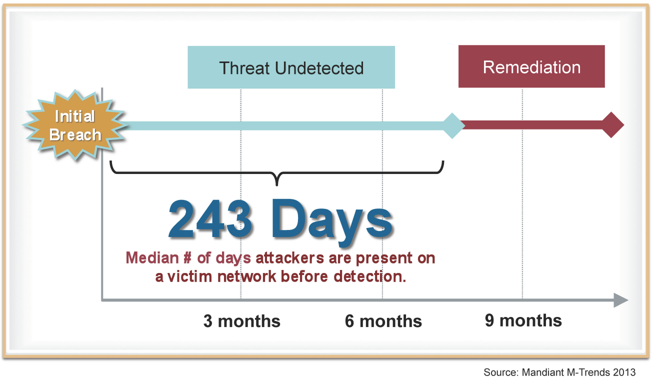
Putting Cyber Crime in Context

Putting Malicious Cyber Activity in Context			
CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURSE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global Cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashed	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Source: The Economic Impact of Cybercrime and Cyber Espionage, Center for Strategic and International Studies, July 2013, sponsored by McAfee.

Cyber Attacks

Every minute, of every hour, of ever day, a major financial institution is under attack (Wilson in *The Telegraph*, October 6, 2013).



Preparation, prediction, and protection are key - which are the weakest links?

Financial Networks

In 2008 and 2009, the world reeled from the effects of the financial credit crisis; leading financial services and banks closed (including the investment bank Lehman Brothers), others merged, and the financial landscape was changed for forever.

Financial Networks

In 2008 and 2009, the world reeled from the effects of the financial credit crisis; leading financial services and banks closed (including the investment bank Lehman Brothers), others merged, and the financial landscape was changed for forever.

The domino effect of the U.S. economic troubles rippled through overseas markets and pushed countries such as Iceland to the verge of bankruptcy.

Financial Networks

In 2008 and 2009, the world reeled from the effects of the financial credit crisis; leading financial services and banks closed (including the investment bank Lehman Brothers), others merged, and the financial landscape was changed for forever.

The domino effect of the U.S. economic troubles rippled through overseas markets and pushed countries such as Iceland to the verge of bankruptcy.

Financial service firms were heavily impacted by the recession and are also dealing with increasing numbers of cyber attacks.

Financial Networks

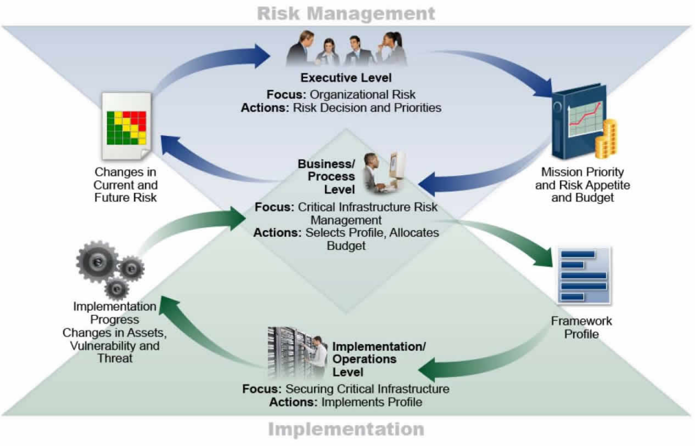
In 2008 and 2009, the world reeled from the effects of the financial credit crisis; leading financial services and banks closed (including the investment bank Lehman Brothers), others merged, and the financial landscape was changed for forever.

The domino effect of the U.S. economic troubles rippled through overseas markets and pushed countries such as Iceland to the verge of bankruptcy.

Financial service firms were heavily impacted by the recession and are also dealing with increasing numbers of cyber attacks.

One third of all cyber breeches in 2012 affected financial organizations and 74% of financial service firms in a recent survey considered cyber crime as a high or very high risk (Tendulkar (2013)).

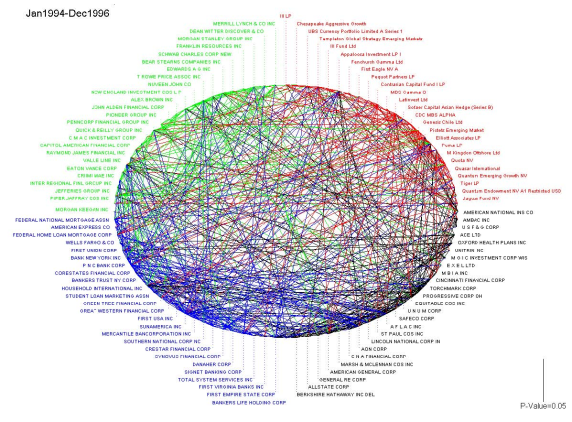
It’s About Risk Management



Source: Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), February 12, 2014

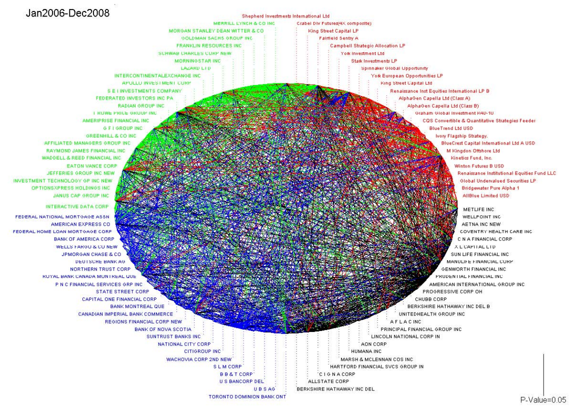
Financial Networks and Operations Research

Empirical Evidence: Jan. 1994 - Dec. 1996 - Connectivity, Vulnerability



Granger Causality Results: Green Broker, Red Hedge Fund, Black Insurer, Blue Bank Source: Billio, Getmansky, Lo, and Pelizzon (2011)

Empirical Evidence: Jan. 2006 - Dec. 2008 - Connectivity, Vulnerability



Granger Causality Results: Green Broker, Red Hedge Fund, Black Insurer, Blue Bank Source: Billio, Getmansky, Lo, and Pelizzon (2011)

The Financial Network Model – A System Perspective

Financial Networks

Nevertheless, there is very little literature that addresses the vulnerability of financial networks.

Our network performance measure for financial networks captures both economic behavior as well as the underlying network/graph structure and the dynamic reallocation after disruptions.

The results are contained in the paper, "Identification of Critical Nodes and Links in Financial Networks with Intermediation and Electronic Transactions," A. Nagurney and Q. Qiang, in *Computational Methods in Financial Engineering*, E. J. Kontoghiorghes, B. Rustem, and P. Winker, Editors, Springer, Berlin, Germany (2008), pp 273-297; see also the book, *Fragile Networks: Identifying Vulnerabilities and Synergies in an Uncertain World*, A. Nagurney and Q. Qiang, Wiley & Sons, 2009. Results are applicable to cybersecurity.

The Financial Network Model

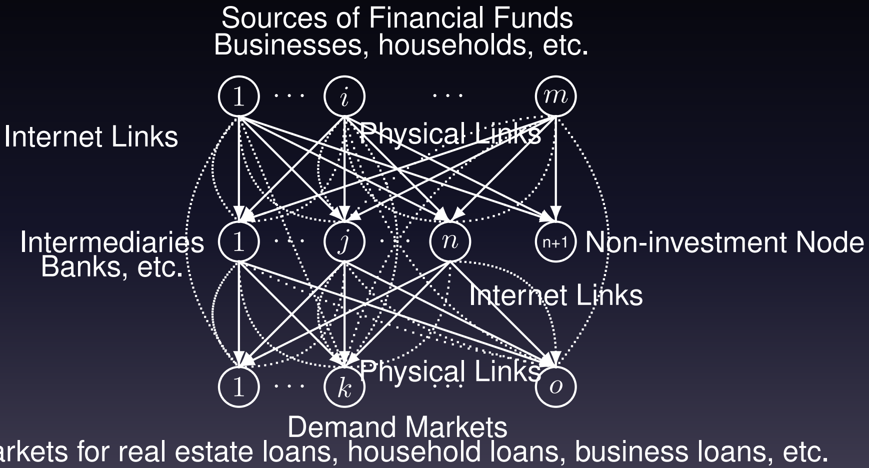


Figure 1: The Structure of the Financial Network with Intermediation

The Financial Network Model

- Both sources of funds and the financial intermediaries seek to maximize net returns and to minimize the risk.

The Financial Network Model

- Both sources of funds and the financial intermediaries seek to maximize net returns and to minimize the risk.

- Consumers at the demand markets, in turn, compare the price charged plus the transaction cost with the elastic price that they are willing to pay in determining their ultimate transactions.

The Financial Network Model

- Both sources of funds and the financial intermediaries seek to maximize net returns and to minimize the risk.

- Consumers at the demand markets, in turn, compare the price charged plus the transaction cost with the elastic price that they are willing to pay in determining their ultimate transactions.

- The competitive game theory model is governed by Nash equilibrium and formulated and solved as a variational inequality problem.

The Financial Network Model

- Both sources of funds and the financial intermediaries seek to maximize net returns and to minimize the risk.

- Consumers at the demand markets, in turn, compare the price charged plus the transaction cost with the elastic price that they are willing to pay in determining their ultimate transactions.

- The competitive game theory model is governed by Nash equilibrium and formulated and solved as a variational inequality problem.

- The underlying dynamics are formulated via projected dynamical systems theory in order to guarantee that the budget and nonnegativity constraints are satisfied. The computational procedure, which tracks the dynamic evolution of the financial flows over time, until an equilibrium state is achieved, and which we also apply to compute the equilibria, is the Euler method.

The Variational Inequality Problem

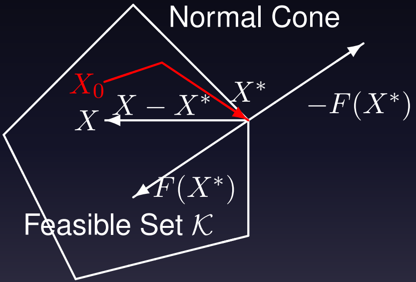
Definition: The Variational Inequality Problem
The finite-dimensional variational inequality problem, $\text{VI}(F, \mathcal{K})$*, is to determine a vector* $X^* \in \mathcal{K}$*, such that:*

$$\langle F(X^*), X - X^* \rangle \geq 0, \quad \forall X \in \mathcal{K},$$

where F *is a given continuous function from* $\mathcal{K}$ *to* R^N*,* $\mathcal{K}$ *is a given closed convex set, and* $\langle \cdot, \cdot \rangle$ *denotes the inner product in* R^N*.*

Geometric Interpretation

In particular, $F(X^*)$ is “orthogonal" to the feasible set $\mathcal{K}$ at the point X^*.



Associated with a VI is a Projected Dynamical System, which provides a natural underlying dynamics associated with travel (and other) behavior to the equilibrium.

The Financial Network Performance Measure

Definition: The Financial Network Performance Measure
The financial network performance measure, $\mathcal{E}^F$, for a given network topology G, and demand price functions $\rho_{3k}(d)$ ($k = 1, 2, \ldots, o$), and available funds held by source agents S, is defined as follows:

$$\mathcal{E}^F = \frac{\sum_{k=1}^{o} \frac{d_k^*}{\rho_{3k}(d^*)}}{o},$$

where o is the number of demand markets in the financial network, and d_k^* and $\rho_{3k}(d^*)$ denote the equilibrium demand and the equilibrium price for demand market k, respectively.

The Importance of a Financial Network Component

The financial network performance is expected to deteriorate when a critical network component is eliminated from the network.

Such a component can include a link or a node or a subset of nodes and links depending on the financial network problem under investigation. Furthermore, the removal of a critical network component will cause severe damage than that of the damage caused by a trivial component.

The importance indicator provides decision-makers with a tool for cybersecurity investments and protection from a system perspective.

The Importance of a Financial Network Component

The importance of a network component is defined as:

Definition: Importance of a Financial Network Component

The importance of a financial network component $g \in G$, $I(g)$, *is measured by the relative financial network performance drop after* g *is removed from the network:*

$$I(g) = \frac{\triangle \mathcal{E}^F}{\mathcal{E}^{\mathcal{F}}} = \frac{\mathcal{E}^F(G) - \mathcal{E}^F(G-g)}{\mathcal{E}^F(G)}$$

where $G - g$ *is the resulting financial network after component* g *is removed from network* G.

A Numerical Example

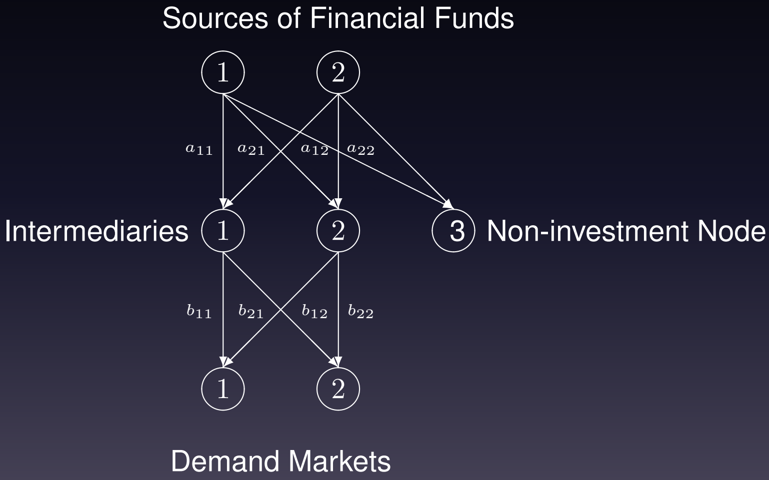


Figure 2: The Financial Network Structure of the Numerical Example

A Numerical Example

The financial holdings for the two source agents in the first example are: $S^1 = 10$ and $S^2 = 10$. The variance-covariance matrices V^i and V^j are identity matrices for all the source agents $i = 1, 2$. The transaction cost function of source agent 1 associated with his transaction with intermediary 1 is given by:

$$c_{11}(q_{11}) = 4q_{11}^2 + q_{11} + 1.$$

The other transaction cost functions of the source agents associated with the transactions with the intermediaries are given by:

$$c_{ij}(q_{ij}) = 2q_{ij}^2 + q_{ij} + 1, \quad \text{for } i = 1, 2; j = 1, 2$$

while i and j are not equal to 1 at the same time.
The transaction cost functions of the intermediaries associated with transacting with the sources agents are given by:

$$\hat{c}_{ij}(q_{ij}) = 3q_{ij}^2 + 2q_{ij} + 1, \quad \text{for } i = 1, 2; j = 1, 2.$$

A Numerical Example

The handling cost functions of the intermediaries are:

$$c_1(Q^1) = 0.5(q_{11} + q_{21})^2, \quad c_2(Q^1) = 0.5(q_{12} + q_{22})^2.$$

We assumed that in the transactions between the intermediaries and the demand markets, the transaction costs perceived by the intermediaries are all equal to zero, that is,

$$c_{jk} = 0, \quad \text{for } j = 1, 2; k = 1, 2.$$

The transaction costs between the intermediaries and the consumers at the demand markets, in turn, are given by:

$$\hat{c}_{jk} = q_{jk} + 2, \quad \text{for } j = 1, 2; k = 1, 2.$$

The demand price functions at the demand markets are:

$$\rho_{3k}(d) = -2d_k + 100, \quad \text{for } k = 1, 2.$$

A Numerical Example

The equilibrium financial flow pattern, the equilibrium demands, and the incurred equilibrium demand market prices are:

For Q^{1*}, we have:

$$q_{11}^* = 3.27, \; q_{12}^* = 4.16, \; q_{21}^* = 4.36, \; q_{22}^* = 4.16.$$

For Q^{2*}, we have:

$$q_{11}^* = 3.81, \; q_{12}^* = 3.81, \; q_{21}^* = 4.16, \; q_{22}^* = 4.16.$$

Also, we have:

$$d_1^* = 7.97, \; d_2^* = 7.97,$$

$$\rho_{31}(d^*) = 84.06, \; \rho_{32}(d^*) = 84.06.$$

The financial network performance is:

$$\mathcal{E} = \frac{\frac{7.97}{84.06} + \frac{7.97}{84.06}}{2} = 0.0949.$$

A Numerical Example

The importance of the links and the nodes and their ranking are reported in the following tables.

Table 1: Importance and Ranking of the Links in Example 1

Link	Importance Value	Ranking
a_{11}	0.1574	3
a_{12}	0.2003	2
a_{21}	0.2226	1
a_{22}	0.2003	2
b_{11}	0.0304	5
b_{12}	0.0304	5
b_{21}	0.0359	4
b_{22}	0.0359	4

A Numerical Example

Table 2: Importance and Ranking of the Nodes in Example 1

Node	Importance Value	Ranking
Source Agent 1	0.4146	4
Source Agent 2	0.4238	3
Intermediary 1	0.4759	2
Intermediary 2	0.5159	1
Demand Market 1	0.0566	5
Demand Market 2	0.0566	5

Discussion

Both source agents choose not to invest a portion of their financial funds. Given the cost structure and the demand price functions, the transaction link between source agent 2 and intermediary 1 is the most important link because it carries a large amount of financial flow, in equilibrium, and the removal of the link causes the highest performance drop assessed by the financial network performance measure.

Similarly, because intermediary 2 handles the largest amount of financial input from the source agents, it is ranked as the most important node in the above network. On the other hand, since the transaction links between intermediary 1 to demand markets 1 and 2 carry the least amount of equilibrium financial flow, they are the least important links.

Cyber Crime and Financial Services

Cyber Crime

- Cyber crimes continue to be quite costly for organizations. The Ponemon Institute (2012) determined that the average annualized cost for 56 benchmarked organizations is $8.9 million per year, with a range from $1.4 million to $46 million each year per company. Last year's average cost per benchmarked organization was $8.4 million.

Cyber Crime

- Cyber crimes continue to be quite costly for organizations. The Ponemon Institute (2012) determined that the average annualized cost for 56 benchmarked organizations is $8.9 million per year, with a range from $1.4 million to $46 million each year per company. Last year's average cost per benchmarked organization was $8.4 million.

- Cyber crime cost varies by organizational size. Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost. However, based on enterprise seats, the Ponemon Institute (2012) determined that small organizations incur a significantly higher per capita cost than larger organizations ($1,324 versus $305).

Cyber Crime

- Cyber crimes continue to be quite costly for organizations. The Ponemon Institute (2012) determined that the average annualized cost for 56 benchmarked organizations is $8.9 million per year, with a range from $1.4 million to $46 million each year per company. Last year's average cost per benchmarked organization was $8.4 million.
- Cyber crime cost varies by organizational size. Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost. However, based on enterprise seats, the Ponemon Institute (2012) determined that small organizations incur a significantly higher per capita cost than larger organizations ($1,324 versus $305).
- All industries fall victim to cyber crime, but to different degrees with defense, utilities and energy, and financial service companies experiencing higher costs than organizations in retail, hospitality, and consumer products.

Cyber Crime and Financial Institutions

According to a recent survey cyber crime is placing heavy strains on the global financial sector, with cyber crime now the second most commonly reported economic crime affecting financial services firms.

Cyber Crime and Financial Institutions

According to a recent survey cyber crime is placing heavy strains on the global financial sector, with cyber crime now the second most commonly reported economic crime affecting financial services firms.

Cyber crime accounted for 38% of all economic crimes in the financial sector, as compared to an average of 16% across all other industries.

Cyber Crime and Financial Institutions

According to a recent survey cyber crime is placing heavy strains on the global financial sector, with cyber crime now the second most commonly reported economic crime affecting financial services firms.

Cyber crime accounted for 38% of all economic crimes in the financial sector, as compared to an average of 16% across all other industries.

Cyber attacks are intrusive and economically costly. In addition, they may adversely affect a company's most valuable asset – its reputation.

Cyber Crime and Financial Institutions

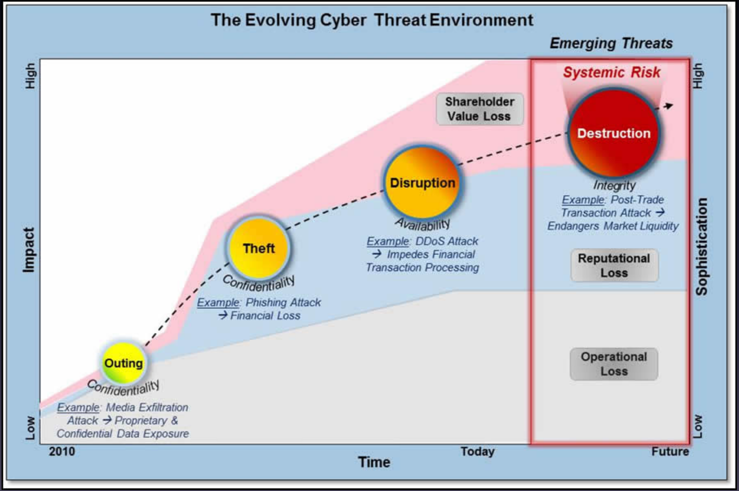
According to a recent survey cyber crime is placing heavy strains on the global financial sector, with cyber crime now the second most commonly reported economic crime affecting financial services firms.

Cyber crime accounted for 38% of all economic crimes in the financial sector, as compared to an average of 16% across all other industries.

Cyber attacks are intrusive and economically costly. In addition, they may adversely affect a company's most valuable asset – its reputation.

Retailers spend 4 percent of their technology budgets on security, compared with 5.5 percent for banks and 5.6 percent for healthcare companies, according to Gartner.

The most costly cyber crimes (58% annually) are those caused by denial of service, malicious insider and web-based attacks. Mitigation may require enabling technologies, intrusion prevention systems, applications security testing solutions and enterprise solutions.

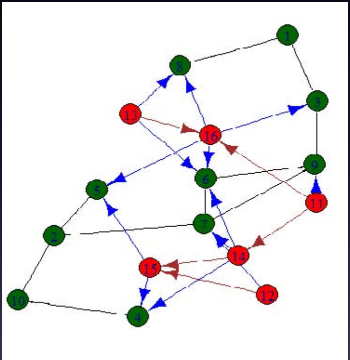


Source: Sarnowski for Booz Allen and Hamilton

A Network Economic Model of Cyber Crime

Network Economics of Cyber Crime

Green Nodes represent Institutions
Red Nodes the Attackers
Red Edges between Attackers can represent collusion or transactions of stolen goods.
Black Edges between Institutions can show sharing of information and mutual dependence.
Blue Edges between the Attacker and Institution can represent threats and attacks.



Network Economics of Cyber Crime

We lay the foundation for the development of network economics based models for cyber crime in financial services.

We use, as the framework, spatial network economic models, for which many advances have been made by operations researchers.

Our view is that financial firms produce/possess commodities (or products) that hackers (criminals) seek to obtain.

Both financial services firms as well as hackers are economic agents.

We assume that the firms (as well as the hackers) can be located in different regions of a country or in different countries. Financial service firms may also be interpreted as prey and the hackers as predators.

Network Economics of Cyber Crime

Commodities or products that the hackers seek to acquire may include: credit card numbers, password information, specific documents, etc.

The financial firms are the producers of these commodities whereas the hackers act as agents and “sell" these products, if they acquire them, at the “going" market prices. There is a “price" at which the hackers acquire the financial commodity from a financial institution and a price at which they sell the hacked product in the demand markets. The former we refer to as the supply price and the latter is the demand price.

Network Economics of Cyber Crime

In addition, we assume that there is a transaction cost associated between each pair of financial and demand markets for each commodity. These transaction costs can be generalized costs that also capture risk.

Network Economics of Cyber Crime

In the financial network cyber crime problem, we seek to determine the commodity supply prices, the demand prices, and the hacked product trade flows satisfying the equilibrium condition that, for each financial commodity, the demand price is equal to the supply price plus the transaction cost, if there is “trade" between the pair of financial and demand markets; if the demand price is less than the supply price plus the transaction cost, then there will be no (illicit) trade.

Network Economics of Cyber Crime

Indeed, if the cyber criminals do not find demand markets for their acquired financial commodities (since there are no consumers willing to pay the price) then there is no economic incentive for them to acquire the financial commodities.

Network Economics of Cyber Crime

Indeed, if the cyber criminals do not find demand markets for their acquired financial commodities (since there are no consumers willing to pay the price) then there is no economic incentive for them to acquire the financial commodities.

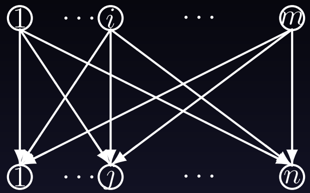
To present another criminal network analogue – consider the market for illegal drugs, with the U.S. market being one of the largest, if not the largest one. If there is no demand for the drugs then the suppliers of illegal drugs cannot recover their costs of production and transaction and the flows of drugs will go to zero.

Network Economics of Cyber Crime

The framework that we utilize as the foundation for our modeling, analysis, and, ultimately, policy-making recommendations is that of spatial economics and network equilibrium. Background can be found in the books by Nagurney (1999, 2003) with analogues to financial networks made in the book by Nagurney and Siokos (1997)

The Model

Financial Service Firms



Demand Markets

Figure 3: A bipartite network of the model with financial institutions and demand markets for hacked products

Denote a typical financial institution by i and a typical demand market by j. Let s_i denote the supply of the commodity associated with i and let π_i denote the supply price of the commodity associated with i. Let d_j denote the demand associated with demand market j and let ρ_j denote the demand price associated with demand market j.

The Model

Let Q_{ij} denote the possible illicit nonnegative commodity trade flow between the firm and demand market pair (i, j) and let c_{ij} denote the nonnegative unit transaction cost associated with obtaining the product between (i, j).

Definition: Market Equilibrium Conditions
The market equilibrium conditions, assuming perfect competition, take the following form: For all pairs of firms and demand markets $(i, j) : i = 1, \ldots, m; j = 1, \ldots, n$:

$$\pi_i + c_{ij} \begin{cases} = \rho_j, & \text{if} \quad Q^*_{ij} > 0 \\ \geq \rho_j, & \text{if} \quad Q^*_{ij} = 0. \end{cases} \tag{1}$$

The Model

The feasibility conditions must hold for every i and j:

$$s_i = \sum_{j=1}^{n} Q_{ij} \tag{2}$$

and

$$d_j = \sum_{i=1}^{m} Q_{ij}. \tag{3}$$

(2) and (3) state that the markets clear and that the supply at each supply market is equal to the sum of the financial commodity flows to all the demand markets. Also, the demand at a demand market must be satisfied by the sum of the commodity shipments from all the supply markets. Let K denote the closed convex set where $K \equiv \{(s, Q, d) | (2)$ and (3) hold$\}$.

The Model

The supply price, demand price, and transaction cost structure is now discussed. Assume that the commodity price associated with a firm may depend upon the supply of the commodity at every firm:

$$\pi = \pi(s) \tag{4}$$

where π is a known smooth function.

The demand price associated with a demand market may depend upon, in general, the demand of the commodity at every demand market:

$$\rho = \rho(d) \tag{5}$$

where ρ is a known smooth function.

The transaction cost between a pair of supply and demand markets may, in general, depend upon the shipments of the commodity between every pair of markets:

$$c = c(Q) \tag{6}$$

The Variational Inequality Formulation

We now present the variational inequality formulation of the equilibrium conditions (1).

Theorem 1. A commodity production, shipment, and consumption pattern $(s^*, Q^*, d^*) \in K$ is in equilibrium if and only if it satisfies the variational inequality problem:

$$\pi(s^*) \cdot (s - s^*) + c(Q^*) \cdot (Q - Q^*) - \rho(d^*) \cdot (d - d^*) \geq 0, \quad \forall (s, Q, d) \in K. \tag{7}$$

Numerical Example

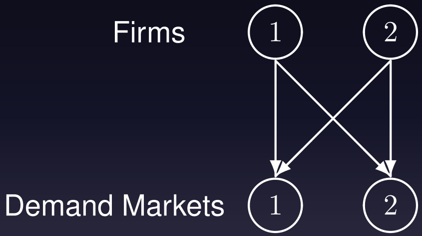


Figure 4: Example Network Topology

Numerical Example

The supply price functions are:

$$\pi_1(s) = 5s_1 + s_2 + 2, \quad \pi_2(s) = 2s_2 + s_1 + 3.$$

The transaction cost functions are:

$$c_{11}(Q) = Q_{11} + .5Q_{12} + 1, \quad c_{12}(Q) = 2Q_{12} + Q_{22} + 1.5,$$

$$c_{21}(Q) = 3Q_{21} + 2Q_{11} + 15, \quad c_{22}(Q) = 2Q_{22} + Q_{12} + 10.$$

The demand price functions are:

$$\rho_1(d) = -2d_1 - d_2 + 28.75, \quad \rho_2(d) = -4d_2 - d_1 + 41.$$

The equilibrium supply, shipment, and consumption pattern is then given by:

$$s_1^* = 3, \quad s_2^* = 2,$$

$$Q_{11}^* = 1.5, \quad Q_{12}^* = 1.5, \quad Q_{21}^* = 0, \quad Q_{22}^* = 2,$$

$$d_1^* = 1.5, \quad d_2^* = 3.5.$$

Numerical Example

The incurred equilibrium supply prices, costs, and demand prices are:

$$\pi_1 = 19, \quad \pi_2 = 10,$$

$$c_{11} = 3.25, \quad c_{12} = 6.5, \quad c_{21} = 18, \quad c_{22} = 15.5,$$

$$\rho_1 = 22.25, \quad \rho_2 = 25.5.$$

Numerical Example

Firm 2 does not “trade" with Demand Market 1. This is due, in part, to the high fixed cost associated with trading between this market pair. Hence, one can interpret this as corresponding to a sufficiently high transaction cost (which can also capture in a generalized setting, the risk of being caught).

The above single commodity model we have generalized to multiple financial commodities.

In addition, we have included a variety of policy interventions.

We have solved problems of this type using variational inequality algorithms with more than 250,000 variables.

Envisioning a New Kind of Internet – ChoiceNet

Envisioning a New Kind of Internet – ChoiceNet

We are one of five teams funded by NSF as part of the Future Internet Architecture (FIA) project. Our project is: *Network Innovation Through Choice* and the envisioned architecture is *ChoiceNet*.

Team:

- University of Kentucky: Jim Griffioen, Ken Calvert
- North Carolina State University: Rudra Dutta, George Rouskas
- RENCI/UNC: Ilia Baldine
- University of Massachusetts Amherst: Tilman Wolf, Anna Nagurney

Network Economic Conundrums and Operations Research to the Rescue

- New architectures are focusing on networking technology, and not on economic interactions. Also, they lack in mechanisms to introduce competition and market forces.

Network Economic Conundrums and Operations Research to the Rescue

- New architectures are focusing on networking technology, and not on economic interactions. Also, they lack in mechanisms to introduce competition and market forces.

- Existing economic models cannot be deployed in today's Internet: no mechanisms in order to create and discover contracts with any provider and to do so on short-time scales, and time-scales of different lengths.

Network Economic Conundrums and Operations Research to the Rescue

- New architectures are focusing on networking technology, and not on economic interactions. Also, they lack in mechanisms to introduce competition and market forces.

- Existing economic models cannot be deployed in today's Internet: no mechanisms in order to create and discover contracts with any provider and to do so on short-time scales, and time-scales of different lengths.

- We have developed multitiered network economic game theory models using novel operations research methodologies, including that of *projected dynamical systems* to study ChoiceNet and to explore the evolution of prices and flows among content and service providers.

Network Economic Conundrums and Operations Research to the Rescue

- Through the a priori evaluation of different business models for Future Internet Architectures, including ChoiceNet, one gains insights into who may win.

Network Economic Conundrums and Operations Research to the Rescue

- Through the a priori evaluation of different business models for Future Internet Architectures, including ChoiceNet, one gains insights into who may win.

- New architectures for the Future Internet, through enhanced authentication and verification services, may also provide more resilient cybersecurity.

ChoiceNet Principles

Competition Drives Innovation!

ChoiceNet Principles

Competition Drives Innovation!

Services are at core of ChoiceNet ("everything is a service")

Services provide a benefit, have a cost Services are created, composed, sold, verified, etc.

ChoiceNet Principles

Competition Drives Innovation!

Services are at core of ChoiceNet ("everything is a service")

Services provide a benefit, have a cost Services are created, composed, sold, verified, etc.

"Encourage alternatives" Provide building blocks for different types of services

ChoiceNet Principles

Competition Drives Innovation!

Services are at core of ChoiceNet ("everything is a service")

Services provide a benefit, have a cost Services are created, composed, sold, verified, etc.

"Encourage alternatives" Provide building blocks for different types of services

"Know what happened" Ability to evaluate services

ChoiceNet Principles

Competition Drives Innovation!

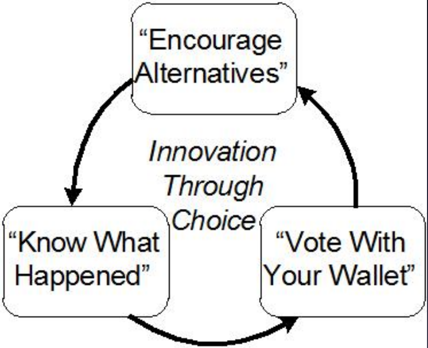
Services are at core of ChoiceNet ("everything is a service")

Services provide a benefit, have a cost Services are created, composed, sold, verified, etc.

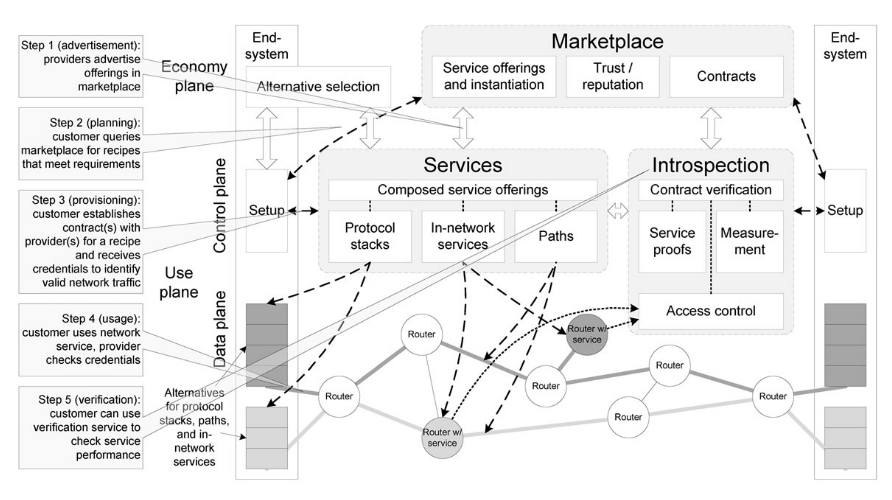
"Encourage alternatives" Provide building blocks for different types of services

"Know what happened" Ability to evaluate services

"Vote with your wallet" Reward good services!



ChoiceNet Architecture



Use Cases Enabled by ChoiceNet

- ChoiceNet / economy plane enables new business models in the Internet

– Very dynamic economic relationships are possible
– All entities get rewarded.

- Examples

– Movie streaming
– reading *The New York Times* in a coffee shop (short-term and long-term contracts)
–Customers as providers.

Summary and Conclusions

- In this presentation, we have overviewed our work on financial services with a focus on vulnerability from a cybersecurity perspective from both a system and a cyber crime perspective. Our "clients" were financial service firms, who, besides dealing with the recession, have also encountered a growing number of cyber attacks.

Summary and Conclusions

• In this presentation, we have overviewed our work on financial services with a focus on vulnerability from a cybersecurity perspective from both a system and a cyber crime perspective. Our “clients" were financial service firms, who, besides dealing with the recession, have also encountered a growing number of cyber attacks.

• In this talk, we also provided an overview of our work on a Future Internet Architecture, known as ChoiceNet, which may provide not only greater flexibility for innovation but also added security in terms of verification and authentication.

Summary and Conclusions

- In this presentation, we have overviewed our work on financial services with a focus on vulnerability from a cybersecurity perspective from both a system and a cyber crime perspective. Our “clients" were financial service firms, who, besides dealing with the recession, have also encountered a growing number of cyber attacks.

- In this talk, we also provided an overview of our work on a Future Internet Architecture, known as ChoiceNet, which may provide not only greater flexibility for innovation but also added security in terms of verification and authentication.

- Our research integrates inputs from practitioners with the goal of providing prescriptive analytics for decision-making.

THANK YOU!

For more information, see: http://supernet.isenberg.umass.edu
Additional references provided upon request.