Cybersecurity Risk Analysis for Enterprise Security
MIT Sloan School, Cambridge, MA. September 19, 2014
I’d like to thank

for support for this workshop.

Also support for some of the research in this presentation has been provided by NSF through the project: Collaborative Research: Network Innovation Through Choice, which envisions a Future Internet Architecture.
Outline

• Background and Motivation
• Networks and Behavior
• Which Nodes and Links Really Matter
• Supply Chains and Risk
• A Network Economic Model of Cyber Crime
• Some Challenging Research Issues
• Envisioning a New Kind of Internet – ChoiceNet
• Summary and Conclusions
Background and Motivation
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.
Cyber crimes continue to be costly for organizations. The Ponemon Institute (2013) determined that the average annualized cost of cyber crime for 60 organizations in their study is $11.6 million per year, with a range of $1.3 million to $58 million. In 2012, the average annualized cost was $8.9 million, an increase in cost of 26 percent or $2.6 million from the results of the 2012 cyber cost study.
Cyber crimes continue to be costly for organizations. The Ponemon Institute (2013) determined that the average annualized cost of cyber crime for 60 organizations in their study is $11.6 million per year, with a range of $1.3 million to $58 million. In 2012, the average annualized cost was $8.9 million, an increase in cost of 26 percent or $2.6 million from the results of the 2012 cyber cost study.

All industries fall victim to cyber crime, but to different degrees with defense, utilities and energy, and financial service companies experiencing higher cyber crime costs than organizations in retail, hospitality, and consumer products.
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
## Putting Malicious Cyber Activity in Context

<table>
<thead>
<tr>
<th>CRIMINAL ACTION</th>
<th>ESTIMATED COST</th>
<th>PERCENT OF GDP</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GLOBAL</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Piracy</td>
<td>$1 billion to $16 billion</td>
<td>0.008% to 0.02%</td>
<td>IMB</td>
</tr>
<tr>
<td>Drug Trafficking</td>
<td>$600 billion</td>
<td>5%</td>
<td>UNODC</td>
</tr>
<tr>
<td>Global cyber activity</td>
<td>$300 billion to $1 trillion</td>
<td>0.4% to 1.4%</td>
<td>Various</td>
</tr>
<tr>
<td><strong>US ONLY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Car Crashes</td>
<td>$99 billion to $168 billion</td>
<td>0.7% to 1.2%</td>
<td>CDC, AAA</td>
</tr>
<tr>
<td>Pilferage</td>
<td>$70 billion to $280 billion</td>
<td>0.5% to 2%</td>
<td>NRF</td>
</tr>
<tr>
<td>US- cyber activity</td>
<td>$24 billion to $120 billion</td>
<td>0.2% to 0.8%</td>
<td>Various</td>
</tr>
</tbody>
</table>

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?

Source: Mandiant M-Trends 2013
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.
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.
It’s About Risk Management

Source: Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), February 12, 2014
Networks and Behavior
Our enterprises and organizations are critically dependent on infrastructure network systems including the Internet. Hence, it makes sense to utilize scientific tools drawn from network science in order to investigate enterprise vulnerabilities and synergies. Such tools must also capture the behavior of decision-makers.
The components of networks as a theoretical (modeling, analysis, and solution) construct include: nodes, links, and flows. We use such a representation to conceptualize, formulate, and study network systems in the real-world.
<table>
<thead>
<tr>
<th>Network System</th>
<th>Nodes</th>
<th>Links</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transportation</td>
<td>Intersections, Homes, Workplaces, Airports, Railyards</td>
<td>Roads, Airline Routes, Railroad Track</td>
<td>Automobiles, Trains, and Planes,</td>
</tr>
<tr>
<td>Manufacturing and logistics</td>
<td>Workstations, Distribution Points</td>
<td>Processing, Shipment</td>
<td>Components, Finished Goods</td>
</tr>
<tr>
<td>Communication</td>
<td>Computers, Satellites, Telephone Exchanges</td>
<td>Fiber Optic Cables, Radio Links</td>
<td>Voice, Data, Video</td>
</tr>
<tr>
<td>Energy</td>
<td>Pumping Stations, Plants</td>
<td>Pipelines, Transmission Lines</td>
<td>Water, Gas, Oil, Electricity</td>
</tr>
</tbody>
</table>
Behavior on Congested Networks

*Decision-makers select their cost-minimizing routes.*

- Decentralized vs. Centralized
  - Selfish vs. Unselfish
    - User-Optimized vs. System-Optimized

*Flows are routed so as to minimize total cost to society.*
Two fundamental principles of travel behavior, due to Wardrop (1952), with terms coined by Dafermos and Sparrow (1969).

**User-optimized (U-O) (network equilibrium) Problem** – each user determines his/her cost minimizing route of travel between an origin/destination, until an equilibrium is reached, in which no user can decrease his/her cost of travel by unilateral action (in the sense of Nash).

**System-optimized (S-O) Problem** – users are allocated among the routes so as to minimize the total cost in the system, where the total cost is equal to the sum over all the links of the link’s user cost times its flow.

*The U-O problems, under certain simplifying assumptions, possesses optimization reformulations. But now we can handle cost asymmetries, multiple modes of transport, and different classes of travelers, without such assumptions.*
We Can State These Conditions Mathematically!
The U-O and S-O Conditions

Definition: U-O or Network Equilibrium – Fixed Demands
A path flow pattern \( x^* \), with nonnegative path flows and O/D pair demand satisfaction, is said to be U-O or in equilibrium, if the following condition holds for each O/D pair \( w \in W \) and each path \( p \in P_w \):

\[
C_p(x^*) \begin{cases} 
= \lambda_w, & \text{if } x_p^* > 0, \\
\geq \lambda_w, & \text{if } x_p^* = 0.
\end{cases}
\]

Definition: S-O Conditions
A path flow pattern \( x \) with nonnegative path flows and O/D pair demand satisfaction, is said to be S-O, if for each O/D pair \( w \in W \) and each path \( p \in P_w \):

\[
\hat{C}'_p(x) \begin{cases} 
= \mu_w, & \text{if } x_p > 0, \\
\geq \mu_w, & \text{if } x_p = 0,
\end{cases}
\]

where \( \hat{C}'_p(x) = \sum_{a \in L} \frac{\partial \hat{c}_a(f_a)}{\partial f_a} \delta_{ap} \), and \( \mu_w \) is a Lagrange multiplier.
The importance of behavior will now be illustrated through a famous example known as the Braess paradox which demonstrates what can happen under \textit{U-O} as opposed to \textit{S-O} behavior.

\textit{Although the paradox was presented in the context of transportation networks, it is relevant to other network systems in which decision-makers act in a noncooperative \textit{(competitive)} manner.}
The Braess (1968) Paradox

Assume a network with a single O/D pair (1,4). There are 2 paths available to travelers:
\[ p_1 = (a, c) \text{ and } p_2 = (b, d). \]

For a travel demand of 6, the equilibrium path flows are
\[ x_{p_1}^* = x_{p_2}^* = 3 \]

The equilibrium path travel cost is
\[ C_{p_1} = C_{p_2} = 83. \]

\[ c_a(f_a) = 10f_a, \quad c_b(f_b) = f_b + 50, \]
\[ c_c(f_c) = f_c + 50, \quad c_d(f_d) = 10f_d. \]
Adding a new link creates a new path $p_3 = (a, e, d)$.

The original flow distribution pattern is no longer an equilibrium pattern, since at this level of flow the cost on path $p_3$, $C_{p_3} = 70$.

The new equilibrium flow pattern network is

$x^*_p = x^*_p = x^*_p = 2$.

The equilibrium path travel cost: $C_{p_1} = C_{p_2} = C_{p_3} = 92$. 

\[ c_e(f_e) = f_e + 10 \]
The 1968 Braess article has been translated from German to English and appears as:

**On a Paradox of Traffic Planning,**

Under S-O behavior, the total cost in the network is minimized, and the new route $p_3$, under the same demand, would not be used.

*The Braess paradox never occurs in S-O networks.*
Recall the Braess network with the added link $e$.

What happens as the demand increases?
For Networks with Time-Dependent Demands
We Use Evolutionary Variational Inequalities

The U-O Solution of the Braess Network with Added Link (Path) and Time-Varying Demands Solved as an *Evolutionary Variational Inequality*.

![Equilibrium Path Flow vs Demand](image-url)

- Black: Paths 1 and 2
- Red: Path 3
In Demand Regime I, **Only the New Path is Used.**
In Demand Regime II, the travel demand lies in the range $[2.58, 8.89]$, and *the Addition of a New Link (Path) Makes Everyone Worse Off!*
In Demand Regime III, when the travel demand exceeds 8.89, **Only the Original Paths are Used!**
The new path is never used, under U-O behavior, when the demand exceeds 8.89, even out to infinity!
Other Networks that Behave like Traffic Networks

The Internet and electric power networks and even supply chains!
Which Nodes and Links Really Matter?
Network Performance and Vulnerability

Disasters have a catastrophic effect on human lives and a region’s or even a nation’s resources and economies.
The analysis and the identification of the vulnerable components in networks have, recently, emerged as a major research theme.

However, in order to be able to evaluate the vulnerability and the reliability of a network, a measure that can quantifiably capture the performance of a network must be developed.
Definition: A Unified Network Performance Measure

The network performance/efficiency measure, \( \mathcal{E}(G, d) \), for a given network topology \( G \) and the equilibrium (or fixed) demand vector \( d \), is:

\[
\mathcal{E} = \mathcal{E}(G, d) = \frac{\sum_{w \in W} d_w \lambda_w}{n_W},
\]

where recall that \( n_W \) is the number of O/D pairs in the network, and \( d_w \) and \( \lambda_w \) denote, for simplicity, the equilibrium (or fixed) demand and the equilibrium disutility for O/D pair \( w \), respectively.

Definition: Importance of a Network Component

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

$$I(g) = \frac{\Delta \mathcal{E}}{\mathcal{E}} = \frac{\mathcal{E}(G, d) - \mathcal{E}(G - g, d)}{\mathcal{E}(G, d)}$$

where $G - g$ is the resulting network after component $g$ is removed from network $G$. 
Approach to Identifying the Importance of Network Components

The elimination of a link is treated in the N-Q network efficiency measure by removing that link while the removal of a node is managed by removing the links entering and exiting that node.

In the case that the removal results in no path connecting an O/D pair, we simply assign the demand for that O/D pair to an abstract path with a cost of infinity.

The N-Q measure is well-defined even in the case of disconnected networks.
The Ranking of Links in the Braess Network

Table 1: Link Results for the Braess Network

<table>
<thead>
<tr>
<th>Link</th>
<th>N-Q Measure</th>
<th></th>
<th>L-M Measure</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Importance Value</td>
<td>Importance Ranking</td>
<td>Importance Value</td>
<td>Importance Ranking</td>
</tr>
<tr>
<td>a</td>
<td>.2069</td>
<td>1</td>
<td>.1056</td>
<td>3</td>
</tr>
<tr>
<td>b</td>
<td>.1794</td>
<td>2</td>
<td>.2153</td>
<td>2</td>
</tr>
<tr>
<td>c</td>
<td>.1794</td>
<td>2</td>
<td>.2153</td>
<td>2</td>
</tr>
<tr>
<td>d</td>
<td>.2069</td>
<td>1</td>
<td>.1056</td>
<td>3</td>
</tr>
<tr>
<td>e</td>
<td>-.1084</td>
<td>3</td>
<td>.3616</td>
<td>1</td>
</tr>
</tbody>
</table>

N-Q (Nagurney-Qiang); L-M (Latora-Marchiori)
## The Ranking of Nodes in the Braess Network

Table 2: Nodal Results for the Braess Network

<table>
<thead>
<tr>
<th>Node</th>
<th>N-Q Measure</th>
<th>L-M Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Importance Value</td>
<td>Importance Ranking</td>
</tr>
<tr>
<td>1</td>
<td>1.0000</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>.2069</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>.2069</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>1.0000</td>
<td>1</td>
</tr>
</tbody>
</table>
Advantages of the N-Q Network Efficiency Measure

- The measure captures *demands, flows, costs, and behavior of users*, in addition to *network topology*.

- The resulting importance definition of network components is applicable and *well-defined even in the case of disconnected networks*.

- It can be used to identify the *importance (and ranking) of either nodes, or links, or both*.

- It can be applied to *assess the efficiency/performance of a wide range of network systems, including financial systems and supply chains under risk and uncertainty*.

- It is applicable also to *elastic demand networks*.
Supply Chains and Risk
Examples of Supply Chains
Supply Chain Risk

*Risk in the context of supply chains may be associated with*

- the production/procurement processes,
- the transportation/shipment of the goods,
- and/or the demand markets.

*Such supply chain risks are directly reflected in firms’ financial performances, and priced in the financial market.*

Hendricks and Singhal (2010) estimated that the average stock price reaction to supply-demand mismatch announcements was approximately $-6.8\%$. In addition, supply chain disruptions can cause firms’ equity risks to increase by $13.50\%$ on average after the disruption announcements (Hendricks and Singhal (2005)).
Illustrations of Supply Chain Risk

Which Suppliers Matter the Most?

Supply Chain Performance Assessment and Supplier and Component Importance Identification in a General Competitive Multitiered Supply Chain Network Model, D. Li and A. Nagurney, UMass Amherst, 2014.
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.
We lay the foundation for the development of network economics based models for cyber crime in financial services.

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.
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.
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.
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.
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.
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.

According to a recent Rand report, for many, the cyber black market can be more profitable than the illegal drug trade.
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 1 · · · i · · · n

Demand Markets 1 · · · j · · · n

Figure 1: 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 $\pi_i$ denote the supply price of the commodity associated with $i$. Let $d_j$ denote the demand associated with demand market $j$ and let $\rho_j$ denote the demand price associated with demand market $j$. 
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 $(i, j)$: $i = 1, \ldots, m; j = 1, \ldots, n$:

$$\pi_i + c_{ij} \begin{cases} = \rho_j, & \text{if } Q^*_{ij} > 0 \\ \geq \rho_j, & \text{if } Q^*_{ij} = 0. \end{cases}$$  (1)
The feasibility conditions must hold for every $i$ and $j$:

\[ s_i = \sum_{j=1}^{n} Q_{ij} \quad (2) \]

and

\[ d_j = \sum_{i=1}^{m} Q_{ij}. \quad (3) \]

(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 $K = \{(s, Q, d) | (2) \text{ and } (3) \text{ hold}\}$. 

Anna Nagurney
Network Science and Economics
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:

$$\pi = \pi(s)$$  \hspace{1cm} (4)

where $\pi$ 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:

$$\rho = \rho(d)$$  \hspace{1cm} (5)

where $\rho$ 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:

$$c = c(Q)$$  \hspace{1cm} (6)
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:

\[
\pi(s^*) \cdot (s - s^*) + c(Q^*) \cdot (Q - Q^*) - \rho(d^*) \cdot (d - d^*) \geq 0, \quad \forall (s, Q, d) \in K.
\]  

(7)
Numerical Example

Figure 2: 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:

\[ \pi_1 = 19, \quad \pi_2 = 10, \]
\[ c_{11} = 3.25, \quad c_{12} = 6.5, \quad c_{21} = 18, \quad c_{22} = 15.5, \]
\[ \rho_1 = 22.25, \quad \rho_2 = 25.5. \]
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.
Some Challenging Research Issues
We have investigated issues of information asymmetry in the context of network systems. In the cyber domain this is a major issue in terms of both vertical information asymmetry and horizontal asymmetry.

For example, hackers know which systems and organizations they have entered and obtain information from. However, firms may be unaware for days or weeks.

Similarly, other firms in the same industry may be unaware of their competitors being hacked.
How confident are you in the antivirus and other software that you have purchased?


Another important research question in the cyber domain is that of information sharing. Our work in mergers & acquisitions from a supply chain network perspective and eye towards risk minimization may help in this area.
Mergers and Acquisitions and Network Synergies

We build upon our recent work in mergers and acquisitions that focuses on horizontal supply chain network integration.

We developed the following significant extension: *we utilize a mean-variance (MV) approach in order to capture the risk associated with supply chain activities both prior to and post the merger/acquisition under investigation.*

The MV approach to the measurement of risk dates to the work of the Nobel laureate Markowitz (1952, 1959) and even today (cf. Schneeweis, Crowder, and Kazemi (2010)) remains a fundamental approach to minimizing volatility.
The Pre- and Post-Merger Supply Chain Networks

All firms, both prior and post the merger, minimize both their expected total costs and the risk, as captured through the variance of the total costs, with a suitable weight assigned to the latter.
Figure 3: The Pre-Merger Supply Chain Network
Figure 4: The Post-Merger Supply Chain Network
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
New architectures are focusing on networking technology, and not on economic interactions. Also, they lack in mechanisms to introduce competition and market forces.
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.
USA NSF Future Internet Architecture (FIA) Projects

- Named Data Networking (NDN) – UCLA (lead) – Content-centric, focus on “what” not “where”
- MobilityFirst – Rutgers University (lead) – Cellular convergence (4-5B devices) interconnected vehicles
- NEBULA – University of Pennsylvania (lead) – Reliable, high-speed core interconnecting data centers
- eXpressive Internet Architecture (XIA) – Carnegie Mellon University (lead) – Rich set of communication entities as network principals
- ChoiceNet – University of Massachusetts Amherst (lead) – project started September 2011; assigned FIA status in 2012.
New architectures are focusing on networking technology, and not on economic interactions. Also, they lack in mechanisms to introduce competition and market forces.

In addition, 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.
ChoiceNet Goals

- **Expose choices throughout the network**
  - Network is no longer a “black box"

- **Interactions between technological alternatives and relationships** — Introduction of a dynamic “economy plane"
  - Money as a driver to overcome inertia by providers
  - Market forces can play out within the network itself

- **Services are at the core of ChoiceNet** — “everything is a service"
  - Services provide a benefit but entail a cost
  - Services are created, composed, sold, verified, etc.
The focus of ChoiceNet is on *choices* and *network economics*. Choice criteria can also include privacy, minimization of risk, even environmental impact minimization.

Transparency associated with ChoiceNet and having more refined routing options can also aid in cybersecurity.
ChoiceNet Principles

*Competition Drives Innovation!*

Services are at the core of ChoiceNet (*“everything is a service”*). Services provide a benefit, have a cost. Services are created, composed, sold, verified, etc.

- "Encourage alternatives" by providing building blocks for different types of services.
- "Know what happened" to have the ability to evaluate services.
- "Vote with your wallet" to reward good 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.
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

Anna Nagurney

Network Science and Economics
ChoiceNet enables the composition of services and economic relationships

- Economy plane: customer-provider relationships
- Use plane: client-service relationships
- Positive feature is the ability to reflect real-world relationships.
• **Incentives for participation?**
  – Everyone can be rewarded (host, verifier, author, integrator)
  – Innovative and good services get rewarded

• **Payments among actors to sustain viability**
  – Economy plane distributes value (i.e., money)

• **Same commercial entities as today?**
  – Similar providers, but also finer-grained providers
  – New providers for composition and verification.
ChoiceNet Technologies (in progress)

- Economy plane
  - Methods for describing composing, and instantiating services
  - Market places for connecting customers and providers (i.e., search for services)
  - IDs associated with entities

- Use plane
  - Verification of the economy plane contracts in use plane
  - Measurement services to verify offerings.
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* or *The Boston Globe* in a coffee shop (short-term and long-term contracts)
  - Customers as providers.
Our Network Models Utilize Game Theory - Flow of Content

Content Providers

Network Providers

Users at Demand Markets

Figure 5: The Network Structure of the Multi-Provider Model's Content Flows
Our Network Models Utilize Game Theory - Flow of Payments

Content Providers

Network Providers

Users at Demand Markets

Anna Nagurney  
Network Science and Economics
Some of Our Publications on the NSF Project


Some of Our Publications on the NSF Project


Some of Our Publications on the NSF Project


Summary and Conclusions

- In this presentation, we have overviewed our work on network vulnerability from a cybersecurity perspective from both a system and a cyber crime perspective. Our “clients” were financial service firms, who have also encountered a growing number of cyber attacks.

- We discussed some results from supply chain risk management that may be useful in cyber security.

- 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.
Summary and Conclusions

• In this presentation, we have overviewed our work on network vulnerability from a cybersecurity perspective from both a system and a cyber crime perspective. Our “clients” were financial service firms, who have also encountered a growing number of cyber attacks.

• We discussed some results from supply chain risk management that may be useful in cyber security.
Summary and Conclusions

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

- We discussed some results from supply chain risk management that may be useful in cyber security.

- 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 network vulnerability from a cybersecurity perspective from both a system and a cyber crime perspective. Our “clients” were financial service firms, who have also encountered a growing number of cyber attacks.

- We discussed some results from supply chain risk management that may be useful in cyber security.

- 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.

Anna Nagurney
Network Science and Economics