Game Theoretic Model for Cybersecurity in Supply Chains with Nonlinear Budget Constraints

Anna Nagurney1, Ladimer S. Nagurney2, Patrizia Daniele3, Shivani Shukla2
1Department of Operations and Information Management, University of Massachusetts, Amherst
2Department of Electrical and Computer Engineering, University of Hartford
3Department of Mathematics and Computer Science, University of Catania, Italy

Introduction

- Estimated annual cost to the global economy from cybercrime is more than $400 billion, conservatively $375 billion in losses, more than the national income of most countries (Center for Strategic and International Studies (2014)).
- According to Mandiant (2014), in 2013, the median number of days cyberattackers were present on a victim network before they were discovered was 229 days.
- Top Security Breaches of 2014: Home Depot attacked four times (employee information and credit/debit cards worth $56 million lost); JP Morgan (financial information worth 1 million stolen); Target (stolen credit cards sold for $120 each on the black market; after weeks the price dropped to $8)
- Each year $15 billion is spent by organizations in the United States to provide cybersecurity (Gartner and Market Research (2013)). Worldwide spending in 2014 - $71.1 billion; Expected in 2015 - $76.9 billion (Gartner (2014)).

The Supply Chain Game Theory Model of Cybersecurity Investments Under Network Vulnerability

Security Level of Firm i, s_i:

0 ≤ s_i ≤ 1; i = 1, ..., n.

Average Network Security of the Chain, s:

s = 1/n \sum_{i=1}^{n} s_i.

Probability of a Successful Cyberattack on i, p_i:

p_i = (1 - s_i)(1 - s) i = 1, ..., n.

Probability = vulnerability level of the retailer × vulnerability level of the network.

Investment Cost Function to Acquire Security, h_i(s_i):

h_i(s_i) = \alpha_i/(1 - s_i) - 1; \alpha_i > 0.

\alpha_i quantifies size and needs of retailer i.

Demand Price Function for Consumer j, p_j:

p_j = p_i(d; \bar{s}) = p_i(Q, s) j = 1, ..., n.

Price is a function of demand (d) and average security.

Profit of Retailer in absence of cyberattack and investments, f_i:

f_i(Q, s) = \sum_{j=1}^{n} p_j(Q, s)Q_j - \sum_{j=1}^{n} c_j(Q_j).

Q_j Quantity from i to j; c_j Cost of processing at j; Cost of transactions from i to j; Financial damage at i; D_i.

Expected Utility/Profit for Retailer i, i = 1, ..., n:

E(U_i) = (1 - p_i)f_i(Q, s) + p_i(f_i(Q, s) - D_i) - h_i(s_i).

Theorem 1 (Variational Inequality Formulation) Assume that, for each retailer i, the expected profit function is concave with respect to the variables (Q_j), \ldots, (Q_m), and s_i, and is continuous and continuously differentiable. Then (Q^*, s^*) in K, the feasible set, is a supply chain Nash equilibrium if and only if it satisfies the variational inequality:

\sum_{j=1}^{n} \frac{\partial E(U_i(Q^*, s^*))}{\partial Q_j} s_j(Q^*_j - Q^*_j) + \sum_{j=1}^{m} \frac{\partial E(U_i(Q^*, s^*))}{\partial s_j} s_j(s_j - s^*_j) ≥ 0.

The SCGT Model of Cybersecurity Investments with Nonlinear Budget Constraints

The network is envisioned as bipartite, similar to the one discussed in the previous study. While the overall notions, functional forms, and structure of the model remain the same, there are a few changes.

Security Level of Firm i, s_i:

0 ≤ s_i ≤ 1

where u_i < 1 indicating that perfect security level of 1 is unattainable.

Numerical Results for the SCGT Model with Nonlinear Constraints

The Euler method was implemented in FORTRAN and run on a Linux system. The convergence criterion was set to 10^{-4}. The following equilibrium results are for two retailers and two demand markets instance.

Cybercrime Impact over Socio-Economic-Political Riders

Results of both studies are consistent with those obtained in practice. The studies fulfill critical need for economic and game theoretic models in cyberspace. The models and results make way for exploring potential law and policy interventions.

- Less social stigma attached to these crimes and economic effect is obvious - Cybercrime has interdependencies with phenomena - economic systems, and political machinery.
- Influenced by rate of urbanization, population, unemployment, income inequality and competition.
- Emotional impact of e-commerce - Consumers feel angry, annoyed and cheated. More than 80% think that the perpetrators will not be brought to justice.
- Salami attack - Structured cybercrime in smaller proportions brought together to perform a larger attack.
- Cyberbullying - Hacking into systems to identify victims and publishing severely defaming material, loss of intellectual property, sensitive data, image and reputation.

Papers:
Nagurney, A., Daniele, P., Shukla, S.: A Supply Chain Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints. Accepted.

Results of both studies are consistent with those obtained in practice. The studies fulfill critical need for economic and game theoretic models in cyberspace. The models and results make way for exploring potential law and policy interventions.

- Less social stigma attached to these crimes and economic effect is obvious - Cybercrime has interdependencies with phenomena - economic systems, and political machinery.
- Influenced by rate of urbanization, population, unemployment, income inequality and competition.
- Emotional impact of e-commerce - Consumers feel angry, annoyed and cheated. More than 80% think that the perpetrators will not be brought to justice.
- Salami attack - Structured cybercrime in smaller proportions brought together to perform a larger attack.
- Cyberbullying - Hacking into systems to identify victims and publishing severely defaming material, loss of intellectual property, sensitive data, image and reputation.

Papers:
Nagurney, A., Daniele, P., Shukla, S.: A Supply Chain Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints. Accepted.