Game Theoretic Models for Cybersecurity in Supply Chains and Financial Services Networks

Anna Nagurney[a], Ladimer S. Nagurney[b], Shivani Shukla[a]

[a]Department of Operations and Information Management, University of Massachusetts, Amherst
[b]Department of Electrical and Computer Engineering, University of Hartford

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); JPMC (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:

$$0 \leq s_i \leq 1; \quad i = 1, ..., m.$$

Average Network Security of the Chain, $\bar{s}$:

$$\bar{s} = \frac{1}{m} \sum_{i=1}^{m} s_i.$$

Probability of a Successful Cyberattack on i, p_i:

$$p_i = (1 - s_i)(1 - \bar{s}), \quad i = 1, ..., m.$$

Probability = vulnerability level of the retailer $\times$ vulnerability level of the network. **Investment Cost Function to Acquire Security s_i, $h_i(s_i)$:**

$$h_i(s_i) = \alpha_i(\frac{1}{\sqrt{(1 - s_i)}} - 1), \quad \alpha_i > 0.$$

α_i quantifies size and needs of retailer i. **Demand Price Function for Consumer j, ρ_j:**

$$\rho_j = \rho_j(d, \bar{s}) \equiv \hat{\rho}_j(Q, s), \quad j = 1, ..., n.$$

Price is a function of demand (d) and average security. **Profit of Retailer in absence of cyberattack and investments, f_i:**

$$f_i(Q, s) = \sum_{j=1}^{n} \hat{\rho}_j(Q, s) Q_{ij} - c_i \sum_{j=1}^{n} Q_{ij} - \sum_{j=1}^{n} c_{ij}(Q_{ij}),$$

Q_{ij} : Quantity from i to j; c_i : Cost of processing at i; c_{ij} : Cost of transactions from i to j. Financial damage at i: D_i.

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

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

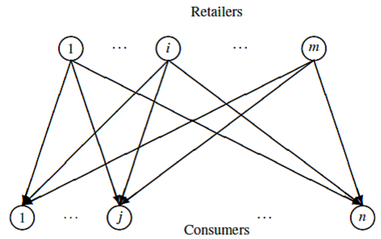
Theorem 1 (Variational Inequality Formulation) *Assume that, for each retailer i, the expected profit function is concave with respect to the variables $\{Q_{i1}, ..., Q_{in}\}$, and s_i, and is continuous and continuously differentiable. Then $(Q^*, s^*) \in K$, the feasible set, is a supply chain Nash equilibrium if and only if it satisfies the variational inequality $\forall (Q, s) \in K$*

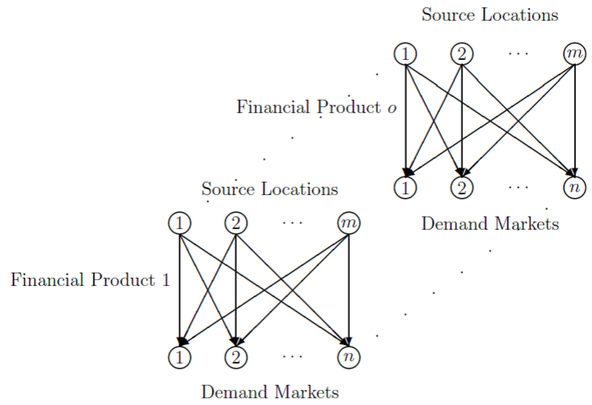
$$-\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} \times (Q_{ij} - Q_{ij}^*) - \sum_{i=1}^{m} \frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} \times (s_i - s_i^*) \geq 0.$$

The Multiproduct Network Economic Model of Cybercrime in Financial Services

The model enables us to capture multiple financial products and asymmetric properties of the underlying economic functions. Specifically, the model can be envisioned as o layered bipartite networks, with each network representing a single financial product. Conservation of flow constraints ensure that the supply of a financial product is equal to the sum of flows to all demand markets, demand is equal to the sum of flows from all sources, and the product flows are nonnegative.

Topologies of the Supply Chain and the Financial Services Networks





Numerical Results for the SCGT Model

For computational purposes, we utilized the Euler method, which is induced by the general iterative scheme of Dupuis and Nagurney (1993). The convergence criterion was $\epsilon = 10^{-4}$. It was implemented using FORTRAN. Following are the results for a three retailer and two consumer instance.

Solution	Ex. 1	Var. 1.1	Var. 1.2	Var. 1.3	Var. 1.4
Q_{11}^*	20.80	20.98	20.98	11.64	12.67
Q_{12}^*	89.45	89.45	89.82	49.62	51.84
Q_{21}^*	17.81	17.98	17.98	9.64	10.67
Q_{22}^*	84.49	84.49	84.83	46.31	48.51
Q_{31}^*	13.87	13.98	13.98	8.73	9.50
Q_{32}^*	35.41	35.41	35.53	24.50	25.59
d_1^*	52.48	52.94	52.95	30.00	32.85
d_2^*	209.35	209.35	210.18	120.43	125.94
s_1^*	.90	.92	.95	.93	.98
s_2^*	.91	.92	.95	.93	.98
s_3^*	.81	.83	.86	.84	.95
$\bar{s}^*$	.87	.89	.917	.90	.97
$\rho_1(d_1^*, \bar{s}^*)$	47.61	47.95	47.96	40.91	44.01
$\rho_2(d_2^*, \bar{s}^*)$	95.50	95.50	95.83	80.47	83.77
$E(U_1)$	6654.73	6665.88	6712.29	3418.66	3761.75
$E(U_2)$	5830.06	5839.65	5882.27	2913.31	3226.90
$E(U_3)$	2264.39	2271.25	2285.93	1428.65	1582.62

Variant 1.1: Consumer 1 is more sensitive to network security. Variant 1.2: Consumer 2 is more sensitive to average security. Variant 1.3: Demand price functions are increased. Variant 1.4: Both Consumers are substantially more sensitive to average security.

Time Expression Capturing Delay associated with Cybercrime Activity:

$$t_{ij}^k Q_{ij}^k + h_{ij}^k = T_{ij}^k,$$

for all i source locations, j demand markets, and k products. The value of product depends on quantity on black market and time. Q_{ij}^k : Quantity of k from i to j. $t_{ij}^k \geq 0$ and h_{ij}^k is positive. T_{ij}^k : Time between getting product k from source i and its sale at j.

Demand Price Function for Demand Market j and Product k, $\hat{\rho}_j^k$:

$$\hat{\rho}_j^k(Q) \equiv \rho_j^k(d, T_{ave}).$$

Demand price function depends on the demand (d) and the average time of delivery of products to demand markets (T_{ave}). $T_{ave,j}^k = \sum_{i=1}^{m} \frac{T_{ij}^k Q_{ij}^k}{d_j^k}$.

Supply Price Function for Product k from Source i, $\hat{\pi}_i^k$:

$$\hat{\pi}_i^k(Q) \equiv \pi_i^k(s).$$

The price of acquiring product k at source location i is a function of all supply. The **unit transaction cost** of k between i and j: $\hat{c}_{ij}^k(Q)$.

The Network Economic Equilibrium Conditions:

$$\hat{\pi}_i^k(Q^*) + c_{ij}^k(Q^*) \begin{cases} = \hat{\rho}_j^k(Q^*), & \text{if } Q_{ij}^{k*} > 0 \\ \geq \hat{\rho}_j^k(Q^*), & \text{if } Q_{ij}^{k*} = 0. \end{cases}$$

Theorem 2 (Variational Inequality Formulation) *A product flow pattern $Q^* \in K$, the feasible set, is a cybercrime network economic equilibrium if and only if it satisfies the variational inequality problem:*

$$\sum_{k=1}^{o}\sum_{i=1}^{m}\sum_{j=1}^{n} [\hat{\pi}_i^k(Q^*) + c_{ij}^k(Q^*) - \hat{\rho}_j^k(Q^*)] \times (Q_{ij}^k - Q_{ij}^{k*}) \geq 0, \quad \forall Q \in K.$$

Numerical Results for the Network Economic Model

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

Financial Flows	Ex. 2	Var 2.1	Var 2.2
$\pi_1^1(s^*)$	195.13	194.35	191.11
$\pi_2^1(s^*)$	154.93	149.88	144.32
$\pi_1^2(s^*)$	62.50	83.86	81.33
$\pi_2^2(s^*)$	70.31	83.33	79.29
$c_{11}^1(Q^*)$	98.94	100.72	109.24
$c_{12}^1(Q^*)$	1.00	1.00	10.00
$c_{21}^1(Q^*)$	139.14	145.19	156.03
$c_{22}^1(Q^*)$	20.58	15.06	22.96
$c_{11}^2(Q^*)$	14.06	6.04	13.59
$c_{12}^2(Q^*)$	7.46	29.97	39.16
$c_{21}^2(Q^*)$	6.17	6.47	15.52
$c_{22}^2(Q^*)$	2.00	30.56	41.26
$\rho_1^1(d^*, T_{ave}^*)$	294.07	295.07	300.35
$\rho_1^2(d^*, T_{ave}^*)$	76.52	89.85	94.87
$\rho_2^1(d^*, T_{ave}^*)$	175.51	164.94	167.28
$\rho_2^2(d^*, T_{ave}^*)$	69.98	113.86	120.52
$T_{ave,1}^1$	22.74	23.32	22.59
$T_{ave,1}^2$	30.78	33.09	33.62
$T_{ave,2}^1$	23.35	22.50	22.32
$T_{ave,2}^2$	10.61	13.75	13.08

Variant 2.1: Value of financial product 2 has increased at demand market 2. Variant 2.2: Increase in the fixed cost terms of all cost functions - cybercriminals have a harder time fencing all the products.

Summary

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

Papers:

Nagurney, A.: A Multiproduct Network Economic Model of Cybercrime in Financial Services. Service Science, Vol 7, 70-81 (2015)

Nagurney, A., Nagurney L.S., Shukla, S.: A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability. Computation, Cryptography, and Network Security. Daras, Nicholas J., Rassias, Michael Th. (Eds.), Springer (2015)

References:

Center for Strategic and International Studies: Net losses: Estimating the global cost of cybercrime. Santa Clara, California (2014)

Dupuis, P., Nagurney, A.: Dynamical systems and variational inequalities. Annals of Operations Research, 44, 9-42 (1993)

Gartner: Gartner reveals Top 10 Security Myths, by Ellen Messmer, NetworkWorld, June 11 (2013)

Mandiant: M-trends: Beyond the breach. 2014 threat report. Alexandria, Virginia (2014)

Market Research: United States Information Technology Report Q2 2012, April 24 (2013)