Dynamic equilibrium framework in cyber-security game

Jin Hyuk Choi

Department of Mathematical Sciences, UNIST

joint with A. Whinston & Y. Choi at UT-Austin

AQFC, April 25th, 2017

Outline

- Goal & Motivation
- Game model
- Literature
- Characterization of equilibrium
- Results

Motivation

- Number of cyber threats is increasing
  - annual cost caused by cyber crimes increased by 19% in USA (2015)
  - 99% of companies experienced cyber attack in 2015
- Needs for cyber-security related insurance is growing
  - \$2 billion in 2014 $\rightarrow$ \$5 billion by 2018
- But cyber-insurance market is premature
  - insurance rates are fluctuating
  - hard to measure cyber risks
  - strategic cyber attacker

Goal

- Construct a game model:
  - strategic attacker and defender
  - financially motivated players
  - containing some specific features of cyber-security
  - general enough (no CS-technology)
  - tractable
- Analyze the game:
  - existence, uniqueness of equilibrium
  - equilibrium with strategic attacker, non-strategic attacker
  - roll of defender

Game model: roll of the players

- **Defender** (example: Internet service provider)
  - can observe user's action with noise
  - doesn't know whether the user is an attacker or not
  - can update the probability that the user is an attacker
  - can block the user based on the suspicion level
  - chooses the optimal threshold to minimize the expected costs
- **User** (example: IP address)
  - can be an attacker or a normal user
  - normal user: no malicious activity
  - attacker: malicious activity $\rightarrow$ profit
  - too much malicious activity $\rightarrow$ blocked by defender sooner
  - attacker chooses optimal activity level to maximize the expected profit

Game model: parameters & notation

- $\theta \in \{0, 1\}$: identity of user ($\theta = 0$ for normal user, $\theta = 1$ for attacker)
- $q_0 = \mathbb{E}[\theta] \in (0, 1)$: Initial suspicion level
- If attacker's action is given by stream $\alpha_t dt$, the defender can observe Y_t with

$$dY_t = \alpha_t 1_{\{\theta=1\}} dt + dW_t$$

  where W_t is a standard Brownian motion, independent of θ.
- Defender continuously updates suspicion level ($q_\cdot$) based on Y.

$$q_t = \mathbb{E}[\theta | \mathcal{F}_t^Y]$$

- If defender chooses blocking threshold $p \in [0, 1]$, the game is over at

$$\tau = \inf\left\{t \geq 0 : \ q_t \geq p\right\}$$

- Attacker believes that the $q_\cdot$ process obeys following SDE:

$$dq_t = \lambda(q_t)\Big(dY_t - \mu(q_t)dt\Big)$$

Game model: equilibrium

Definition of equilibrium: $(\lambda, \mu, \alpha, \hat{p})$ is called an equilibrium if following holds. $(\lambda, \mu, \alpha : \mathbb{R}^2 \to \mathbb{R}, \hat{p} \in [0,1].)$

(1) (Attacker's optimization) Let $p \in [0,1]$ be given. Assume that attacker **believes** that when his attacking intensity is Δ_t, then the q_t obeys the following SDE:

$$dq_t = \lambda(p, q_t)\Big(\Delta_t dt + dW_t - \mu(p, q_t)dt\Big).$$

Then, α solves attacker's maximization problem:

$$\alpha(p, q_\cdot) = \underset{0 \le \Delta_\cdot \le M}{\arg\max}\ \mathbb{E}\Big[\int_0^\tau e^{-rt}\Delta_t dt\Big]$$
$$\text{where}\quad \tau := \inf\{t \ge 0 :\ q_t \ge p\}$$

r: discounting factor
M: limit of attacker's action

Game model: equilibrium

(2) (Defender's optimization) Let $q_\cdot$ be the solution of following SDE:

$$dq_t = \lambda(p, q_t)\Big(d\Upsilon_t - \mu(p, q_t)dt\Big)$$
$$\text{where} \quad d\Upsilon_t = \alpha(p, q_t)1_{\{\theta=1\}}dt + dW_t$$

Then q_t agrees with suspicion level, i.e., $q_t = \mathbb{E}[\theta|\mathcal{F}_t^{\Upsilon}]$ holds.
And $\hat{p}$ solves the defender's cost-minimization problem:

$$\hat{p} = \arg\max_{p\in[0,1]} \mathbb{E}\Big[\int_0^{\tau} \Big(e^{-rt}\alpha(p, q_t)\cdot 1_{\{\theta=1\}}\Big)dt + e^{-r\tau}l\cdot 1_{\{\theta=0\}}\Big]$$
$$\text{where} \quad \tau := \inf\{t \geq 0 : \ q_t \geq p\}$$

where $l > 0$ is an one-time-cost of blocking an innocent user.

Related literature

- Insider trading models
  - game between insider(private info) and market maker
  - Kyle (1985), Back (1992), etc.
  - our model: market maker can stop the game
- Attacker-Defender framework
  - game between attacker and myopic defender
  -
  - our model: defender is not myopic and stops the game
- Sequential hypothesis testing
  - obtain sequence of test results for hypothesis testing
  - optimal stopping problem to minimize expected costs
  - Wald (1945), etc.
  - our model: game between test-result-provider and tester

Remarks on our game model

- **Unique feature**
  - Internet security provider (defender) has authority to block users (ability to stop the game)
  - Defender is not myopic (focused on the defender's roll)
- **General feature**
  - Attacker's and defender's strategies are driven by financial motives
  - No specific hacking-technology: our model can be used for any warfare-type situation

Characterization of equilibrium

(1) Attacker's optimization problem:

$$V(q_0) := \max_{0 \le \Delta_\cdot \le M} \mathbb{E}\Big[\int_0^{\tau} e^{-rt} \Delta_t dt \Big]$$

$$\text{where} \quad \begin{cases} dq_t = \lambda\Big(\Delta_t dt + dW_t - \mu dt\Big) \\ \tau := \inf\{t \ge 0 : \ q_t \ge p\} \end{cases}$$

DPP implies HJB equation:

$$\begin{cases} \max_{\Delta \in [0,M]} \Big(-rV(q) - V'(q)\lambda(q)\mu(q) + \frac{1}{2}V''(q)\lambda^2(q) + \Delta(1 + V'(q)\lambda(q)) \Big) = 0 \\ V(p) = 0 \\ V(0+) = \frac{M}{r} \end{cases}$$

Characterization of equilibrium

(2) Defender's estimation: The solution of the SDE

$$dq_t = \lambda(q_t)\Big(dY_t - \mu(q_t)dt\Big)$$
$$\text{where} \quad dY_t = \alpha(q_t)1_{\{\theta=1\}}dt + dW_t$$

should satisfy $q_t = \mathbb{E}[\theta|\mathcal{F}_t^Y]$. Filtering equation produces

$$\begin{aligned} dq_t &= \Big(\mathbb{E}[\theta\alpha(q_t)1_{\{\theta=1\}}|Y_{[0,t]}] - \mathbb{E}[\theta|Y_{[0,t]}]\mathbb{E}[\alpha(q_t)1_{\{\theta=1\}}|Y_{[0,t]}]\Big) \\ &\qquad \Big(dY_t - \mathbb{E}[\alpha(q_t)1_{\{\theta=1\}}|Y_{[0,t]}]dt\Big) \qquad (1) \\ &= q_t(1-q_t)\alpha(q_t)\Big(dY_t - q_t\alpha(q_t)dt\Big) \end{aligned}$$

By comparing SDEs for q_t, we obtain relations among λ, μ, α:

$$\alpha(q) = \frac{\lambda(q)}{(1-q)q}, \quad \mu(q) = \frac{\lambda(q)}{1-q}$$

Characterization of equilibrium

Combine these relations with the attacker's HJB,

$$\begin{cases} \frac{V''(q)}{2} - \frac{V'(q)}{1-q} - rV(q)V'(q)^2 = 0, & \text{if } V'(q) < -\frac{1}{M(1-q)q} \\ \frac{V''(q)}{2} + \frac{V'(q)}{q} - \frac{rV(q)}{M^2q^2(1-q)^2} + \frac{1}{Mq^2(1-q)^2} = 0, & \text{if } V'(q) \geq -\frac{\sigma^2}{M(1-q)q} \\ V(0+) = \frac{M}{r}, \quad V(p) = 0 \end{cases}$$

$$\mu(q) = \frac{\lambda(q)}{1-q}, \quad \alpha(q) = \frac{\lambda(q)}{(1-q)q}$$

Finally, the defender's optimization problem is

$$\mathbb{E}\Big[\int_0^{\tau} \Big(e^{-rt}\alpha(q_t)\cdot 1_{\{\theta=1\}}\Big)dt + e^{-r\tau}l\cdot 1_{\{\theta=0\}}\Big] \quad \text{with} \quad \tau := \inf\{t\geq 0 : \ q_t \geq p\}$$
$$= q_0V(q_0) + (1-q_0)u(q_0)$$

where $u(q_0) := \mathbb{E}[e^{-r\tau}|\theta = 0]$. Then u should satisfy

$$\frac{1}{2}u''(q) - \frac{u'(q)}{1-q} - \frac{ru(q)}{\lambda(q)^2} = 0, \quad u(p) = 1, \quad u(0) = 0$$

Results

Let φ, a, b, c, x^* be defined as

$$\varphi(x) := \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$$

$$a := \frac{1}{2}\left(\sqrt{1 + \frac{8r}{M^2}} - 1 \right)$$

$$b := \frac{M}{\sqrt{r}} - \frac{\sqrt{r}}{aM}$$

$$c := \frac{2\sqrt{r}e^{-b^2} + M\sqrt{\pi}\varphi(b)}{Mp\sqrt{\pi}}$$

$$x^* := \frac{pc - \varphi(b)}{c - \varphi(b)}$$

Let V be defined as

If $\frac{r}{M^2} \geq 1$:

$$V(x) := \frac{M}{r}\left(1 - \left(\frac{1-p}{p}\right)^a \left(\frac{x}{1-x}\right)^a\right), \quad x \in [0, p]$$

If $\frac{r}{M^2} < 1$:

$$V(x) := \begin{cases} \frac{M}{r} - \frac{\sigma^2}{aM}\left(\frac{(1-p)c}{pc - \varphi(b)}\right)^a \cdot \left(\frac{x}{1-x}\right)^a, & \text{for } 0 \leq x \leq x^* \\ \frac{\sigma}{\sqrt{r}}\, \varphi^{-1}\left(c \cdot \frac{p-x}{1-x}\right), & \text{for } x^* < x \leq p \end{cases}$$

Results

Theorem

We have the unique equilibrium:

$$\lambda(p,x) = \begin{cases} M(1-x)x, & for\ 0 \le x \le x^* \\ -\frac{1}{V'(x)}, & for\ x^* < x \le p \end{cases},$$

$$\mu(p,x) = \frac{\lambda(x)}{1-x}, \quad \alpha(p,x) = \frac{\lambda(x)}{(1-x)x}$$

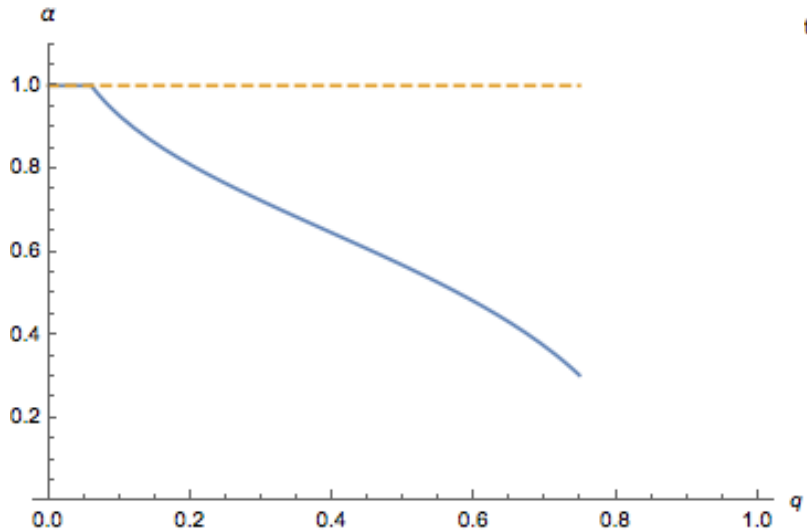
$$If \quad \frac{r}{M^2} \ge 1: \quad \hat{p} = \frac{(1+a)rl}{(1+a)rl+aM}$$

$$If \quad \frac{r}{M^2} < 1: \quad \hat{p} = \frac{l\sqrt{r}\left(2\sqrt{r}e^{-b^2} + M\sqrt{\pi}\varphi(b)\right)}{M + l\sqrt{r}\left(2\sqrt{r}e^{-b^2} + M\sqrt{\pi}\varphi(b)\right)}$$

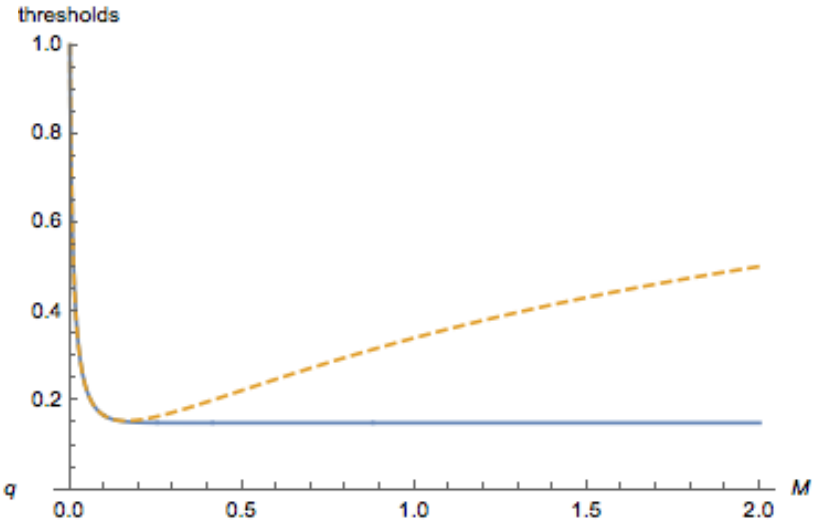
Ingredients of proof

- Need to check the solutions of SDEs are well defined ($q_t = 0$ is an absorbing state)
- Check that q cannot reach 0, using Feller's explosion test
- Verification of optimization problems, filtering equation, stochastic representation $\mathbb{E}[e^{-r\tau}|\theta = 0]$

Equilibrium strategies



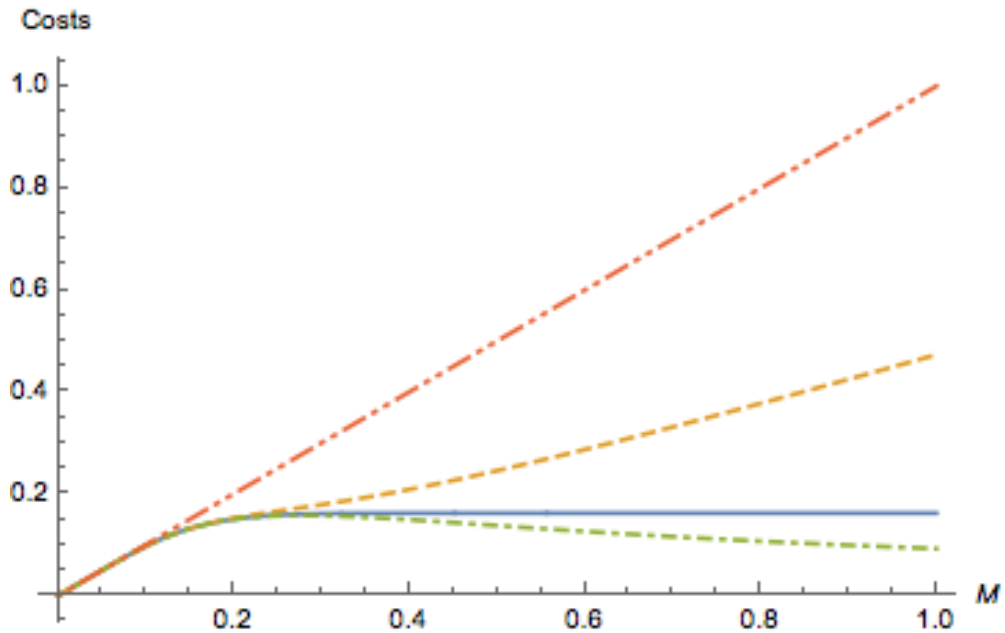
$\alpha(q)$



$\hat{p}(M)$

(—): strategic attacker
(- - -): non-strategic attacker

Equilibrium costs comparison with benchmarks



expected cost of defender (M)

(-·-·-·-): no defender (no blocking at all)

(-·-·-): non-strategic attacker VS defender

(- - -): strategic attacker VS naive defender

(—-): strategic attacker VS defender (our model)

Conclusion

- Dynamic game model for cyber-security
- Unique feature of non-myopic defender who can optimally stop the game
- Strategic nature of attacker is important factor
- Applicable to cyber-insurance market