Rational Theory of Information Security Battle: Economic Analysis of Preemptive Behavior

*Makoto GOTO[a] Ken-ichi TATSUMI[b]

[a]Hokkaido University

[b]Gakushuin University

Plan of Talk

1. Introduction
2. The Model
   - Gordon and Loeb (2002)
   - Tatsumi and Goto (2010)
   - Our Model
3. Numerical Example
4. Conclusion

Introduction

- Importance of information security has emerged very rapidly as information society has developed great deal.
- The information security investment has accordingly been considered by Gordon and Loeb (2002).
  - The highlight of their analysis is an introduction of vulnerability concept to formal optimization problem.
- Although their analysis is static, Tatsumi and Goto (2010) explored a dynamic analysis of information security investment from the defender's perspective.
- In this paper, we add the attacker's perspective to the information security investment problem, so that we formulate the problem as a 2-player zero-sum game.

Gordon and Loeb (2002)

- The potential loss associated with the threat against the information system:

$$L = T\lambda,$$

  - $T > 0$: a random variable of the threat occurring,
  - $\lambda \in [0, 1]$: the monetary loss suffered on conditioned on the breach occurring.
- $v \in [0, 1]$: vulnerability (the success probability of the attack once launched).
- The total expected loss:

$$vL = v\lambda T.$$

- Remaining vulnerability if a firm invests z dollars in security:

$$S(z, v) \in [0, 1].$$

- The expected net benefit from the investment:

$$(v - S(z, v))\lambda T - z.$$

Remaining Vulnerability

Assumption (Remaining vulnerability)

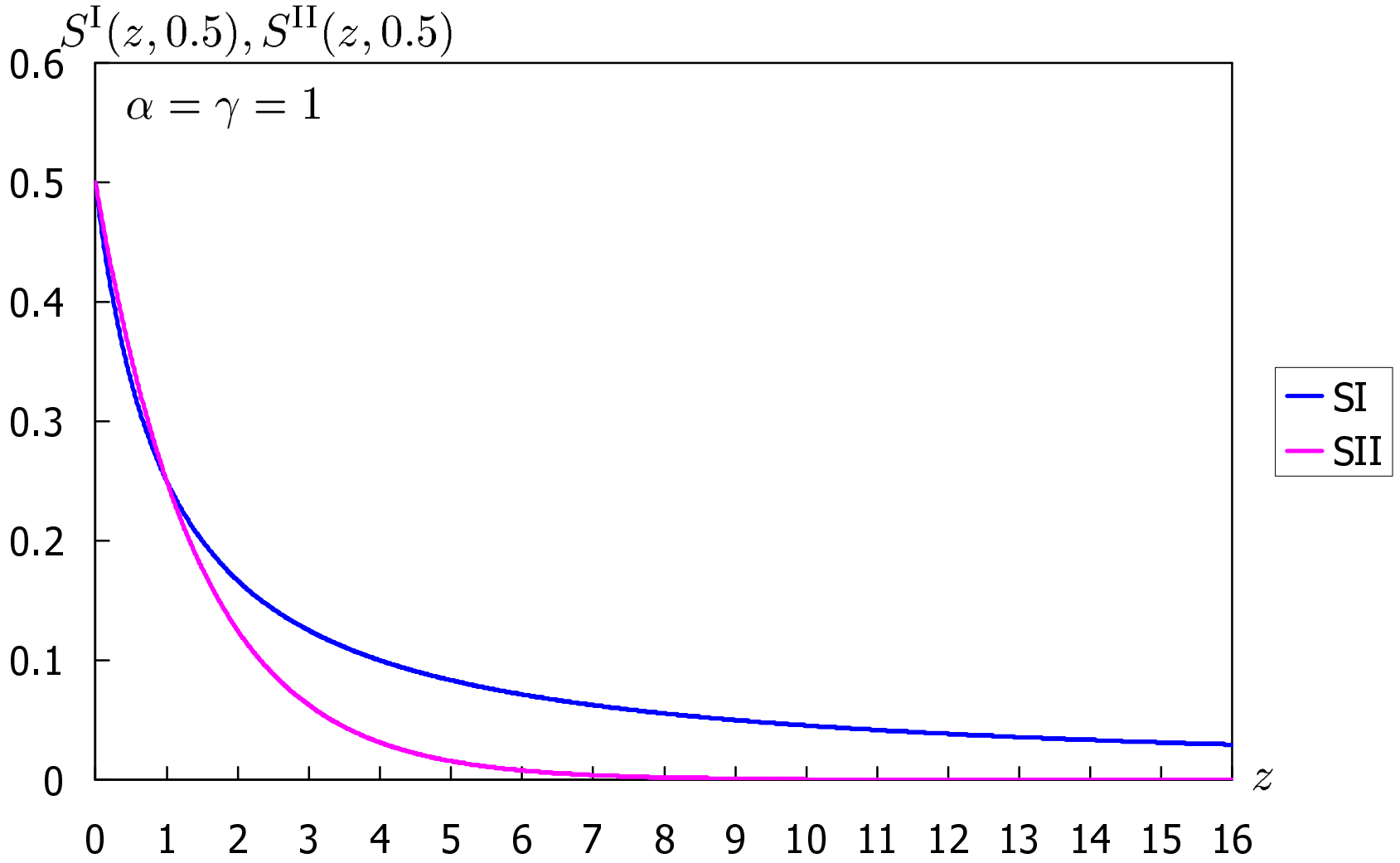
1. *If the attack success probability is 0, it stays so after every possible investment:* $\forall z, S(z,0) = 0$.
2. *If we spend no money for investment, there will be no change in the attack success probability:* $\forall v, S(0,v) = v$.
3. *The function is continuously twice differentiable and*

$$\text{for } 0 < v, \quad \frac{\partial S(z,v)}{\partial z} < 0, \quad \frac{\partial^2 S(z,v)}{\partial z^2} > 0,$$
$$\forall v, \quad \lim_{z \to \infty} S(z,v) = 0.$$

- Examples:

$$S^{\mathrm{I}} = \frac{v}{(\alpha z + 1)^{\gamma}}, \quad \alpha > 0, \ \gamma \in \mathbb{R},$$
$$S^{\mathrm{II}} = v^{\alpha z + 1}, \quad \alpha > 0.$$

The Remaining Vulnerability Functions



The Optimal Level of Investment

- Maximizing the expected net benefit from the investment:

$$\frac{\partial[(v - S(z, v))L - z]}{\partial z} = 0 \Rightarrow -\frac{\partial S(z^*, v)L}{\partial z} = 1.$$

- Case I:

$$z^* = \frac{(v\gamma\alpha\lambda T)^{1/(\gamma+1)} - 1}{\alpha}.$$

- Case II:

$$z^* = \frac{-\ln(-\alpha v\lambda T \ln v)}{\alpha \ln v}.$$

Tatsumi and Goto (2010)

- The threat of attempted breach:

$$\mathrm{d}T_t = \mu T_t \mathrm{d}t + \sigma T_t \mathrm{d}W_t, \quad T_0 = T.$$

- The maximized expected present value of the expected benefit from the security investment:

$$\begin{aligned} V(T) &= \sup_{\tau \in \mathcal{T}} \mathbb{E}\left[\int_\tau^\infty \mathrm{e}^{-rt}\{(v - S(z,v))\lambda T_t - z\}\mathrm{d}t\right], \\ &= \begin{cases} \left(\dfrac{(v - S(z,v))\lambda T^*}{r-\mu} - \dfrac{z}{r}\right)\left(\dfrac{T}{T^*}\right)^{\beta_1}, & \text{for } T < T^*, \\ \dfrac{(v - S(z,v))\lambda T}{r-\mu} - \dfrac{z}{r}, & \text{for } T \geq T^*, \end{cases} \\ T^* &= \frac{\beta_1}{\beta_1 - 1}\frac{r-\mu}{(v - S(z,v))\lambda}\frac{z}{r}. \end{aligned}$$

- r $(< \mu)$: discount rate.

Optimal Level of Investment

- Case I:

$$z^* = \frac{(\frac{r}{r-\mu} v\gamma\alpha\lambda T^*)^{1/(\gamma+1)} - 1}{\alpha}.$$

- Case II:

$$z^* = \frac{\ln \frac{r-\mu}{r} - \ln(-\alpha v\lambda T^* \ln v)}{\alpha \ln v}.$$

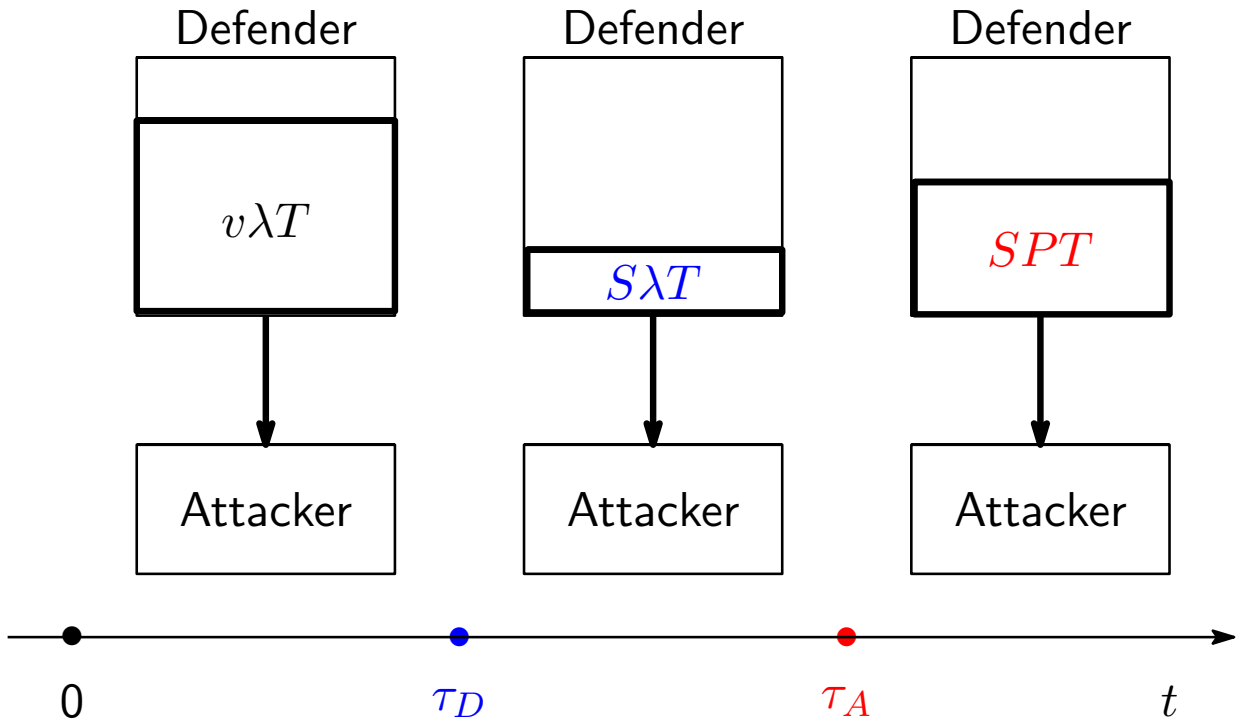
- Fixed point problem:

$$z^* = z(T^*(z)),$$

$\Rightarrow$ Iterative calculation.

Our Settings

- We add the attacker's perspective:
  - Defender's investment time: τ_D;
  - Attacker's investment time: τ_A,
  - The monetary loss will increase to $P(y, \lambda)$ by investing y dollar.



Increased Monetary Loss

Assumption (Increased monetary loss)

1. $\forall y, P(y,0) = 0,$
2. $\forall \lambda, P(0,\lambda) = \lambda,$
3. $\dfrac{\partial P(y,\lambda)}{\partial y} > 0,\ \dfrac{\partial^2 P(y,\lambda)}{\partial y^2} < 0$ *and* $\lim_{y\to\infty} P(y,v) = 1.$

- Example:

$$P^{\mathrm{II}} = 1 - (1-\lambda)^{\theta y+1}, \quad \theta > 0.$$

$\Rightarrow$ We consider only the Case II.

Preemptive Attack (1)

- We suppose that the attacker invests first at $\tau_A = 0$ $(< \tau_D)$.
- Defender maximizes its own value by choosing the investment timing:

$$F_D(T) = \sup_{\tau_D \in \mathcal{T}} \mathbb{E}\left[\int_0^{\tau_D} \mathrm{e}^{-rt} v(\lambda - P) T_t \mathrm{d}t + \int_{\tau_D}^{\infty} \mathrm{e}^{-rt}\{(v\lambda - SP)T_t - z\}\mathrm{d}t\right],$$

$$= \begin{cases} \left(\dfrac{(v-S)PT_D}{r-\mu} - \dfrac{z}{r}\right)\left(\dfrac{T}{T_D}\right)^{\beta_1} + \dfrac{v(\lambda - P)T}{r-\mu}, & T < T_D, \\ \dfrac{(v\lambda - SP)T}{r-\mu} - \dfrac{z}{r}, & T \geq T_D, \end{cases}$$

$$T_D = \frac{\beta_1}{\beta_1 - 1} \frac{r-\mu}{(v-S)P} \frac{z}{r}.$$

- $S := S(z, v)$ and $P := P(y, \lambda)$.

Preemptive Attack (2)

- On the other hand, the attacker's value depends on the defender's strategy T_D:

$$
\begin{aligned}
L_A(T) &= \mathbb{E}\left[\int_0^{\tau_D} \mathrm{e}^{-rt}\{v(P-\lambda)T_t - y\}\mathrm{d}t \right. \\
&\qquad \left. + \int_{\tau_D}^{\infty} \mathrm{e}^{-rt}\{(SP-v\lambda)T_t - y\}\mathrm{d}t\right], \\
&= \begin{cases} \dfrac{(S-v)PT_D}{r-\mu}\left(\dfrac{T}{T_D}\right)^{\beta_1} + \dfrac{v(P-\lambda)T}{r-\mu} - \dfrac{y}{r}, & T < T_D, \\ \dfrac{(SP-v\lambda)T}{r-\mu} - \dfrac{y}{r}, & T \geq T_D. \end{cases}
\end{aligned}
$$

- Optimal preemption at T_A^*:

$$
L_A^*(T) = L_A(T_A^*)\left(\frac{T}{T_A^*}\right)^{\beta_1}, \quad T < T_A^* = \frac{\beta_1}{\beta_1 - 1}\frac{r-\mu}{v(P-\lambda)}\frac{y}{r}.
$$

Preemptive Defense (1)

- We suppose that the defender invests first at $\tau_D = 0$ $(< \tau_A)$.
- Similar to the previous subsection, we can get the following attacker's value:

$$
\begin{aligned}
F_A(T) &= \sup_{\tau_A \in \mathcal{T}} \mathbb{E}\left[\int_0^{\tau_A} \mathrm{e}^{-rt}(S-v)\lambda T_t \mathrm{d}t \right. \\
&\qquad \left. + \int_{\tau_A}^{\infty} \mathrm{e}^{-rt}\left\{(SP-v\lambda)T_t - y\right\}\mathrm{d}t\right], \\
&= \begin{cases} \left(\dfrac{S(P-\lambda)T_A}{r-\mu} - \dfrac{y}{r}\right)\left(\dfrac{T}{T_A}\right)^{\beta_1} + \dfrac{(S-v)\lambda T}{r-\mu}, & T < T_A, \\ \dfrac{(SP-v\lambda)T}{r-\mu} - \dfrac{y}{r}, & T \geq T_A, \end{cases} \\
T_A &= \frac{\beta_1}{\beta_1 - 1}\frac{r-\mu}{S(P-\lambda)}\frac{y}{r}.
\end{aligned}
$$

Preemptive Defense (2)

- Defender's value:

$$L_D(T) = \mathbb{E}\left[\int_0^{\tau_A} \mathrm{e}^{-rt}\{(v-S)\lambda T_t - z\}\mathrm{d}t + \int_{\tau_A}^{\infty} \mathrm{e}^{-rt}\{(v\lambda - SP)T_t - z\}\mathrm{d}t\right],$$

$$= \begin{cases} \dfrac{S(\lambda-P)T_A}{r-\mu}\left(\dfrac{T}{T_A}\right)^{\beta_1} + \dfrac{(v-S)\lambda T}{r-\mu} - \dfrac{z}{r}, & T < T_A, \\ \dfrac{(v\lambda - SP)T}{r-\mu} - \dfrac{z}{r}, & T \geq T_A. \end{cases}$$

- Optimal preemption at T_D^*:

$$L_D^*(T) = L_D(T_D^*)\left(\frac{T}{T_D^*}\right)^{\beta_1}, \quad T < T_D^* = \frac{\beta_1}{\beta_1 - 1}\frac{r-\mu}{(v-S)\lambda}\frac{z}{r}.$$

Which is the preemptor?

- Attacker and defender has the incentive to preempt at $\bar{T}_A$ and $\bar{T}_D$:

$$L_i(\bar{T}_i) = F_i(\bar{T}_i), \quad i = A, D.$$

  - $\bar{T}_D < \bar{T}_A \Rightarrow$ defender is the preemptor,
  - $\bar{T}_D > \bar{T}_A \Rightarrow$ attacker is the preemptor.
- Four possibilities:
  1. $T_D^* < \bar{T}_A \Rightarrow$ defender's optimal preemption at T_D^*,
  2. $\bar{T}_D < \bar{T}_A < T_D^* \Rightarrow$ defender's preemption at $\bar{T}_A$,
  3. $T_A^* < \bar{T}_D \Rightarrow$ attacker's optimal preemption at T_A^*,
  4. $\bar{T}_A < \bar{T}_D < T_A^* \Rightarrow$ attacker's preemption at $\bar{T}_D$.

Optimal Solutions (1)

- Optimal solutions consist of the investment timing and level.
- The optimal level of investment at investment thresholds:

$$y_A = \arg\max_{y\in\mathbb{R}} F_A(T_A; y) = \frac{\ln\frac{r-\mu}{r} - \ln(-\theta S(1-\lambda)T_A \ln(1-\lambda))}{\theta \ln(1-\lambda)},$$

$$y_A^* = \arg\max_{y\in\mathbb{R}} F_A(T_A^*; y) = \frac{\ln\frac{r-\mu}{r} - \ln(-\theta S(1-\lambda)T_A^* \ln(1-\lambda))}{\theta \ln(1-\lambda)},$$

$$z_D = \arg\max_{z\in\mathbb{R}} F_D(T_D; z) = \frac{\ln\frac{r-\mu}{r} - \ln(-\alpha v P T_D \ln v)}{\alpha \ln v},$$

$$z_D^* = \arg\max_{z\in\mathbb{R}} F_D(T_D^*; z) = \frac{\ln\frac{r-\mu}{r} - \ln(-\alpha v P T_D^* \ln v)}{\alpha \ln v}.$$

- Calculation procedure (unverified):
  1. Fixed point problem: $y_A(T_A) = y_A^*(T_A^*)$ and $z_D(T_D) = z_D^*(T_D^*)$,
  2. Optimal response: $y_A^*(z) = y_A^*$ and $z_D^*(y) = z_D^*$,
  3. Equilibrium: (y_A^*, z_D^*).

Optimal Solutions (2)

- If preemption is not optimal at $\bar{T}_A$ and $\bar{T}_D$,
  - Investment level is not updated:

$$\bar{y}_A(\bar{T}_A) \neq y_A^*(T_A^*) \text{ and } \bar{z}_D(\bar{T}_D) \neq z_D^*(T_D^*).$$

  - In this case, optimal solutions cannot be converged.

Numerical Example

- Base case parameter:

σ	volatility	0.2
μ	expected growth rate	0.02
r	discount rate	0.05
v	vulnerability	0.5
λ	monetary loss	0.5
α	S-function	1
θ	P-function	1
z_D^*	defender's optimal investment	2.53
y_A^*	attacker's optimal investment	2.53
$S(z_D^*, v)$	remaining vulnerability	0.087
$P(y_A^*, \lambda)$	increased monetary loss	0.91
$T_D^*(z_D^*)$	defender's threshold	19.96
$T_A(y_A^*)$	attacker's threshold	115.02

Comparative Statics: v and λ

v	z_D^*	T_D^*	$\bar{T}_D$	T_D	y_A^*	T_A^*	$\bar{T}_A$	T_A
0.1	0.76	30.05	9.75	16.45	2.53	99.85	—	575.73
0.3	1.45	19.16	6.30	10.49	2.53	33.29	—	191.88
0.5	2.53	19.96	6.65	10.93	2.53	19.96	—	115.02
0.7	4.91	27.71	9.50	15.17	2.53	14.26	5.30	82.18
0.9	16.63	72.99	28.40	39.96	2.53	11.10	2.50	64.01
λ	z_D^*	T_D^*	$\bar{T}_D$	T_D	y_A^*	T_A^*	$\bar{T}_A$	T_A
0.1	2.53	99.85	5.75	11.83	16.63	72.99	—	420.98
0.3	2.53	33.29	6.20	11.37	4.91	27.71	—	159.91
0.5	2.53	19.96	6.65	10.93	2.53	19.96	—	115.02
0.7	2.53	14.26	7.20	10.53	1.45	19.16	—	110.38
0.9	2.53	11.10	8.10	10.16	0.76	30.05	1.65	173.43

Comparative Statics: θ and σ

θ	z_D^*	T_D^*	$\bar{T}_D$	T_D	y_A^*	T_A^*	$\bar{T}_A$	T_A
1	2.53	19.96	6.65	10.93	2.53	19.96	—	115.02
2	2.53	19.96	6.85	10.93	1.27	9.99	3.60	57.56
3	2.53	19.96	7.05	10.93	0.84	6.65	1.80	38.34
4	2.53	19.96	7.20	10.93	0.63	5.00	1.25	28.78
5	2.53	19.96	7.40	10.93	0.51	4.00	0.95	23.02
σ	z_D^*	T_D^*	$\bar{T}_D$	T_D	y_A^*	T_A^*	$\bar{T}_A$	T_A
0.1	1.81	12.16	4.10	7.09	1.81	12.16	—	42.66
0.2	2.53	19.96	6.65	10.93	2.53	19.96	—	115.02
0.3	3.21	32.15	10.90	16.99	3.21	32.15	—	298.56
0.4	3.84	49.51	17.20	25.65	3.84	49.51	—	707.86
0.5	4.40	72.88	26.10	37.33	4.40	72.88	—	1534.54

Comparative Statics: θ with $v = 0.1$ and $\lambda = 0.1$

$v = 0.1$

θ	z_D^*	T_D^*	$\bar{T}_D$	T_D	y_A^*	T_A^*	$\bar{T}_A$	T_A
1	0.76	30.05	9.75	16.45	2.53	99.85	—	575.73
3	0.76	30.05	10.00	16.45	0.84	33.29	—	191.94
5	0.76	30.05	10.20	16.46	0.51	19.96	—	115.10
7	0.76	30.05	10.35	16.46	0.36	14.26	4.80	82.22
9	0.76	30.05	10.55	16.45	0.28	11.10	3.15	63.98

$\lambda = 0.1$

θ	z_D^*	T_D^*	$\bar{T}_D$	T_D	y_A^*	T_A^*	$\bar{T}_A$	T_A
1	2.53	99.85	5.75	11.83	16.63	72.99	—	420.98
3	2.53	99.85	5.90	11.83	5.55	24.34	—	140.36
5	2.53	99.85	6.05	11.83	3.33	14.60	—	84.20
7	2.53	99.85	6.20	11.83	2.38	10.43	—	60.18
9	2.53	99.85	6.30	11.83	1.85	8.11	—	46.75
11	2.53	99.85	6.40	11.83	1.51	6.64	8.65	38.30

Comparative Statics: θ with $\sigma = 0.5$

$\sigma = 0.5$

θ	z_D^*	T_D^*	$\bar{T}_D$	T_D	y_A^*	T_A^*	$\bar{T}_A$	T_A
1	4.40	72.88	26.10	37.33	4.40	72.88	—	1534.54
2	4.40	72.88	26.70	37.33	2.20	36.44	—	767.27
3	4.40	72.88	27.10	37.33	1.47	24.29	6.80	511.51
4	4.40	72.88	27.45	37.33	1.10	18.21	4.15	383.49
5	4.40	72.88	27.75	37.33	0.88	14.58	2.95	307.02
6	—	—	—	—	—	—	—	—

Conclusion

- In this paper, we formulate a 2-players zero-sum game of information security investment from the defender's and attacker's perspectives in terms of real options approach.
- From numerical results:
  - In many cases, defender can preempt optimally and attacker has to wait.
  - If attacker can preempt, he invests immediately and slightly.
  - Efficiency of attack has large impact.
- Future works:
  - Rational setting for P-function,
  - Economic implications.