Security investment (failures) in five economic environments: A comparison of homogeneous and heterogeneous user agents

Jens Grossklags Nicolas Christin John Chuang

Presented By Qi Xie

Outline

- Introduction
- Three security games
- Nash with homogeneous and heterogeneous agents
- Social optima with homogeneous agents
- Conclusion & Discussion

Outline

- Introduction
- Three security games
- Nash with homogeneous and heterogeneous agents
- Social optima with homogeneous agents
- Conclusion & Discussion

Introduction

- Security game
  - A game-theoretic model
- Two key components
  - Self-protection
  - Self-insurance

Assumptions

- All entities in the network share a single purely public protection output
- A single individual decides on protection efforts for each entity

Generic utility function

$$U_i = M_i - p_i L_i (1 - s_i)(1 - H(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Generic utility function

Individual endowment

$$U_i = M_i - p_i L_i (1 - s_i)(1 - H(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Generic utility function

Individual endowment

$$U_i = M_i - p_i L_i (1 - s_i)(1 - H(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Probability attacks arrive

Generic utility function

Individual endowment   Loss

$$U_i = M_i - p_i L_i (1 - s_i)(1 - H(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Probability attacks arrive

Generic utility function

Individual endowment　Loss　Insurance level

$$U_i = M_i - p_i L_i (1 - s_i)(1 - H(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Probability attacks arrive

Generic utility function

$$U_i = M_i - p_i L_i (1 - s_i)(1 - H(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Individual endowment: M_i

Probability attacks arrive: p_i

Loss: L_i

Insurance level: s_i

Protection level: e_i

Generic utility function

Individual endowment Loss Insurance level

$$U_i = M_i - p_i L_i (1 - s_i)(1 - H(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Probability attacks arrive Protection levels other than i Protection level

Generic utility function

Individual endowment   Loss   Insurance level   Contribution function

$$U_i = M_i - p_i L_i (1 - s_i)(1 - H(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Probability attacks arrive   Protection levels other than i   Protection level

Generic utility function

Individual endowment
Loss
Insurance level
Contribution function
Unit cost of protection

$$U_i = M_i - p_i L_i (1 - s_i)(1 - H(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Probability attacks arrive
Protection levels other than i
Protection level

Generic utility function

$$U_i = M_i - p_i L_i (1 - s_i)(1 - H(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Individual endowment: M_i
Probability attacks arrive: p_i
Loss: L_i
Insurance level: s_i
Contribution function: $H(e_i, e_{-i})$
Protection levels other than i: e_{-i}
Unit cost of protection: b_i
Protection level: e_i
Unit cost of insurance: c_i

Outline

- Introduction
- Three security games
- Nash with homogeneous and heterogeneous agents
- Social optima with homogeneous agents
- Conclusion & Discussion

Three canonical security games

- Total effort security game
- Weakest-link security game
- Best shot security game
- Weakest target security game (without mitigation)
- Weakest target security game (with mitigation)

Total effort security game

- The overall protection level
  - Normalized sum of contributions

$$H(e_i, e_{-i}) = \frac{1}{N} \sum_i e_i$$

$$U_i = M_i - p_i L_i (1 - s_i)(1 - \frac{1}{N} \sum_k e_k) - b_i e_i - c_i s_i$$

Total effort security game

- Example:
  - In the BitTorrent p2p service, an attacker wants to slow down transfer of a given piece of information.

Weakest-link security game

- The overall protection level
  - The minimum contribution offered over all entities

$$H(e_i, e_{-i}) = \min(e_i, e_{-i})$$

$$U_i = M_i - p_i L_i (1 - s_i)(1 - \min(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Weakest-link security game

- Example:
  - A two-way communication, where the security of the communication is determined by the least secure communication parties.

Best shot security game

- The overall protection level
  - Maximum contribution offered over all entities

$$H(e_i, e_{-i}) = \max(e_i, e_{-i})$$

$$U_i = M_i - p_i L_i (1 - s_i)(1 - \max(e_i, e_{-i})) - b_i e_i - c_i s_i$$

Best shot security game

- Example:
  - A piece of information will remain available as long as a single node serving that piece of information can remain unharmed.

Summary of three security games

- Practical scenarios may involve social composition functions combining two or more of these games
- Example: Protecting a communication flow between two hosts

Outline

- Introduction
- Three security games
- Nash with homogeneous and heterogeneous agents
- Social optima with homogeneous agents
- Conclusion & Discussion

Homogeneous agents VS Heterogeneous agents

- Homogeneous agents
  - Share the same values for cost of protection and self-insurance
  - Individual faces the same threats with identical consequence if compromised
- Heterogeneous agents
  - Protection and self-insurance costs per unit are NOT necessary identical
  - The threats individual faces are NOT necessary the same
  - If compromised, consequences are NOT necessary identical

Homogeneous agents VS Heterogeneous agents (cont.)

- Recall the generic function

$$U_i = M_i - p_i L_i (1 - s_i) H(e_i, e_{-i}) - b_i e_i - c_i s_i$$

- Simplified generic function with homogeneous agents

$$U_i = M - pL(1 - s_i) H(e_i, e_{-i}) - be_i - cs_i$$

Nash Equilibrium analysis Total effort

- Homogeneous agents
  - Full protection eq: $(e_i, s_i) = (1, 0)$ if $(pL>bN$ && $c>b+pL(N-1)/N)$
  - Full self-insurance eq: $(e_i, s_i) = (0, 1)$ if $((pL>bN$ && $c<=b+pL(N-1)/N)$ || $c<pL<bN)$
  - Passive eq : $(e_i, s_i) = (0, 0)$ if $(pL<bN$ && $pL<c)$

Nash Equilibrium analysis Total effort

- Heterogeneous agents
  - Condition to select a protection-only strategy

$$\frac{1}{N-1}\sum_{j \neq i} e_j > 1 - \frac{N}{N-1}\frac{c_i - b_i}{p_i L_i}$$

Nash Equilibrium analysis Weakest-link

- Homogeneous agents
  - Multiple protection eq. $(e_i, s_i) = (e_0, 0)$ if (pL>b && (pL<c || (pL>=c && e_0>(pL-c)/(pL-b)))
  - Full self-insurance eq. $(e_i, s_i) = (0, 1)$ if (pL>c && (pL<b || (pL>=b && e_0<(pL-c)/(pL-b)))
  - Passive eq. $(e_i, s_i) = (0, 0)$ if (pL<b && pL<c)

Nash Equilibrium analysis Weakest-link

- Heterogeneous agents
  - Full protection eq. $(e_i, s_i) = (e_0, 0)$ if $(p_iL_i>b_i \;\&\&\; (p_iL_i<c_i \;||\; (p_iL_i>=c_i \;\&\&\; e_0>\max_i\{(p_iL_i-c_i)/(p_iL_i-b_i)\})))$
  - Multiple eq. without protection (above condition not hold)

Nash Equilibrium analysis Best shot

- Homogeneous agents
  - Full self-insurance eq. $(e_i, s_i) = (0, 1)$ if $(b<c)$
    - Should the condition be $c<b$ && $pL>c$?
  - Passive eq. $(e_i, s_i) = (0, 0)$ if ($pL<b$ && $pL<c$)
  - No protection eq.

Nash Equilibrium analysis
Best shot

- Heterogeneous agents
  - Possible protection eq. (e, s) = (1, 0) (Only one player faces disproportional losses || her protection costs are small)
  - Protection eq. are increasingly unlikely to happen as N grows

Outline

- Introduction
- Three security games
- Nash with homogeneous and heterogeneous agents
- Social optima with homogeneous agents
- Conclusion & Discussion

Social optima with homogeneous agents

- Total effort game
  - Protection $(e_i, s_i) = (1, 0)$ if (b<pL && b<c)
  - Self-insurance $(e_i, s_i) = (0, 1)$ if (c<pL && c<b)
  - Passive $(e_i, s_i) = (0, 0)$ if (c>pL && b>pL)
- Nash eq. of total effort game
  - Full protection eq: $(e_i, s_i) = (1, 0)$ (pL>bN && c>b+pL(N-1)/N)
  - Full self-insurance eq: $(e_i, s_i) = (0, 1)$ ((pL>bN && c<=b+pL(N-1)/N)) || c<pL<bN)
  - Passive eq : $(e_i, s_i) = (0, 0)$ (pL<bN && pL<c)

Social optima with homogeneous agents

- Total effort game
  - Protection $(e_i, s_i) = (1, 0)$ if $(b<pL$ && $b<c)$
  - Self-insurance $(e_i, s_i) = (0, 1)$ if $(c<pL$ && $c<b)$
  - Passive $(e_i, s_i) = (0, 0)$ if $(c>pL$ && $b>pL)$
- Nash eq. of total effort game
  - Full protection eq: $(e_i, s_i) = (1, 0)$ if $(pL>bN$ && $c>b+pL(N-1)/N)$
  - Full self-insurance eq: $(e_i, s_i) = (0, 1)$ if $((pL>bN$ && $c<=b+pL(N-1)/N))$ || $c<pL<bN)$
  - Passive eq : $(e_i, s_i) = (0, 0)$ if $(pL<bN$ && $pL<c)$

Social optima with homogeneous agents

- Weakest-link game
  - Protection $(e_i, s_i) = (1, 0)$ if $(b<pL \;\&\&\; b<c)$
  - Self-insurance $(e_i, s_i) = (0, 1)$ if $(c<pL \;\&\&\; c<b)$
  - Passive $(e_i, s_i) = (0, 0)$ if $(c>pL \;\&\&\; b>pL)$
- Nash eq. of weakest-link game
  - Multiple protection eq. $(e_i, s_i) = (e_0, 0)$ if $(pL>b \;\&\&\; (pL<c \;||\; (pL>=c \;\&\&\; e_0>(pL-c)/(pL-b)))$
  - Full self-insurance eq. $(e_i, s_i) = (0, 1)$ if $(pL>c \;\&\&\; (pL<b \;||\; (pL>=b \;\&\&\; e_0<(pL-c)/(pL-b)))$
  - Passive eq. $(e_i, s_i) = (0, 0)$ if $(pL<b \;\&\&\; pL<c)$

Social optima with homogeneous agents

- Weakest-link game
  - Protection $(e_i, s_i) = (1, 0)$ if $(b<pL$ && $b<c)$
  - Self-insurance $(e_i, s_i) = (0, 1)$ if $(c<pL$ && $c<b)$
  - Passive $(e_i, s_i) = (0, 0)$ if $(c>pL$ && $b>pL)$
- Nash eq. of weakest-link game
  - Multiple protection eq. $(e_i, s_i) = (e_0, 0)$ if $(pL>b$ && $(pL<c$ || $(pL>=c$ && $e_0>(pL-c)/(pL-b)))$
  - Full self-insurance eq. $(e_i, s_i) = (0, 1)$ if $(pL>c$ && $(pL<b$ || $(pL>=b$ && $e_0<(pL-c)/(pL-b)))$
  - Passive eq. $(e_i, s_i) = (0, 0)$ if $(pL<b$ && $pL<c)$

Social optima with homogeneous agents

- Best shot game
  - Protection (e, s) = (1, 0) if (b/c<N)
  - Insurance (e_i, s_i) = (0, 1) if (b/c>N)
- Nash eq. of best shot game
  - Full self-insurance eq. (e_i, s_i) = (0, 1) if (c<b && pL>c)
  - Passive eq. (e_i, s_i) = (0, 0) if (pL<b && pL<c)
  - No protection eq.

Social optima with homogeneous agents

- Best shot game
  - Protection (e, s) = (1, 0) if (b/c<N)
  - Insurance $(e_i, s_i) = (0, 1)$ if (b/c>N)
- Nash eq. of best shot game
  - Full self-insurance eq. $(e_i, s_i) = (0, 1)$ if (c<b && pL>c)
  - Passive eq. $(e_i, s_i) = (0, 0)$ if (pL<b && pL<c)
  - No protection eq.

Outline

- Introduction
- Three security games
- Nash with homogeneous and heterogeneous agents
- Social optima with homogeneous agents
- Conclusion & Discussion

Conclusions

- Model security decision-making by homogeneous and heterogeneous agents in selection of five games
- Find Nash Equilibria for homogeneous and heterogeneous agents in selection of five games
- Compare the Nash and social optima for homogeneous agents

Future research directions

- Extend the analysis to more formally explain the impact of limited information on agents strategies
- Develop a set of laboratory experiments to conduct user studies and attempt to measure the differences between rational behavior and actual strategies played

Discussions

- Strength
  - Plenty of examples
  - Well done proofs and computations
  - Good conclusion
- Weakness
  - Does not provide the simplified generic function
  - The condition of the protection Nash eq. is incorrect for the Best shot game with homogeneous agents