

Competitive Cyber-Insurance and Network Security

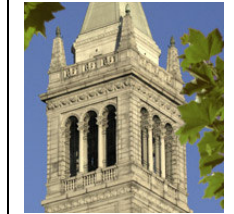


Nikhil Shetty
Galina Schwartz
Mark Felegyhazi
Jean Walrand

WEIS 2009 Presentation

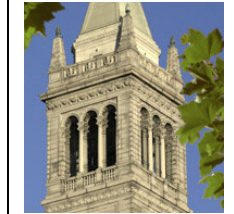
EECS, UC-Berkeley

Plan of talk



- Model [no-insurance]
- Model + insurance, if user security
 - I. non-contractible
 - II. contractible
- Main results
 - In many cases, missing cyber-insurance market (if I.)
 - In general, network security worsens with cyber-insurers
- Discussion

Model [no-insurance]

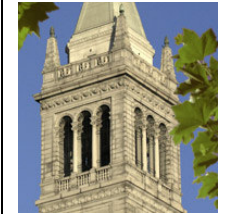


- Players: Identical users
 - W - Wealth
 - D - Damage (if successful attack) $D \in (0, W)$
 - If successful attack, wealth is $W - D$
 - p – probability of successful attack
 - Risk-averse users

$f(W)$ is concave: $f' > 0, f'' < 0$

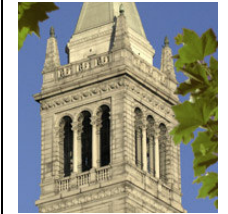
$$(1 - p) \cdot f(W) + p \cdot f(W - D)$$

Probability of successful attack [interdependent security]



- Probability p depends on
 - user security (“private good”) AND
 - network security (“public good”) [externality]
- Interdependent security = externality:
 - Individual users: no effect on network security, but
 - User’s security choice affects network security

Network Security

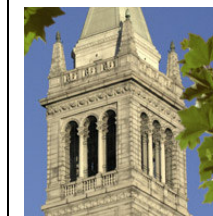


- Popular - Varian (2002) (weakest link, best shot, total effort)
- Our assumptions about network security:
 - Idea: network security is a function of average user security
 - This paper: network security = average user security

$$p_i = (1 - s_i) \cdot (1 - \bar{s}) = v_i \cdot \bar{v} \text{ and } \bar{s} = \frac{1}{N} \sum_{n=1, \dots, N} s_n$$

$$p = v\bar{v}$$

User Utility



- User's trade-off: Security vs convenience (usability)

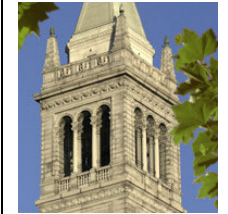
$$U = (1 - p) \cdot f(W) + p \cdot f(W - D) + g(a) - h(s, a)$$

$$p = v\bar{v}$$

$f(\cdot)$ & $g(\cdot)$ are concave: $f', g' > 0, f'', g'' < 0$

$h(\cdot)|_{\text{fixed } a}$ is convex: $h', h'' > 0, h(0) = 0$ and $h(1) = \infty$

Optimized User Utility



$$U = (1 - p) \cdot f(W) + p \cdot f(W - D) + g(a) - h(s, a)$$

$$p = v\bar{v}$$

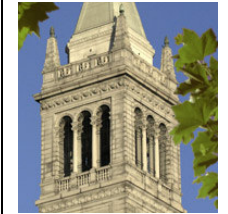
- A companion paper - similar results for general functions (f & h).

- This paper: $f(x) = g(x) = \sqrt{x}$ and $h(x) = \frac{1}{\sqrt{1-x} - 1}$

After users
optimize
applications:

$$U = (1 - p)\sqrt{W} + p \cdot \sqrt{W - D} + \sqrt{v}$$

Nash Equil. vs Social Optimum [No-Insurance]



- User Utility

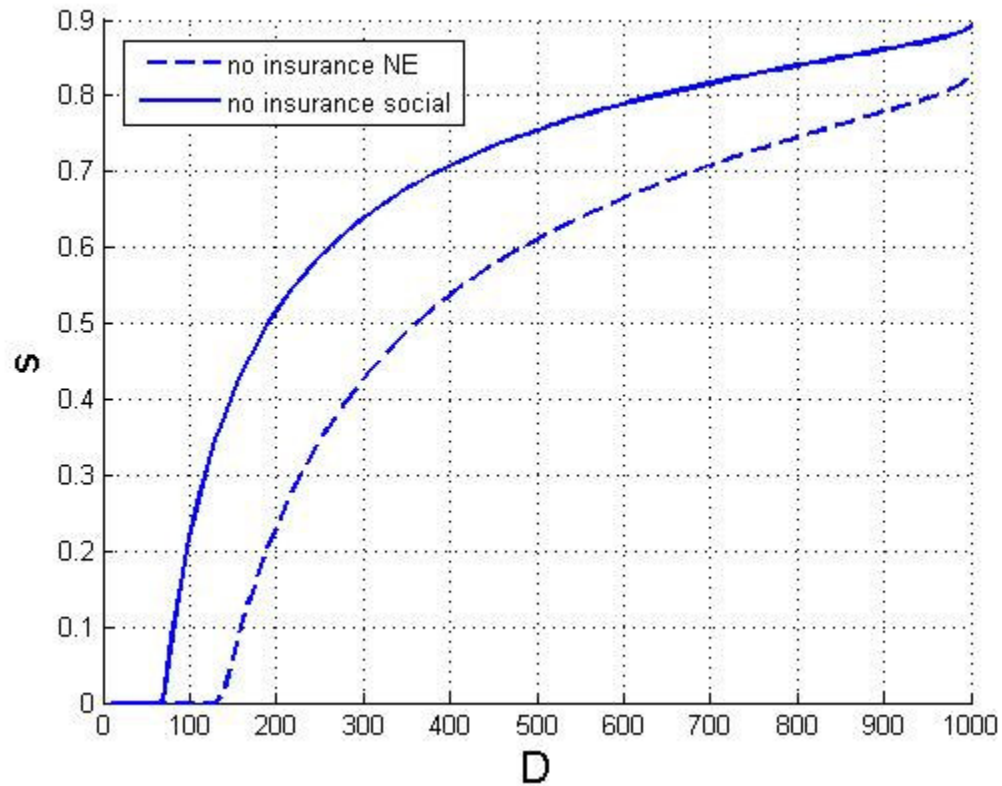
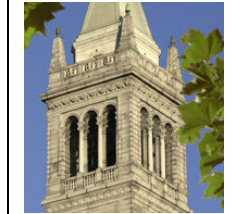
$$U = \sqrt{W} - v\bar{v}(\sqrt{W} - \sqrt{W - D}) + \sqrt{v}$$

- Nash equilibrium vs Social Optimum

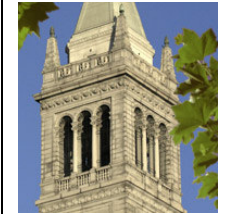
$$v^{soc} < v^* \text{ or } s^{soc} > s^*$$

- If D/W is small, security is zero (or close to 0)

Security: Nash vs Social Optimum

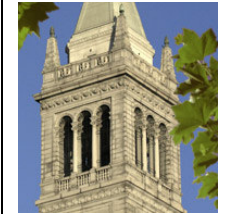


Model of competitive cyber-insurers



- We follow Rothschild & Stiglitz (1976)
- Each insurer offers a single contract. Nash equilibrium is a set of admissible contracts
 - i) each insurer's profit is non-negative
- For a given set of offered contracts
 - ii) no entrant-insurer can enter and make a strictly positive profit
 - iii) no incumbent-insurer can increase his profit by altering his contract

Competitive cyber-insurers



- Insurers are risk neutral & each maximizes his profit

$$\Pi = \rho - v\bar{v}L$$

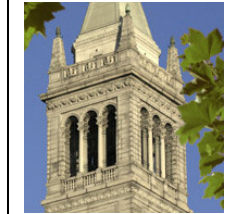
ρ - user's premium, L - the covered loss

- Perfectly competitive insurers \rightarrow zero profits

$$\rho = v\bar{v}L$$

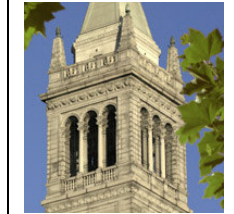
- We consider 2 cases. If user security is:
 - I. Non-contractible
 - II. Contractible

Competitive cyber-insurers (cont.)



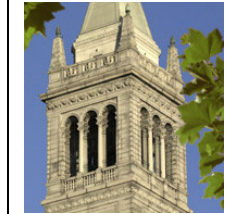
- Insurers:
 - free entry
 - zero operating costs
 - take network security as given
- Cases: if user security is
- I. Non-contractible Contract (ρ, L)
 - Contract prohibits purchasing extra coverage
- II. Contractible Contract (v, ρ, L)

Equilibrium with cyber-insurers



- From insurer competition:
- User chooses from which insurer to buy a contract
 - ➔ In equilibrium,
all contracts give a user identical utility
- Only contracts maximizing user utility attract users
 - ➔ In equilibrium,
all contracts maximize user utility
- User participation constraint must hold

I. non-contractible v



- Contract: (ρ, L) ; extra coverage is prohibited

ρ - user's premium, L - the covered loss

$$U(v, \bar{v}, \rho, L) = (1 - v\bar{v})\sqrt{W - \rho + v\bar{v}\sqrt{W - \rho - D + L} + \sqrt{v}}$$

- If $D < 8/9 W$ - Missing cyber-insurance market

[no equilibrium with positive insurance coverage exists]

- If $D > 8/9 W$ - equilibrium contract may exist but loss covered is small \rightarrow market is small

$$(\rho^\ddagger, L^\ddagger)$$

Equilibrium security

[I. non-contractible v]

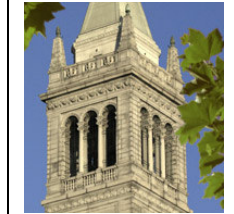


- When equilibrium with positive coverage exists, security worsens relative to no-insurance Nash

$$v^{\dagger} > v^*.$$

- Why security is worse? user's incentives to invest in security worsen (risk is covered!)
- With insurance [& non-contractible v]
 - utility is higher than with no-insurance
 - but aggregate damage is higher too

II. contractible v



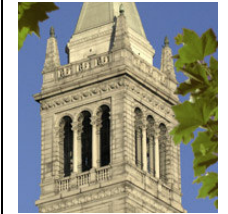
Contract (v, ρ, L)

v - vulnerability is at most v
(required user security is at least $s = 1 - v$)

ρ - user's premium
 L - the covered loss

Equilibrium

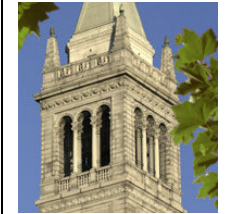
[II. contractible v]



- In equilibrium, no user deviates to no insurance
 - If not, some insurer will offer contract with a deviating security level (with insurance, user utility is higher)
- Entire damage D is covered
 - If not, some insurer will offer a contract with a higher coverage →

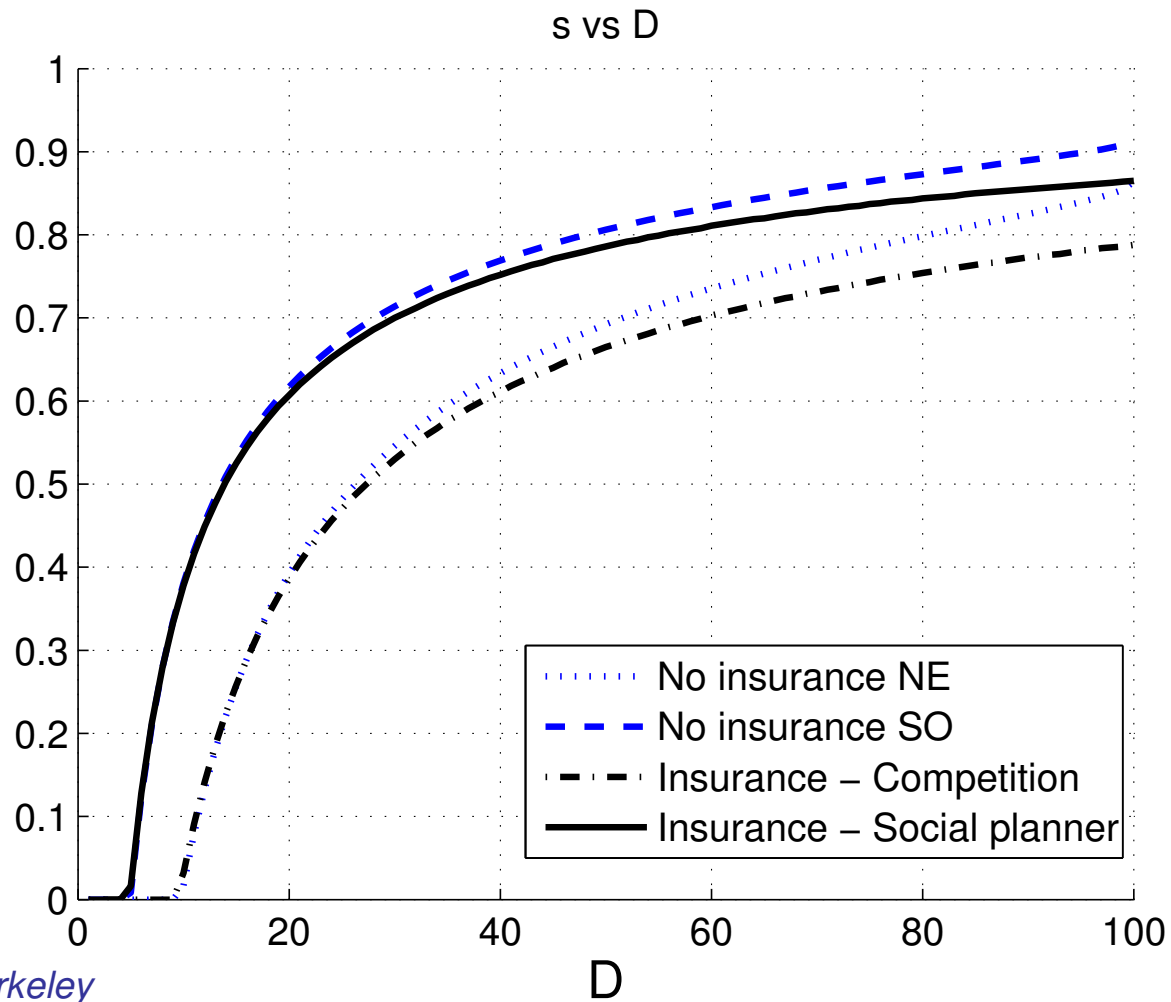
$$L^\dagger = D \text{ and } \rho^\dagger = v\bar{v}D$$

Equilibrium security with insurance [II. contractible v]

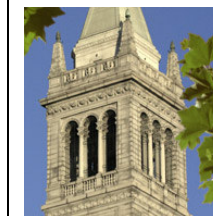


- Equilibrium contract $(v^\dagger, \rho^\dagger, L^\dagger)$
 - is unique
 - it covers the entire damage D
- We have: $v^* \gtrless v^\dagger$
 - If D/W is very low: $v^\dagger < v^*$
 - If D/W is high: $v^* < v^\dagger$

Security Levels [II. Contractible]



Conclusion



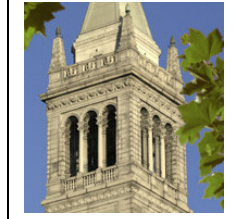
- Asymmetric information causes missing markets
 - A well know result of missing markets from the classical papers:
Akerlof (1970) ; Rothschild and Stiglitz (1976)
 - Cyber-insurance is a convincing case of market failure
- I. non-contractible user security (a lot of asymmetric info)
 - For most parameters, cyber insurance market is missing
- II. contractible user security (only some asymmetric info)
 - For most parameters, security worsens relative to no-insurance case

Missing cyber-insurance market & information asymmetries – a link



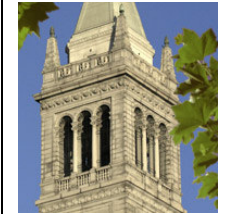
- Asymmetric information (present in our model):
 - I. non-contractible case:
 - Insurers: no info about user security
 - Insurers: no info about each other
 - II. Contractible case:
 - Insurers: no info about each other
- Other info asymmetries could matter:
 - damage size and attack probability (for both, users & insurers)

Conclusion (cont.)



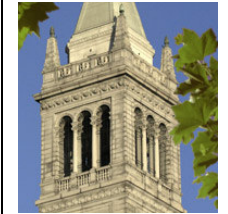
- Even if cyber insurance would exist, improved network security is unlikely
 - With cyber-insurers, user utility improves, but in general, network security worsens; sec. increases only if D/W is very low
- Insurers fail to improve security. Why?
 - Insurers free-ride on other insurers, which lowers security
 - Insurance is a tool for risk redistribution, not risk reduction

Extensions



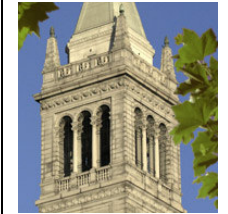
- Our setting: identical users
 - If user types differ: results should hold for each subtype
- Our setting: specific functions for user utility & security costs
 - A companion paper shows that most results holds for general functions

Cyber-insurers as car dealers: trading lemons?



- What do cyber-insurers sell?
 - Indulgences??
 - Are cyber insurers selling us the peace of mind?
- Connecting with the next talk: Developing security ratings: how to get from I. (non-contractible v) to II. (contractible v)?

How to?



- Problems to resolve (for cyber-insurance to take off)
 - Reduce information asymmetries (tools: disclosure laws, requirements on standard (defaults) settings on security software ...)
 - Reduce network externalities (tools: imposition of limited user liability, i.e., mandating user security level)
- But – this is very difficult (technologically and politically)