



University of  
Connecticut

School of Business

# Economics of Information Security

Dmitry Zhdanov, University of Connecticut

MIS Research Center, University of Minnesota

May 1, 2009

# Agenda

---

- ▶ Why look at economics of information security?
- ▶ IS Security and Risk Management
- ▶ Economics of Managed Security
- ▶ Economics of Compliance Incentives
- ▶ Issues in Measurement and Policy for IS Security





## Computer Crime & Intellectual Property Section United States Department of Justice

[Home](#)[Computer Crime](#)[Intellectual Property](#)[Electronic Evidence](#)[Other High Tech Legal Issues](#)[About CCIPS](#)[News](#)[Site Index](#) 

## Computer Crime & Intellectual Property Section

### Latest Press Releases

- [Virginia Man Pleads Guilty to Selling Counterfeit Computer Software Worth \\$1 Million \(April 16, 2009\)](#)
- [Florida Man Arrested on Federal Sex Trafficking Charges for Prostituting Girl He Solicited on Internet \(April 15, 2009\)](#)
- [Owner and Operator of Massachusetts Computer Parts Company Pleads Guilty to Wire Fraud and Money Laundering in Connection with \\$15.4 Million Dollar Cisco Networking Equipment Fraud \(April 10, 2009\)](#)
- [San Antonio Woman Sentenced to Federal Prison for Trafficking over Two Million Dollars Worth of Counterfeit Goods \(April 9, 2009\)](#)
- [Maple Grove Man Sentenced for Wire Fraud, Identity Theft \(March 31, 2009\)](#)
- [Statement of Rita M. Glavin, Acting Assistant Attorney General, Criminal Division, Concerning "Do the Payment Card Industry Standards Reduce Cybercrime?" \(March 31, 2009\)](#)
- [Ramsey Couple Sentenced for Conspiracy to Defraud Cable Television Service Providers \(March 26, 2009\)](#)
- [Former Folsom Resident Pleads Guilty to Trafficking in Counterfeit Merchandise \(March 25, 2009\)](#)
- [Distributor of Counterfeit Pharmaceuticals Drugs Convicted \(March 23, 2009\)](#)
- [Upland Man Indicted for Allegedly Damaging Computer Systems Used to Monitor Off-shore Oil Platforms \(March 17, 2009\)](#)
- [60th Felony Conviction Obtained in Software Piracy Crackdown "Operation Fastlink" \(March 6, 2009\)](#)
- [Two Indicted for Conspiring to Steal Trade Secrets from Goodyear Tire and Rubber Company \(March 6, 2009\)](#)
- [Information Security Consultant Sentenced to 4 Years in Prison in Federal Wiretapping and Identity Theft Case \(March 4, 2009\)](#)
- [Two Plead Guilty to Defrauding Trucking Companies in Multi-million Dollar Scheme That Used Internet Site \(February 24, 2009\)](#)
- [Three Charged in Movie Piracy Cases Involving Illegal Posting of Theatrical Films on Internet \(February 20, 2009\)](#)
- [Texas Man Sentenced to 41 Months in Prison for Selling Counterfeit Software Worth \\$1 Million on Web Sites \(February 17, 2009\)](#)
- [Former Metaldyne Employees Sentenced to Prison in to Conspiracy to Steal Confidential Business Information to Benefit Chinese Competitor \(F](#)

## CSI survey 2008

---

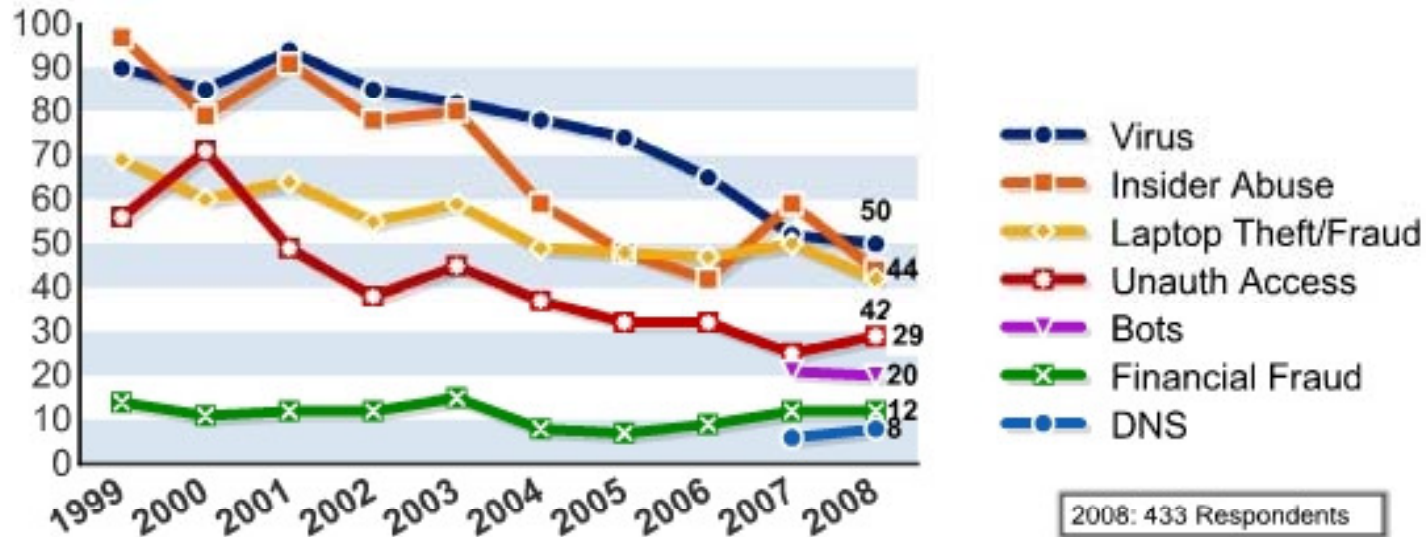
- ▶ The most expensive computer security incidents were those involving financial fraud...
- ▶ ...with an average reported cost of close to \$500,000 (for those who experienced financial fraud). The second-most expensive, on average, was dealing with “bot” computers within the organization’s network, reported to cost an average of nearly \$350,000 per respondent. The overall average annual loss reported was just under \$300,000

<http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf>

---



# 2008 CSI Survey

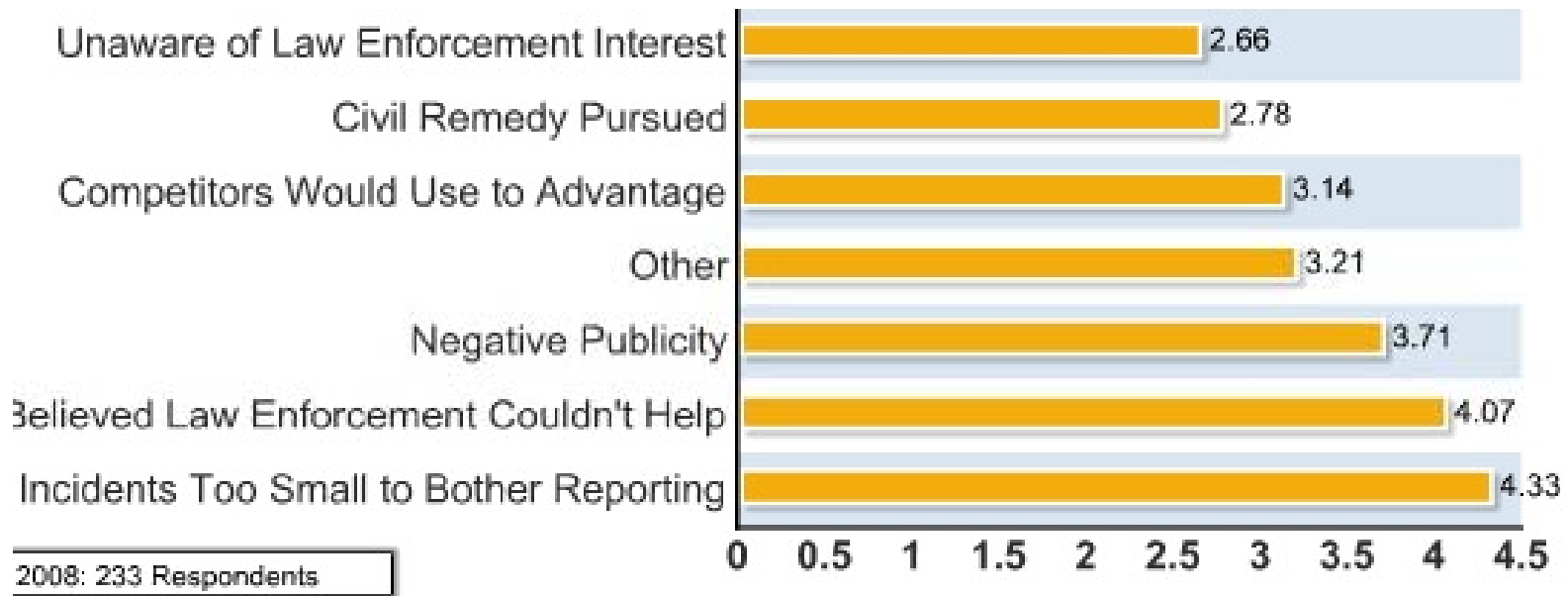


Also, abuse of wireless – 14%; IM abuse – 21%, loss of customer data – 17%

<http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf>

# Companies are secretive

---



Only 27% of incidents were reported to law enforcement

<http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf>

---



# Why does cybercrime exist?

---

- The potential value of engaging in cybercrime would not be realized if a market for stolen data did not exist. The social network that is the by-product of the information black market enables players in the criminal underground (hackers, fraudsters, and organized crime groups) to collaborate with one another to find vulnerable systems, compromise data, and commit fraud. Additionally, this market has made the incentives available to a broader population and has allowed individuals and smaller groups to participate in any phase of the data compromise life cycle they choose.
- This combination of powerful motivation and an accessible market has enabled the business of cybercrime to grow quickly and rapidly. Prior to the market's existence, the hacker may not have had the social network to sell stolen data and the fraudster may have been limited in the volume of data available to them. A marketplace for compromised data facilitates networking among likeminded criminals, lowers barriers to entry, and enables individuals or groups to make money through cybercrime. Ultimately, it allows the pilfered zeros and ones to be converted into cash and material goods.

# More scary things

---

- ▶ 69% of breaches were not discovered by the victim
- ▶ 83% of attacks were not highly difficult
- ▶ 67% were aided by significant errors
- ▶ 39% involved multiple parties
- ▶ 87% were considered avoidable through reasonable controls

Verizon Data Breach Report 2009

<http://www.verizonbusiness.com/resources/security/databreachreport.pdf>



# 10 Deadly Sins of Information Security

---

- ▶ 1. Not realizing that information security is a corporate governance responsibility
- ▶ 2. Not realizing that information security is a business issue and not a technical issue
- ▶ 3. Not realizing that information security governance is a multi-dimensional discipline
- ▶ 4. Not realizing that information security plan must be based on identified risks
- ▶ 5. Not realizing (and leveraging) the importance of international best practices

B.Von Solms, R. von Solms, 2004 (Computers and Security)

---



# 10 Deadly Sins of Information Security

---

- ▶ 6. Not realizing that a corporate information security policy is absolutely essential
- ▶ 7. Not realizing that information security compliance enforcement and monitoring is absolutely essential
- ▶ 8. Not realizing that a proper information security governance structure is absolutely essential
- ▶ 9. Not realizing the core importance of information security awareness amongst users
- ▶ 10. Not empowering information security managers with the infrastructure, tools and supporting mechanisms to properly perform their responsibilities

B.Von Solms, R. von Solms, 2004 (Computers and Security)

---



# Why do good users make bad decisions?

---

- ▶ Users do not think they are at risk
- ▶ Users aren't stupid, they are unmotivated
- ▶ Safety is an abstract concept
- ▶ Feedback and learning from security-related decisions is weak
- ▶ Making trade-offs between risk, losses, gains and costs
- ▶ Users are more likely to gamble on a loss than accept a guaranteed loss
- ▶ Losses are perceived disproportionately to gains
- ▶ Security is a secondary task

R. West "The Psychology of Security", 2008 (CACM)

---



# Why economics?

---

- ▶ Focuses on business and individual decision making
- ▶ Provides policy advice
- ▶ Suited well to do numerical estimates, which can translate to quantifiable decisions
- ▶ Some level of abstraction allows to focus on a few key issues and filter out “noise”
  
- ▶ “All models are wrong, but some are useful”
  - ▶ Attributed to George Cox



# IS Security and Risk Management

# Risk Management

---

- ▶ The dictionary defines risk as the possibility of loss.
- ▶ Carnegie Mellon University's Software Engineering Institute (SEI) defines *continuous risk management* as: processes, methods, and tools for managing risks in a project.
- ▶ Information security is not a *state*, it is a *process*!



# Qualitative versus Quantitative Risk Assessment

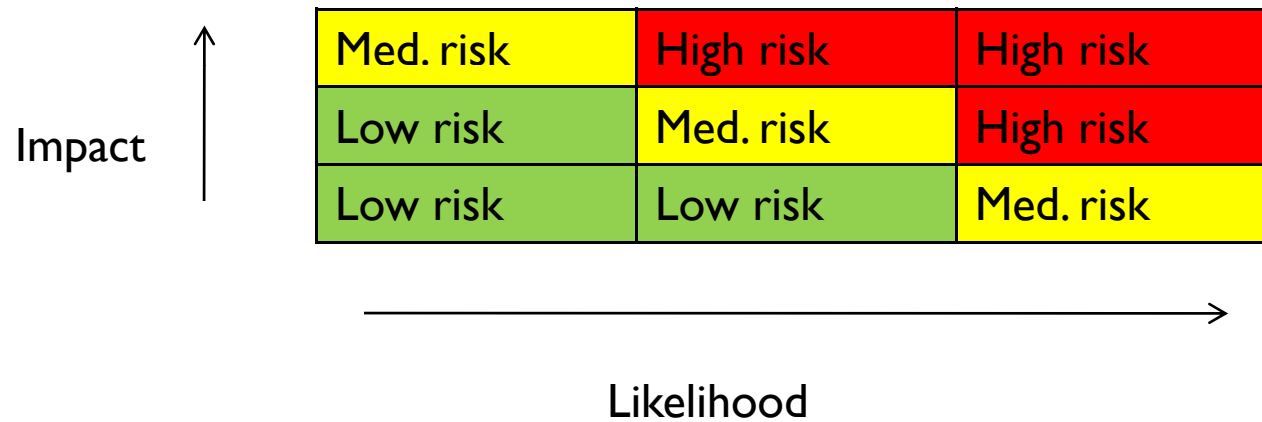
---

- ▶ It is impossible to conduct risk management that is purely quantitative.
- ▶ Usually risk management includes both qualitative and quantitative elements, requiring both analysis and judgment or experience.
- ▶ It is possible to accomplish purely qualitative risk management.



# Qualitative risk assessment

---



A qualitative risk assessment matrix with 'Impact' on the vertical axis and 'Likelihood' on the horizontal axis. The matrix is a 3x3 grid of colored cells. The top row contains 'Med. risk' (yellow), 'High risk' (red), and 'High risk' (red). The middle row contains 'Low risk' (green), 'Med. risk' (yellow), and 'High risk' (red). The bottom row contains 'Low risk' (green), 'Low risk' (green), and 'Med. risk' (yellow). Arrows indicate the direction of increasing impact and likelihood.

Med. risk	High risk	High risk
Low risk	Med. risk	High risk
Low risk	Low risk	Med. risk



# Quantitative risk assessment

---

▶  **$ALE = ARO \times SLE$**

□  $SLE = AV \times EF$

- ▶ ALE = Annualized loss expectancy
- ▶ ARO = Annual rate of occurrence
- ▶ SLE = Single loss expectancy
- ▶ AV = Asset value
- ▶ EF = Exposure factor

Is there something wrong with this approach?



# Alternative methods

---

- ▶ Value at risk
- ▶ Ruin theory
- ▶ Info-gap decision theory



# Some tools include

---

- ▶ **Threat Modeling Tool (Microsoft)**

- ▶ <http://www.microsoft.com/downloads/details.aspx?FamilyID=62830f95-0e61-4f87-88a6-e7c663444ac1&displaylang=en>

- ▶ **Practical Threat Analysis (PTA)**

- ▶ <http://www.ptatechnologies.com/>

- ▶ **Security Officer's Best Friend (SOBF/ORICO)**

- ▶ <http://www.somap.org/>
- ▶ [http://sourceforge.net/project/showfiles.php?group\\_id=105538](http://sourceforge.net/project/showfiles.php?group_id=105538)



# SOBF

---

- ▶ Free
- ▶ Part of SOMAP
  - ▶ Security Officer Management and Analysis Project
  - ▶ Includes a good risk management guide
- ▶ Requires (properly configured) Java runtime



# Threat Modeling Tool

---

- ▶ Kind of dated (2004)
- ▶ Integrates support for diagrams in Visio
- ▶ Makes use of STRIDE and DREAD classifications
- ▶ Includes mitigation and investigation scenarios
- ▶ Does not include financial estimates



# What is STRIDE

---

- ▶ Microsoft's approach to threat modeling
- ▶ **S**poofing Identity
- ▶ **T**ampering with data
- ▶ **R**epudiation
- ▶ **I**nformation Disclosure
- ▶ **D**enial of Service
- ▶ **E**levation of privilege
  
- ▶ <http://msdn.microsoft.com/en-us/library/ms954176.aspx>



# What is DREAD

---

- OWASP's extension to STRIDE, providing some quantifiable measure for vulnerabilities
- **D**amage Potential
- **R**eproducibility
- **E**xploitability
- **A**ffected users
- **D**iscoverability
- All scored on the scale 0-10
- $DREAD = (D_1 + R + E + A + D_2)/5$
- [http://www.owasp.org/index.php/Threat\\_Risk\\_Modeling#DREAD](http://www.owasp.org/index.php/Threat_Risk_Modeling#DREAD)



# PTA

---

- ▶ Geared for quantitative risk analysis
- ▶ For assets, includes fixed and recurring values
- ▶ For countermeasures, includes cost of implementation
- ▶ For threats, includes probability of occurrence, damage to assets and mitigation level



# Economics of Managed Security

# Motivation

---

- ▶ Many IT professionals feel strongly that information security is a core business function, and outsourcing it would be equivalent to handing over the keys to the kingdom. (Network Computing, Aug. '06)
- ▶ Organizations are increasingly accepting the appropriateness and potential value of the selective outsourcing of operational security activities (Gartner, 2007)
- ▶ “We anticipate this market will continue its [26 percent annual] growth trajectory for at least the next five years.” (Yankee Group 2006).



# Research Problem

---

- ▶ Explore the issues of size and growth of a Managed Security Services Provider (MSSP) network
  - ▶ Explore potential stalling problem and role of investment in overcoming it
  - ▶ Compare the growth dynamics for consortium-based and for-profit MSSPs



# Background Literature

---

- ▶ Economic incentives in information security decisions
- ▶ Alliance formation
- ▶ Network effects in economics
  - ▶ Growth and optimal size of networks
  - ▶ Network ownership
  - ▶ Pricing of service
  - ▶ Direction of network effects



# Model setup

---

- ▶ Single provider, identical firms
- ▶ Counter-acting forces
  - ▶ Larger networks are more attractive, but also can learn and apply defenses faster for all network members
- ▶ Provisioning of higher security levels is increasingly hard
- ▶ Firms as price takers; arrive one at a time after some starting size



# Model constructs

---

- ▶  $N$  – network size
- ▶  $V(N)$  – value of the network
- ▶  $R(N)$  – resources required to maintain the network
  
- ▶  $P_a(N)$  – probability of a random attack
- ▶  $P_s(N)$  – probability of attack success



# Model Exploration

---

- ▶ A simulation using KDD CUP data set
- ▶ Firms are represented by randomly pooling a set of connections together
- ▶ Attack classification using decision trees
- ▶ Classification error measures the probability of attack success
- ▶ As network grows, firms' resources are pooled together



# Example decision tree

---

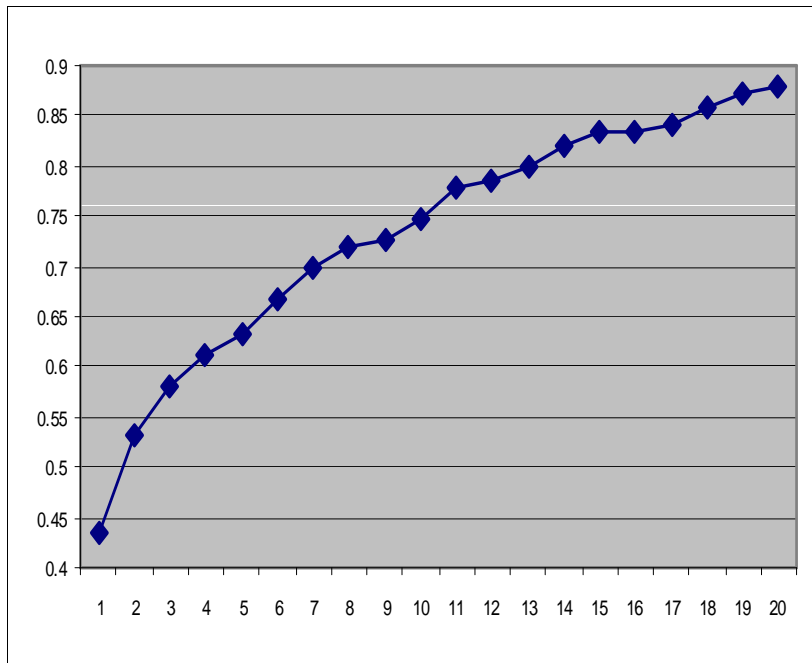
## Decision tree

- Count < 367,5000
  - same\_srv\_rate < 0.3050 then attack\_type = **neptune**. (99.54 % of 219 examples)
  - same\_srv\_rate >= 0.3050
    - Hot < 1.5000 then attack\_type = **normal**. (96.98 % of 199 examples)
    - Hot >= 1.5000 then attack\_type = **back**. (60.00 % of 5 examples)
- Count >= 367,5000
  - protocol\_type in [udp] then attack\_type = **normal**. (0.00 % of 0 examples)
  - protocol\_type in [icmp] then attack\_type = **smurf**. (100.00 % of 570 examples)
  - protocol\_type in [tcp] then attack\_type = **satan**. (100.00 % of 6 examples)

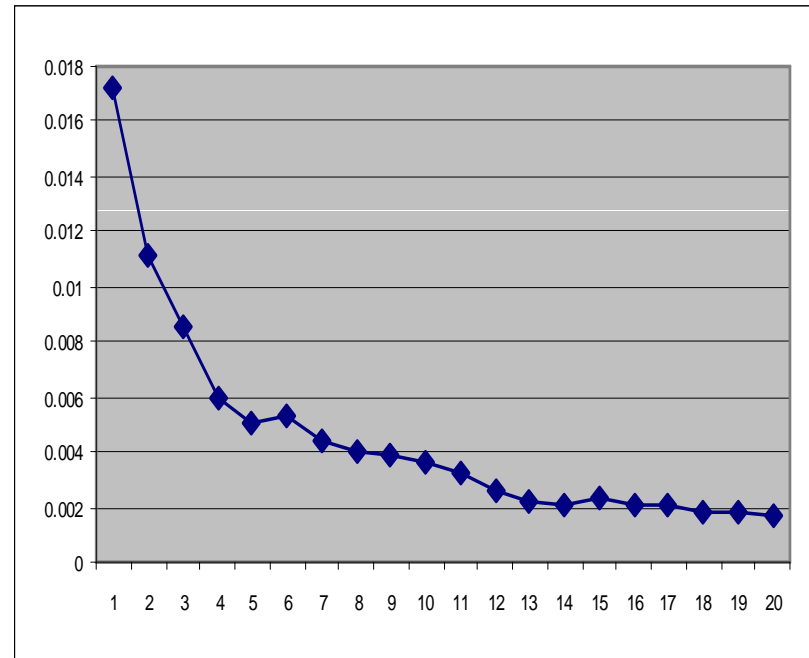


# Probability plots

---



Pa



Ps

---



# Hiding and Knowledge Effects

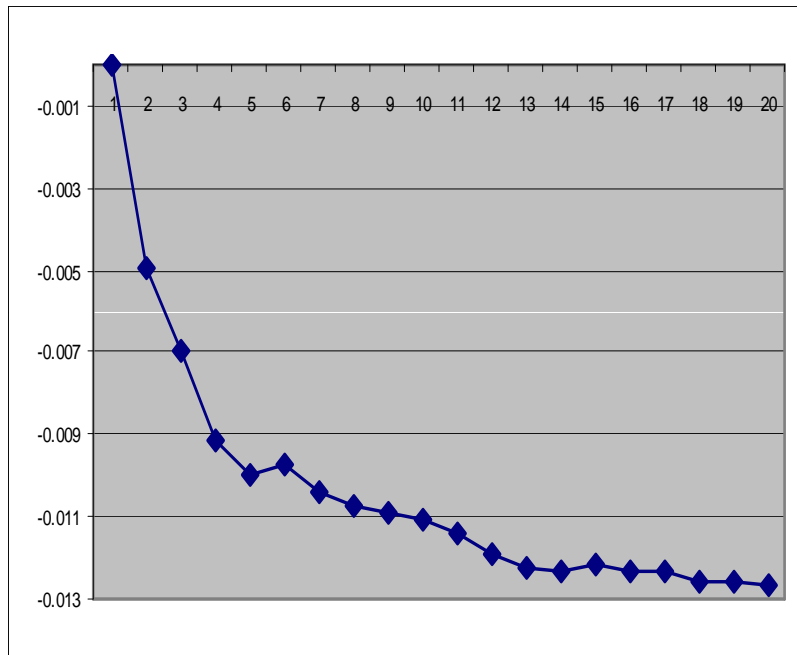
---

- ▶ Two reasons why being on a larger network may reduce the individual risk of being attacked
  - ▶ Being less noticeable among similar targets
  - ▶ Better detection capabilities due to access to larger knowledge base
- ▶ “Generally, recognizing a bad external thing on behalf of one customer means you've recognized it for all customers” (Gartner, 2006)
- ▶ BT Counterpane: “Over 850,000 event rules for a broad range of network devices, monitoring 550 networks in 38 countries”

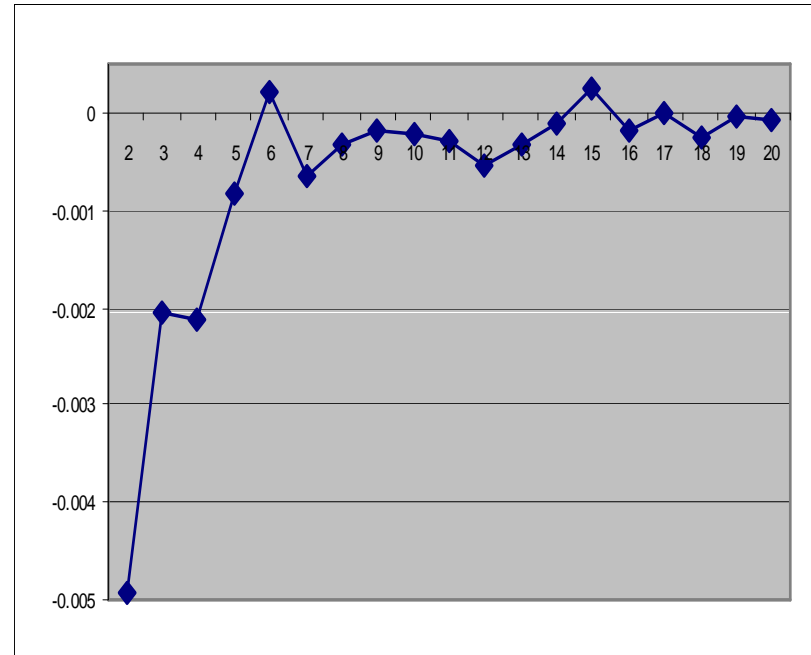


# Hiding and Knowledge Effects

---



Hiding Effect



Knowledge Effect



# Consortium MSSP

---

- ▶ Several firms decide to start the network
- ▶ Equal sharing of initial investment cost
- ▶ Key results: consortium size will not exceed welfare maximizing size
- ▶ Consortia that require start-up investment will be of larger size
- ▶ Equal sharing is optimal strategy



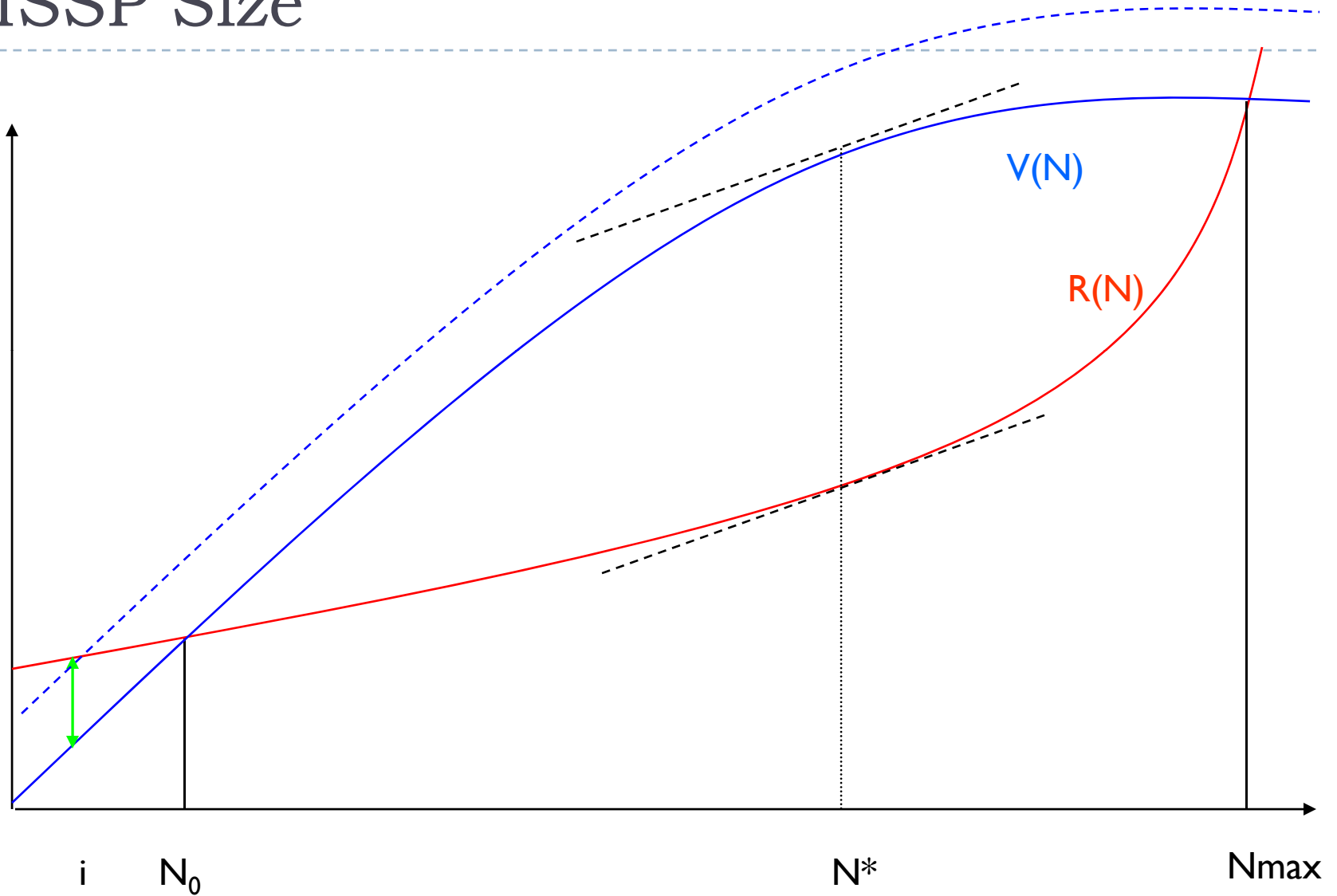
# For-profit MSSP

---

- ▶ Single provider starts the network
- ▶ Acting as a monopolist, able to execute price discrimination
  
- ▶ Key results:
- ▶ Network size may be larger than welfare maximizing (thus, larger than consortium)
- ▶ Optimal size does not depend on the initial investment
- ▶ Introductory pricing (free access) helps build critical mass



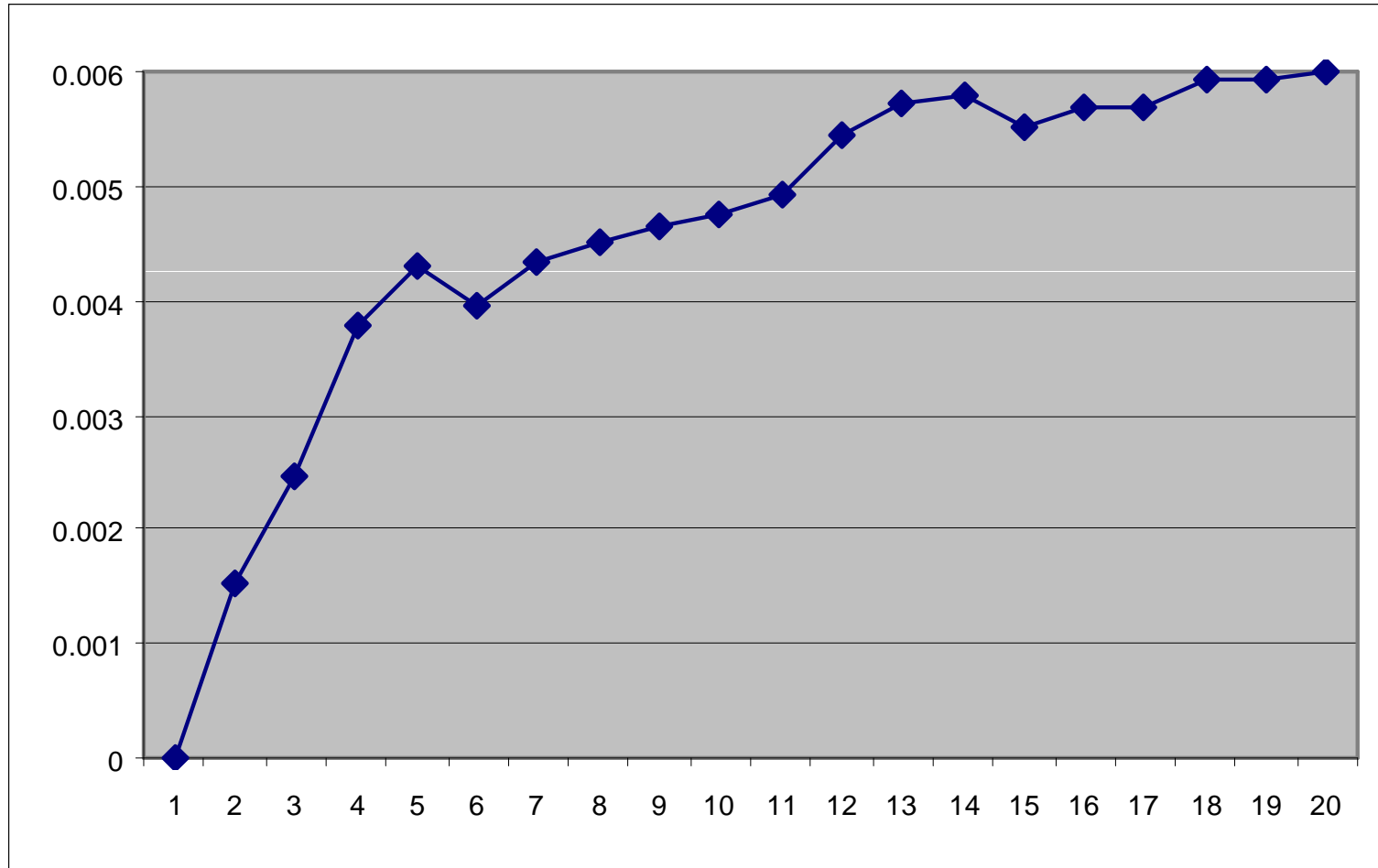
# MSSP Size



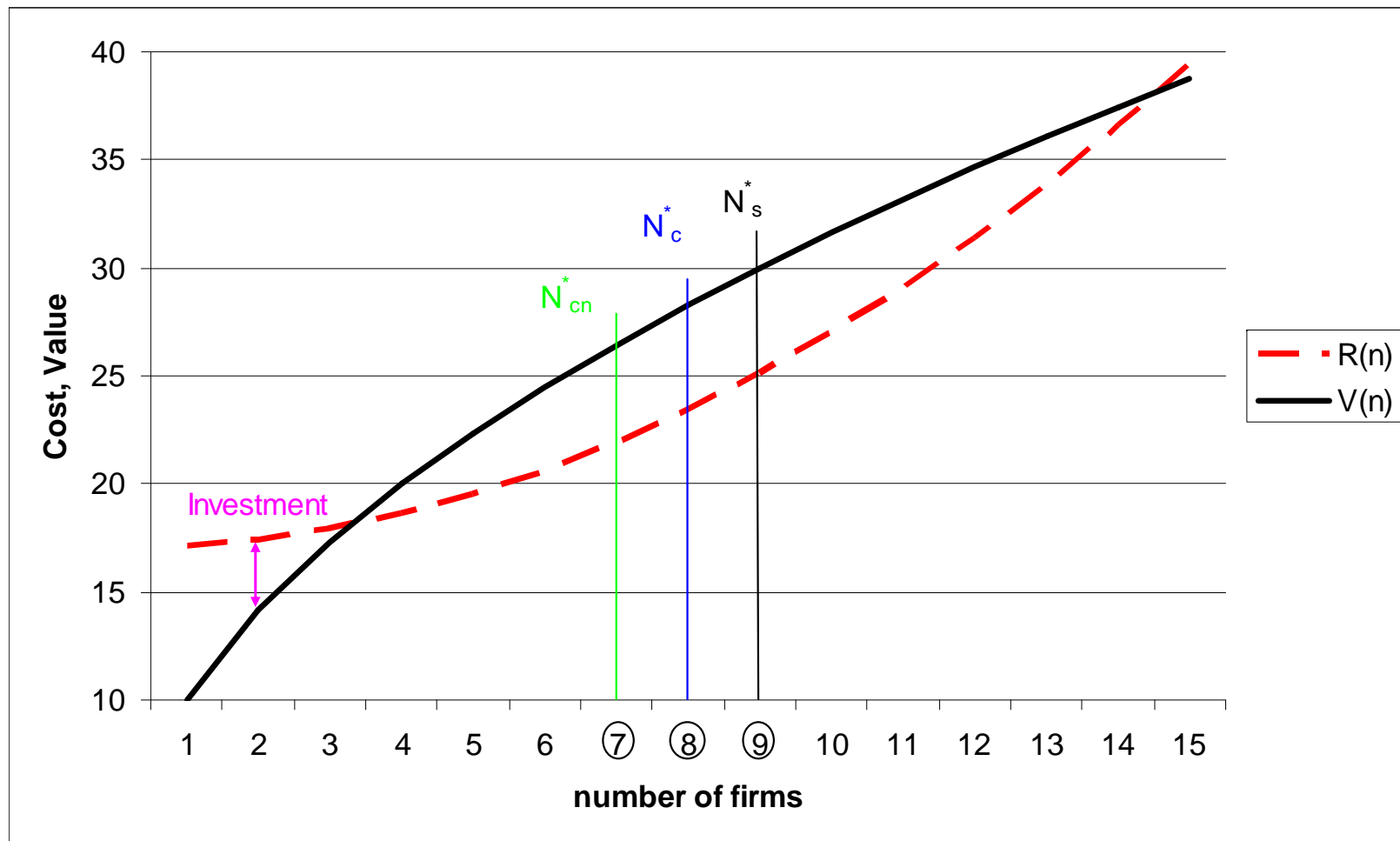
Link =  $V(N)$

# Prototype Value Function

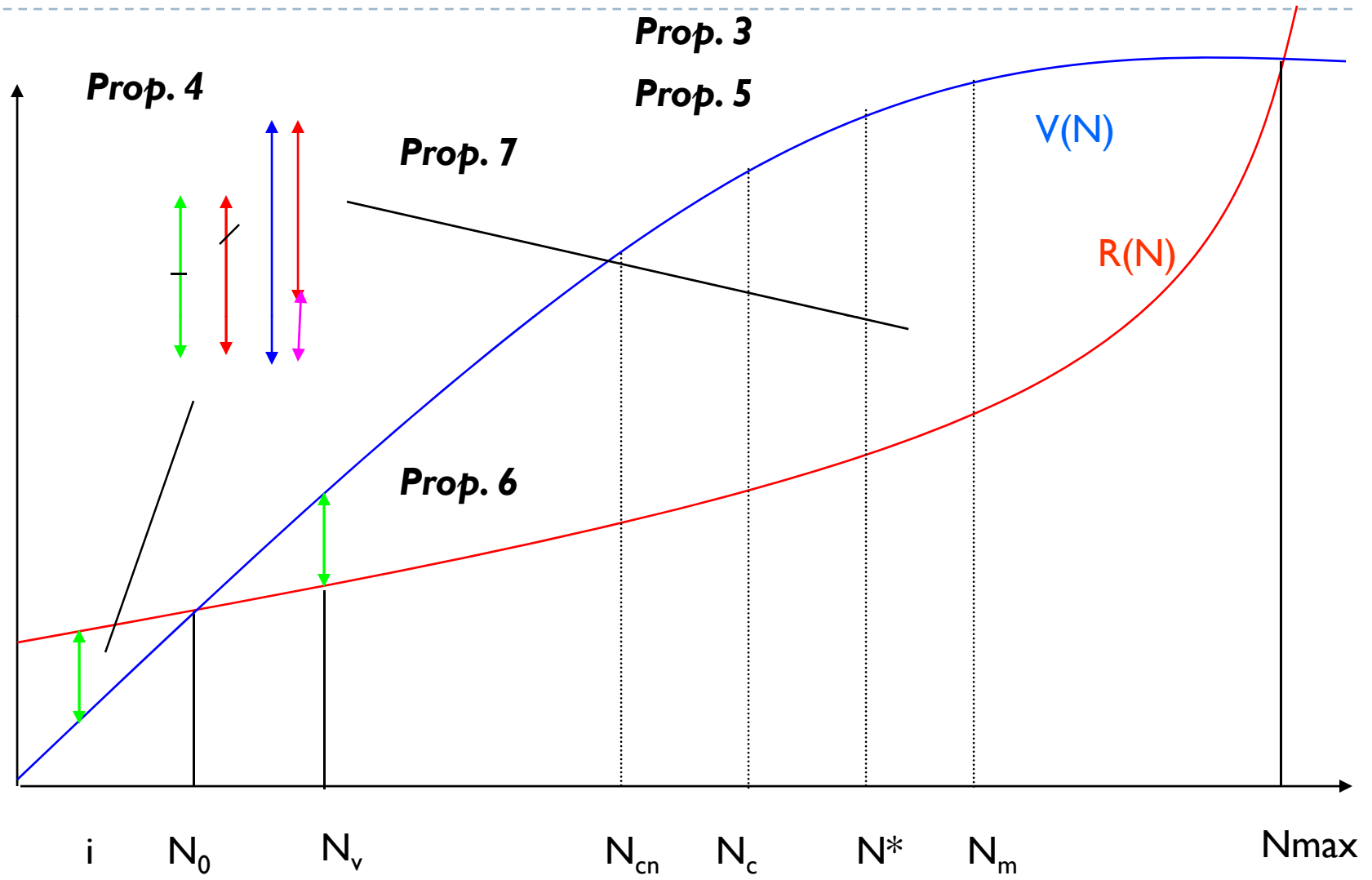
---



# Determining network size



# MSSP Results



[link](#)

# Conclusions

---

<b>MSSP Type\effects</b>	<b>Consortium MSSP</b>	<b>For-profit MSSP</b>
Effect of initial investment on network size	Initial investment may induce larger size; equal sharing is optimal	No effect
Maximum size	Not larger than net benefit maximizing	May be larger than net benefit maximizing
Viability	Minimum start-up size may be smaller than monopolist	Due to zero prices at start-up may require larger initial size



## Further reading

---

- ▶ <http://www.managedsecuritysource.com/benefits-of-managed-security.html>
- ▶ <http://weis07.infoseccon.net/papers/65.pdf>



# Economics of Compliance Incentives

## From the headlines

---

- ▶ 73% of mobile users said they are not always aware of security threats and best practices when working on the go. Although many said they are "sometimes" aware, another 28% admitted they "hardly ever" consider security risks and proper behavior. Some even said they "never" consider safety best practices and didn't know they needed to be aware of security risks.

<http://www.informationweek.com/showArticle.jhtml?articleID=201801429>

- ▶ 34% agree or strongly agree that survey participants perceive interference from existing security systems. When over one-third of the users perceive a problem, it is time to take notice.

<http://linkinghub.elsevier.com/retrieve/pii/S0167404806001532>

---



# Problem complexity

---

- ▶ Information security has direct costs for the agents, but often vague benefits
- ▶ Information security is not the main productive activity for most functional departments
- ▶ In case of the security failure at organizational level, an individual agent may or may not be affected
- ▶ Relationship between behavior and incidents is not clearly defined



# Literature

---

- ▶ **Choice of incentive structure**
  - ▶ environmental regulations - Sandmo 2002, Strand 1994;
  - ▶ experimental economics - Gatcher et al 2006, Fehr and Schmidt 1999
- ▶ **Policy enforcement in games**
  - ▶ repeated games with discounting – Friedman 1971
  - ▶ penal code – Abreu 1986, 1988
- ▶ **Fairness in games - Rabin 1991, Dufwenberg and Kirchsteiger 2004**



# The Model

---

- ▶ A game between *the user* and *the organization*
- ▶ If the user does not comply with security policies, incidents occur
- ▶ The organization may provide bonus, fine or both as compliance incentives
- ▶ **z** – organization's cost of protection and/or cleanup costs for an attack
- ▶ **c** – user's cost of compliance
- ▶ **d** – user's expected loss due to non-compliance
- ▶ **b** - amount of bonus
- ▶ **f** – amount of fine
- ▶ **d < c < (b,f) < z**



# Notation

---

- ▶ **z** – organization's cost of protection and/or cleanup costs for an attack
- ▶ **c** – user's cost of compliance
- ▶ **d** – user's expected loss due to non-compliance
- ▶ **b** - amount of bonus
- ▶ **f** – amount of fine
- ▶ **d < c < (b,f) < z**



## Payoff matrix (bonus and fine)

---

	Org.	Bonus	Fine
User			
Compliance		$+b-c; +z-b$	$-c-f; +z+f$
No Compliance		$+b-d; -z-b$	$-f-d; -z+f$

Nash equilibrium is (No Compliance, Fine)

---



## Solution: building trust

---

- ▶ Information security interactions rarely take place just once
- ▶ Payoffs of future period have less value today
  - ▶  $g$  ( $0 < g < 1$ ) represents today's value of 1 dollar tomorrow

**Conclusion: compliance with information security policies is easier to achieve if parties expect continued interactions in the future**

---



# Trust and incentive structures

---

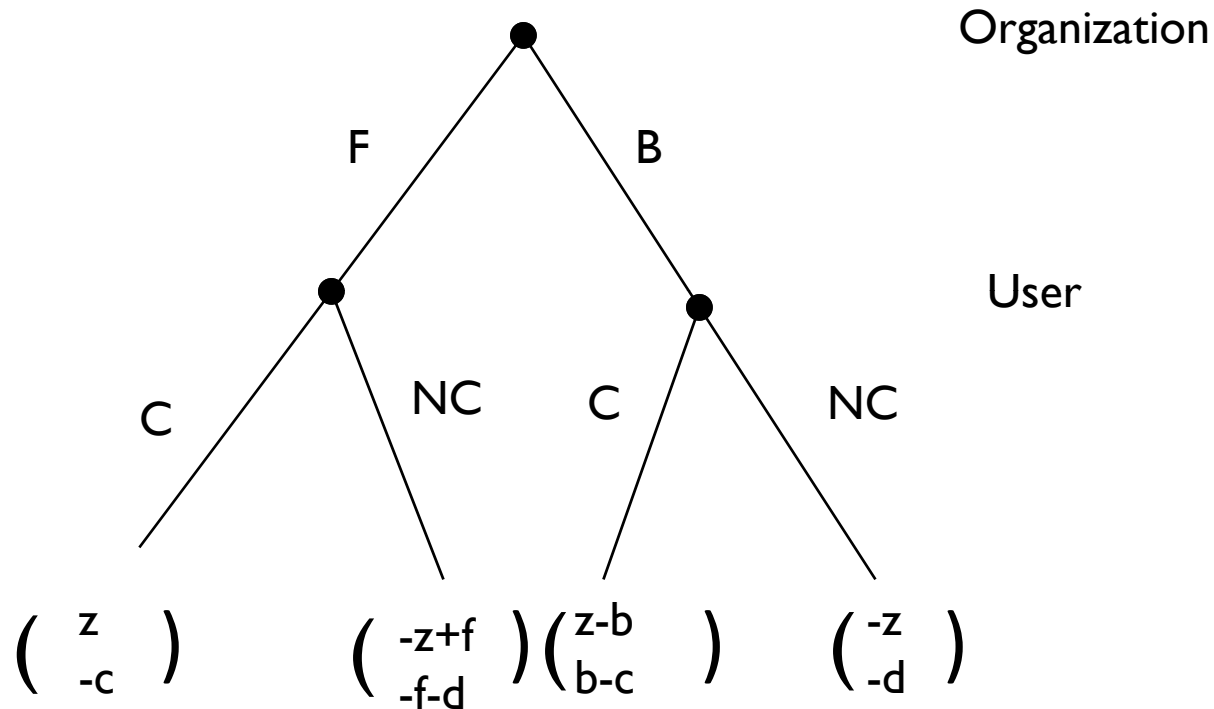
Incentive mechanism	Incentive range	Compliance – inducing value of $g$
Bonus only	$(c-d)/g < b < 2zg$	$1/\sqrt{2}$
Fine only	$(c-d)/g < f < 2zg$	$1/\sqrt{2}$
Bonus and fine	$(c-d)/2g < b=f < zg$	$1/\sqrt{2}$

- Compliance-inducing value of  $g$  is practically significant
  - Bonus and fine are interchangeable as incentives
  - Joint use of bonus and fine narrows the negotiation space
- 



# Pre-commitment to action

---



**Theorem. Compliance is possible if**

- 1)  $c-d < f$
- 2)  $c-d > f$ ,  $c-d < b$  and  $z > (f+b)/2$

---



# Penal code

---

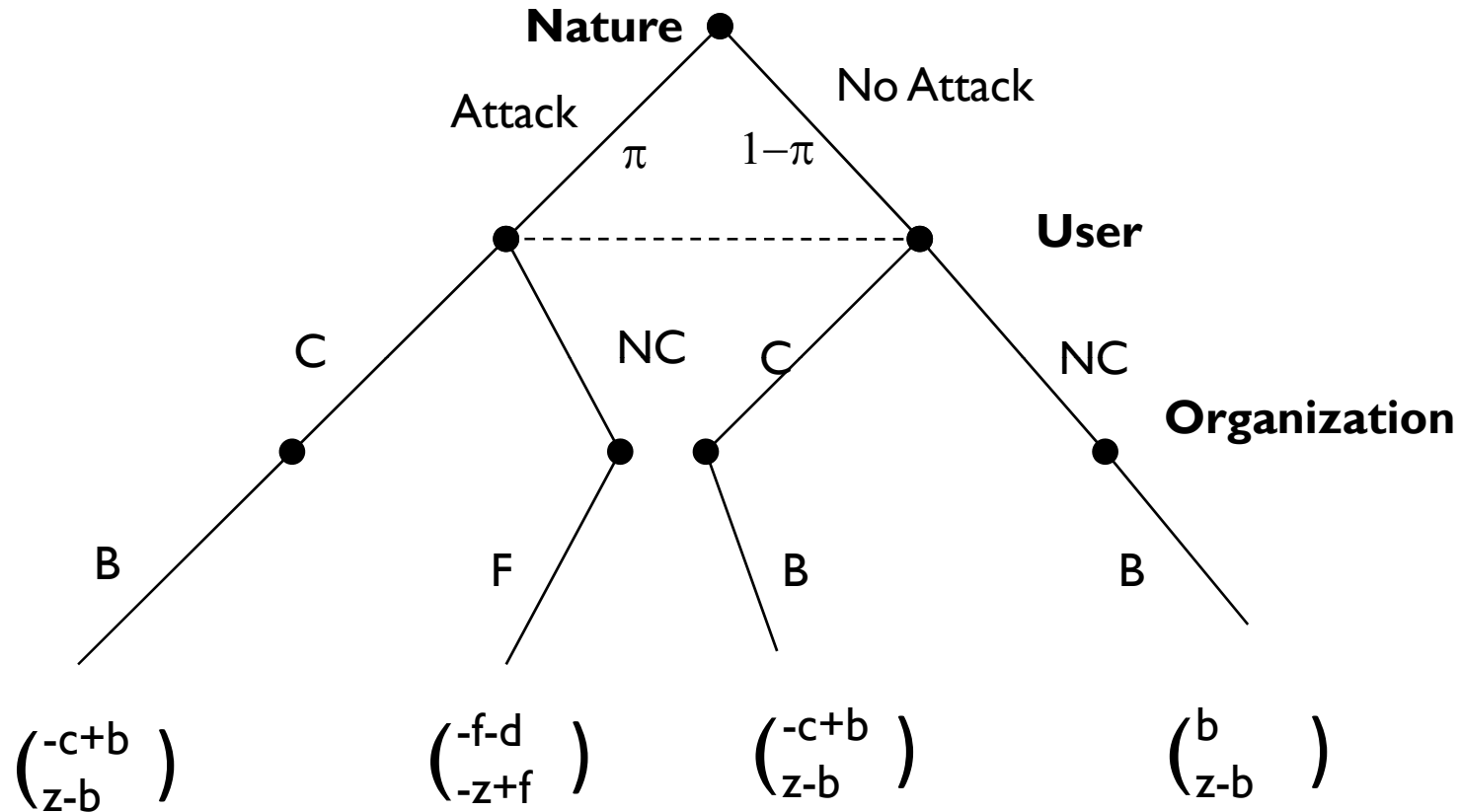
	Org.	Bonus	No Bonus
User			
Compliance		$+b-c$ ; $+z-b$	$-c$ ; $+z$
No Compliance		$+b-d$ ; $-z-b$	$-d$ ; $-z$

**Theorem: For the specified penal code, compliance is enforced if  $b > (c-d)/g$**

---



# Unobservable compliance



**Theorem.** When compliance is not directly observed and attacks take place with probability  $\pi$ , then compliance possible if  $\pi > c / (f+b+d)$



# Fairness as incentive

---

- ▶ Fairness as reciprocity
  - ▶ I will treat you well if you do the same
- ▶ Introduces a psychological component to the material payoff
- ▶ Proven to exist in experimental settings; plausible approach to principal-agent analysis
- ▶ Allows to control the balance of bargaining power



# Kindness and fairness

---

- ▶ Kindness function:

$$f_j(a_i, b_j) \equiv \frac{\pi_i(b_j, a_i) - \pi_i^E(a_i)}{\pi_i^H(a_i) - \pi_i^{\min}(a_i)}$$

- ▶ Fairness-based utility

$$U_i = \pi_i(a_i, a_j) + \alpha_i \beta_i \pi_j(a_i, a_j), \text{ where}$$

$\pi_i(a_i, a_j)$  - player  $i$ 's material payoff

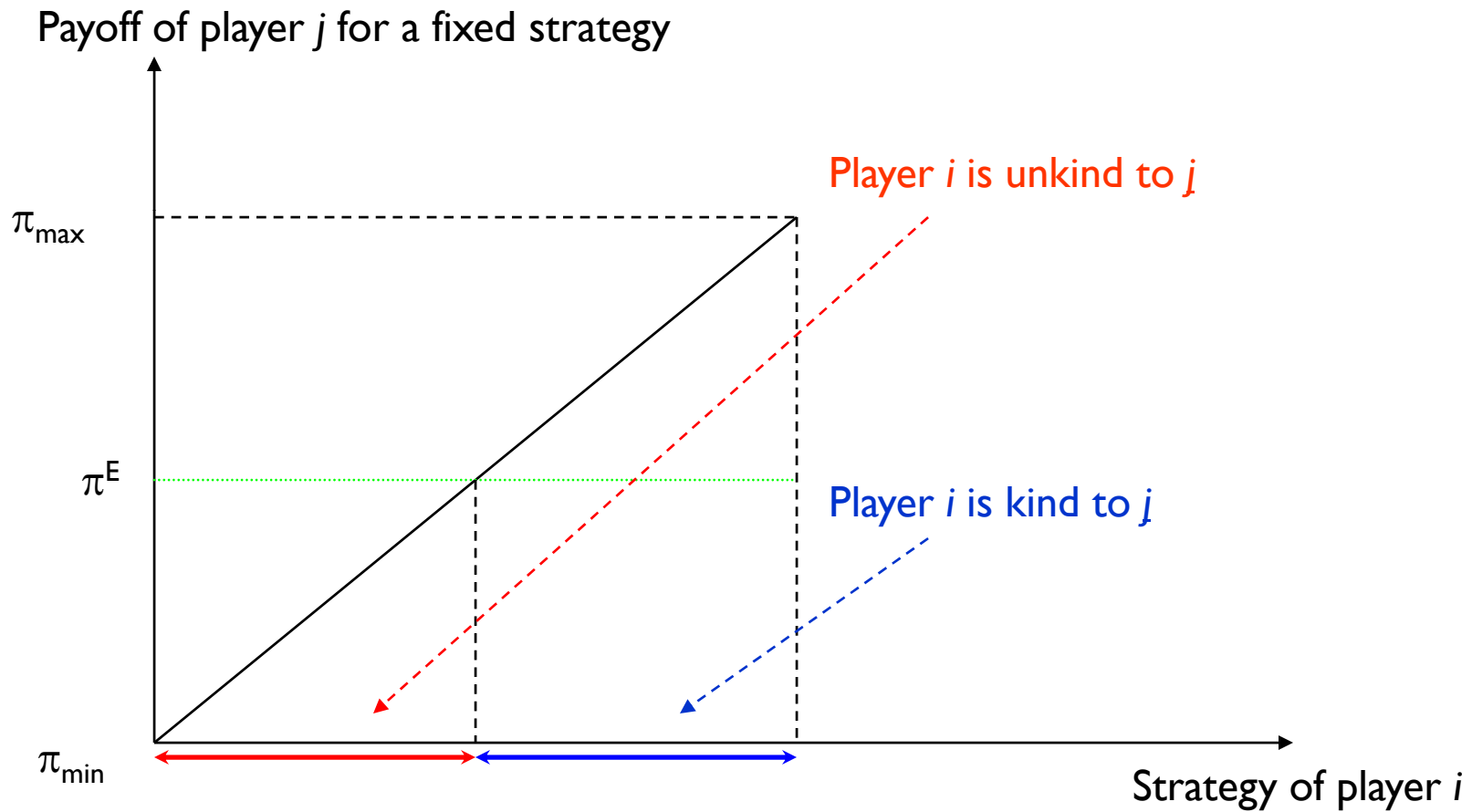
$\alpha_i$  - kindness of the opponent to player  $i$

$\beta_i$  - player  $i$ 's degree of concern for the opponent



# Fairness explained

---



---

**Table 1. Characteristic payoffs for the organization**

Strategy	$\pi_o^H$	$\pi_o^L = \pi_o^{min}$	$\pi_o^E = (\pi_o^H + \pi_o^L)/2$
Bonus	$z-b$	$-z-b$	$-b$
No bonus	$z$	$-z$	$0$

**Table 2. Characteristic payoffs for the user**

Strategy	$\pi_u^H$	$\pi_u^L = \pi_u^{min}$	$\pi_u^E = (\pi_u^H + \pi_u^L)/2$
No compliance	$b$	$0$	$b/2$
Compliance	$b-c$	$-c$	$b/2-c$

---



# Fairness results

---

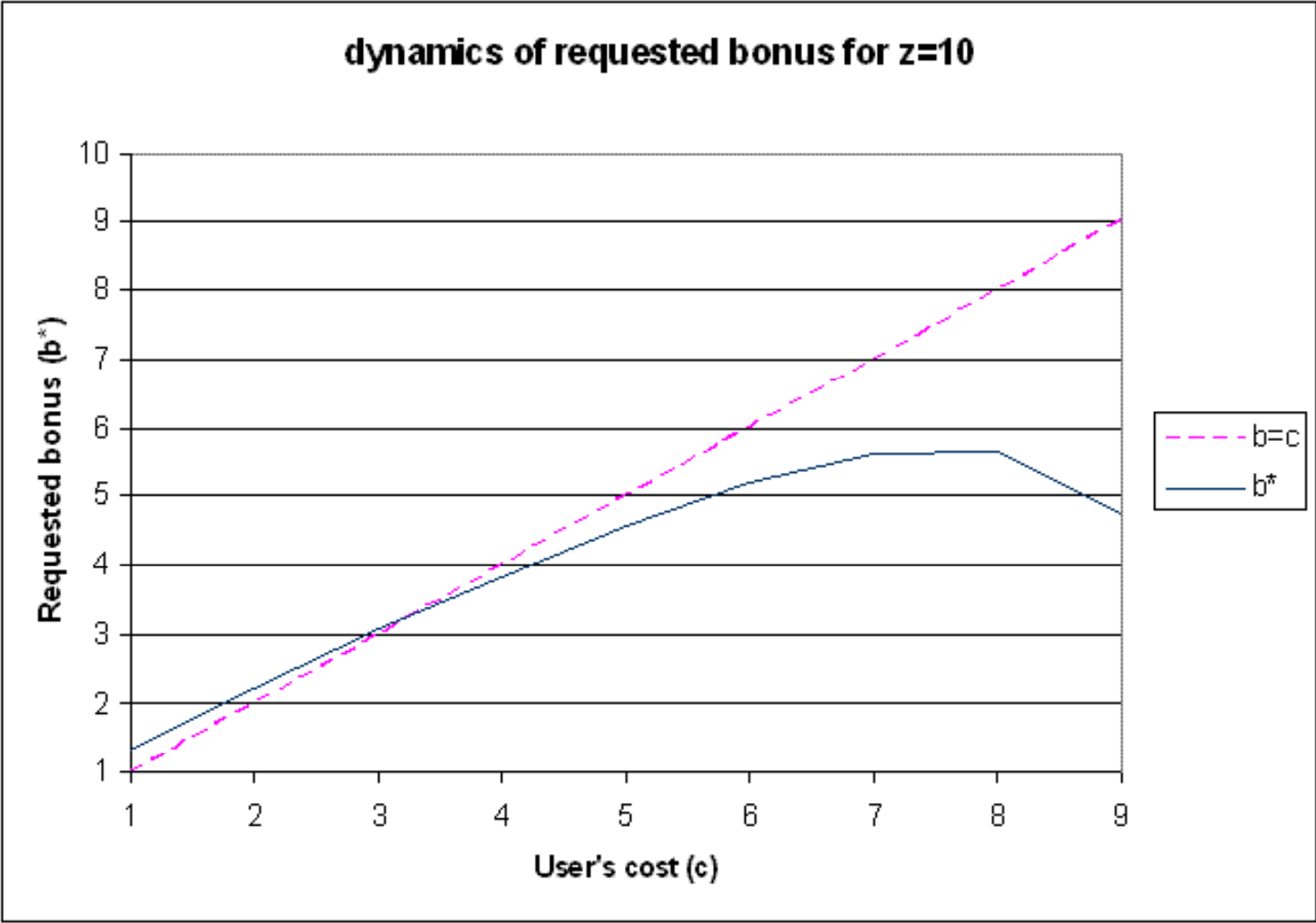
- ▶ In a simultaneous move game, compliance is a fairness equilibrium if  $\beta_o > 1$  and  $\beta_u > c/(2z)$ .

If bonus is negotiable and user's loss due to non-compliance is zero, fair bonus amount is

$$b^* = \max\left(c; \frac{z - c + 2zc - 2c^2}{2(z - c + 1)}\right) = \begin{cases} c : c \geq z/3 \\ \frac{z - c + 2zc - 2c^2}{2(z - c + 1)} : c < z/3 \end{cases}$$



dynamics of requested bonus for z=10



# Conclusions

---

- ▶ Building trust is important
- ▶ Combination of costs and benefits define the appropriate level of incentives
- ▶ Fairness considerations lead to compliance even in single-period games



# Issues in Measurement and Policies for IS Security

# The Problem

---

- ▶ There is no universal method to identify information security policies (Diver 2007)
- ▶ However, each information security policy must be specific, realistic and measurable
- ▶ Comprehensiveness and technical complexity of policies must be balanced with ease of understanding and presentation



# Metagraphs and other graphs

---

- ▶ Metagraphs (Basu and Blanning 2007) are graphical formalisms that include directed set-to-set mappings. They also allow the use of quantitative and qualitative attributes on the edges
- ▶ **Alternative structures include**
  - ▶ Directed graphs
  - ▶ Petri Nets (Peterson 1977)
  - ▶ Higraphs (Paige 1995)
  - ▶ Hypergraphs (Gallo et al. 1990)



# Metagraph Formalisms

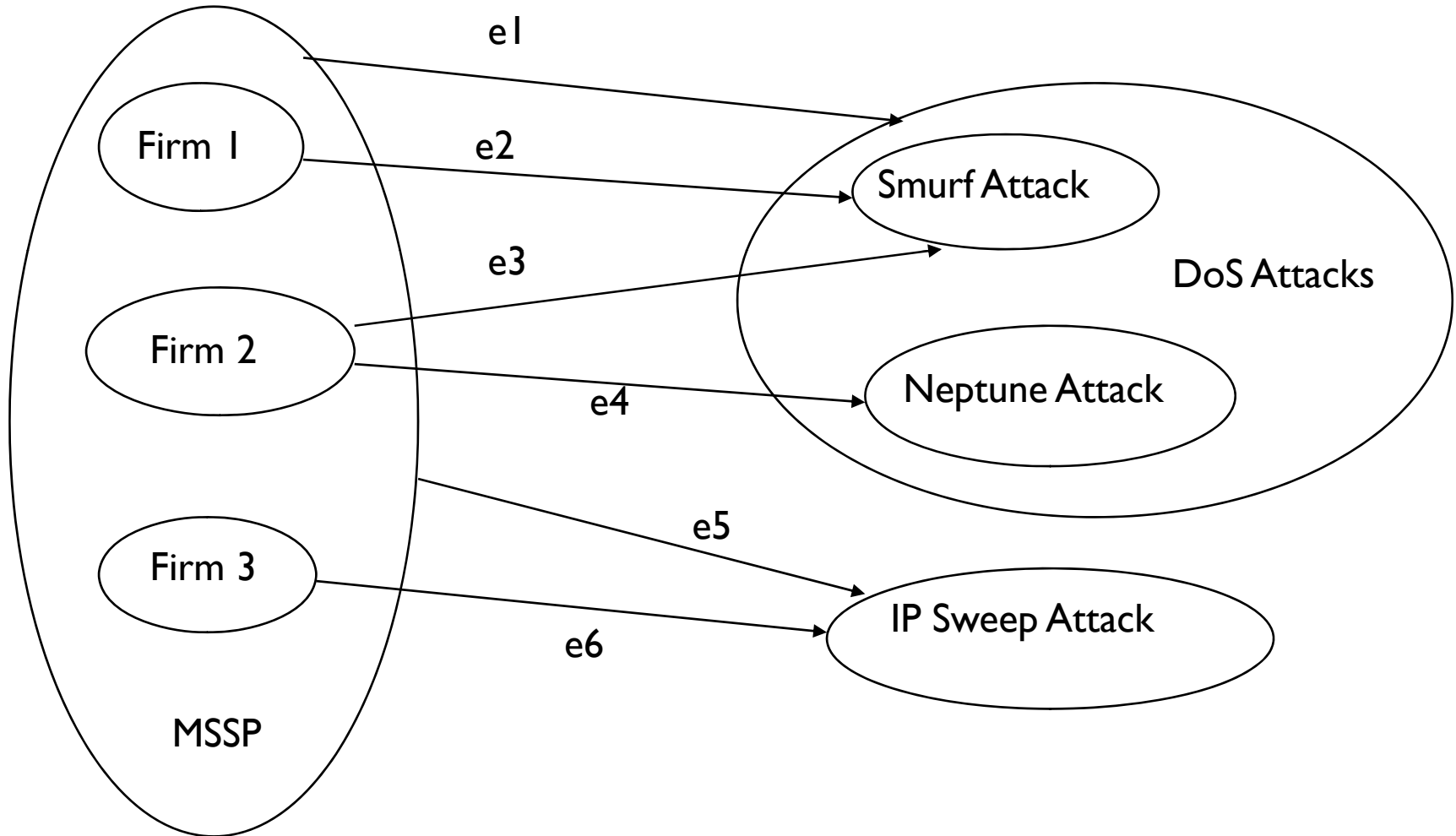
---

- ▶ *Generating Set  $X$*  included elementary nodes of the metagraph
- ▶ Each vertex  $v$  is a subset of  $X$
- ▶ Each directed edge  $e$  connects two vertices (invertex and outvertex)
- ▶ If a vertex includes more than one elementary node, such nodes are called co-inputs (co-outputs)
- ▶ Metagraph may be represented in the form of either *adjacency or incidence matrix*



# Example metagraph

---



# Dataset description

---

- ▶ Intrusion detection dataset used for KDD Cup 1999.
- ▶ Over 4 million records
- ▶ 42 attributes for each record
- ▶ 22 types of attacks in four attack classes, as well as normal traffic



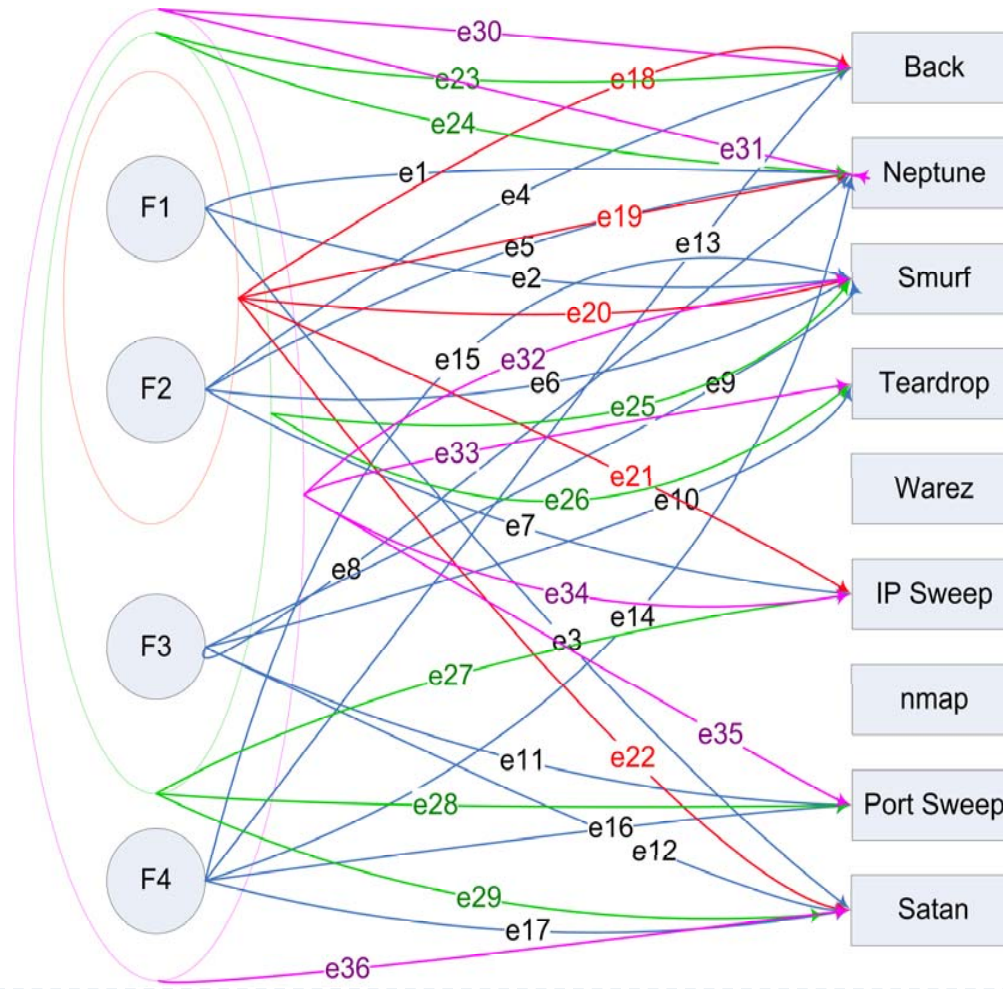
# Simulation procedure

---

- ▶ 20,000 connections randomly sampled
- ▶ Network grows from 1 to 20
- ▶ C4.5 decision tree algorithm
- ▶ Each network tested on the set of connections from the same distribution
- ▶ Individual performance as well as overall performance is recorded

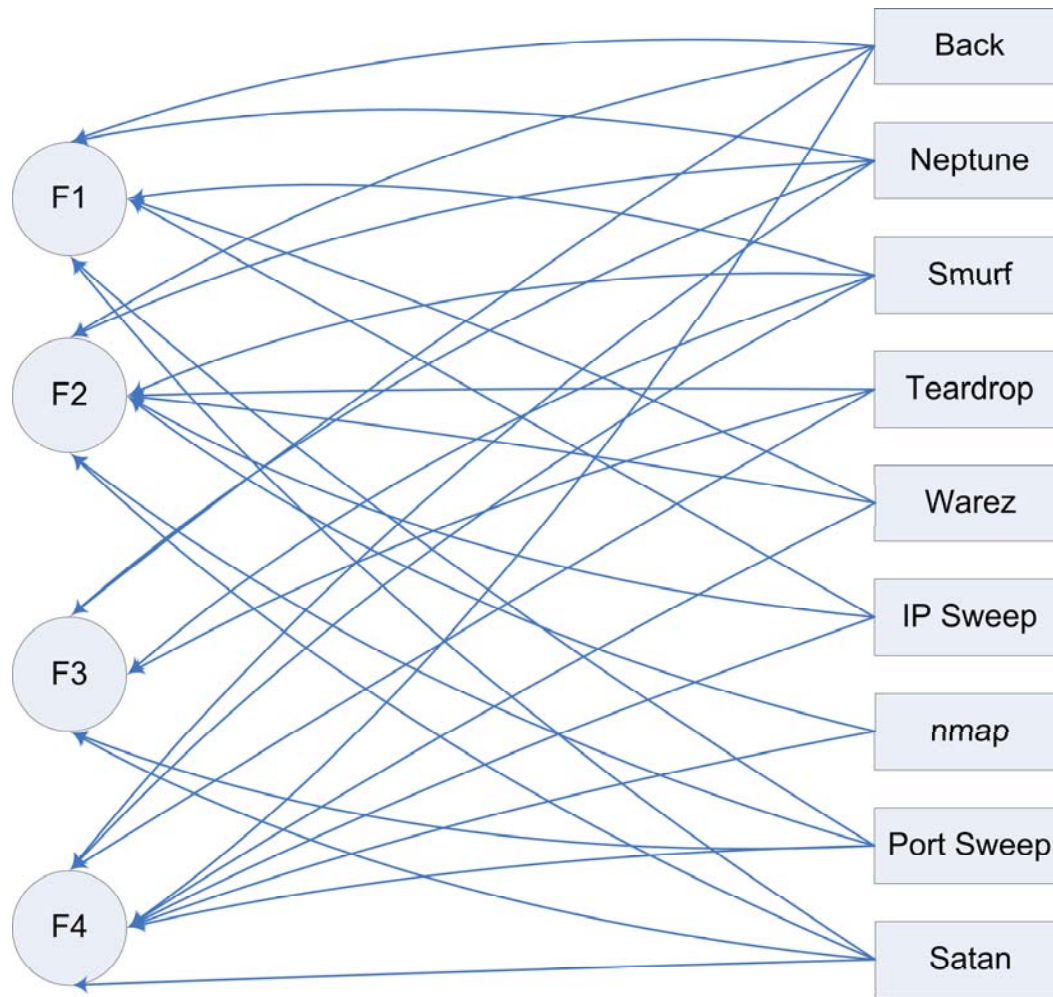


# Detection metagraph



# Exposure metagraph

---



# Gap Analysis

---

- ▶ *Detection-Exposure Gap* is present when there are attacks which are not correctly detected
- ▶ It can be formally extracted from the analysis of adjacency matrices of metagraphs
- ▶ **Policy rules:**
  - ▶ If gap is present, invest in non-technical prevention solutions
  - ▶ If gap is present, seek partnerships
  - ▶ If gap is absent, maintain the system state



# Identification of critical resources

---

- ▶ Identify dominant metapaths from resources to attacks and enumerate co-inputs in these metapaths
- ▶ Policy rules:
  - ▶ If co-inputs are always present, seek more expertise
  - ▶ A resource is critical if it is included in all cuts as a co-input, or on a single edge with no other co-inputs. Extra care is needed to protect this resource



# Forward integration

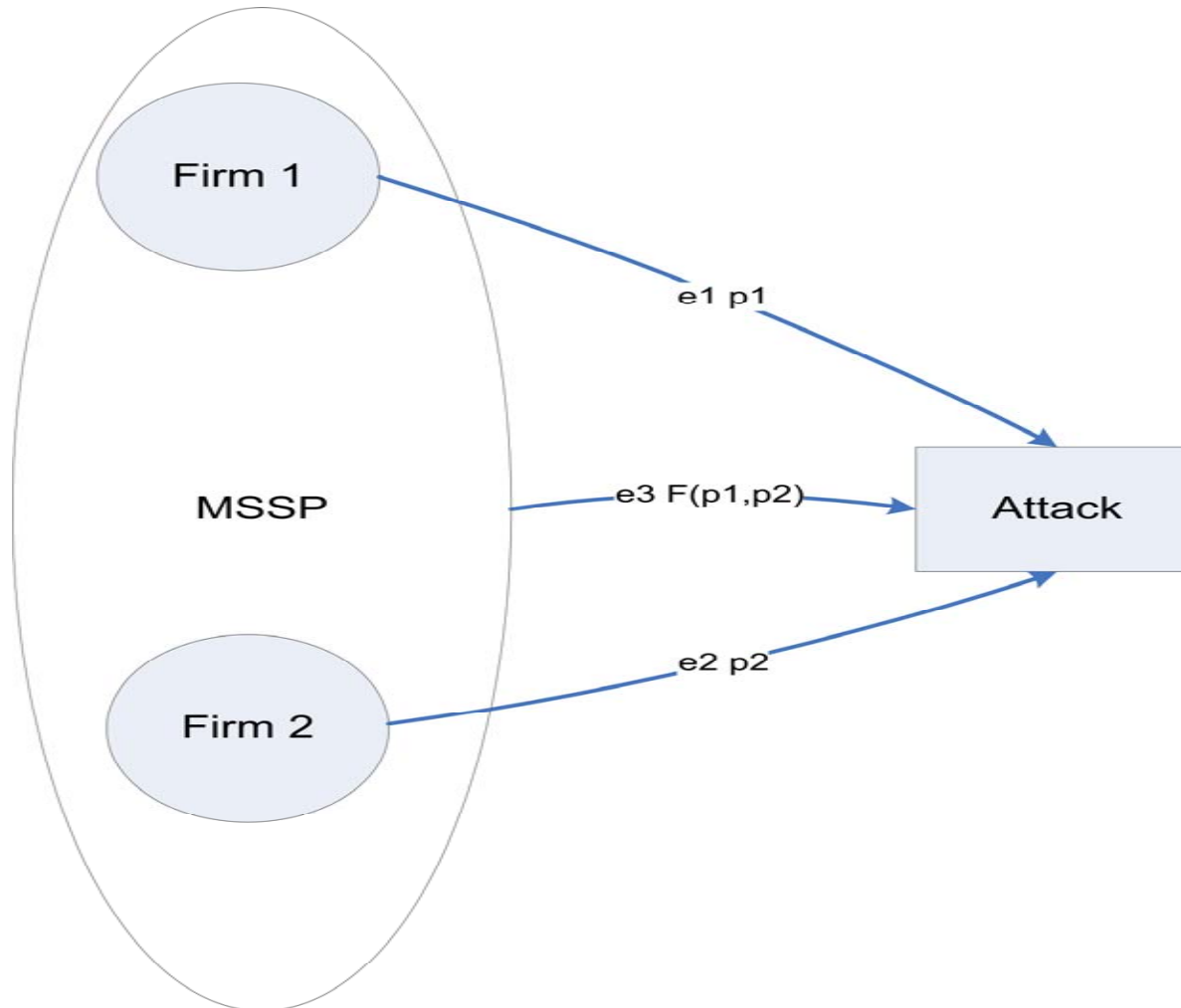
---

- ▶ Sometimes it is necessary to estimate the effect of multiple resources on the system state
- ▶ Can be achieved using quantitative attributes and *reallocation function*
- ▶ For information security, three types of such functions are plausible (Varian 2004):
  - ▶ Total effort
  - ▶ Weakest link
  - ▶ Best shot



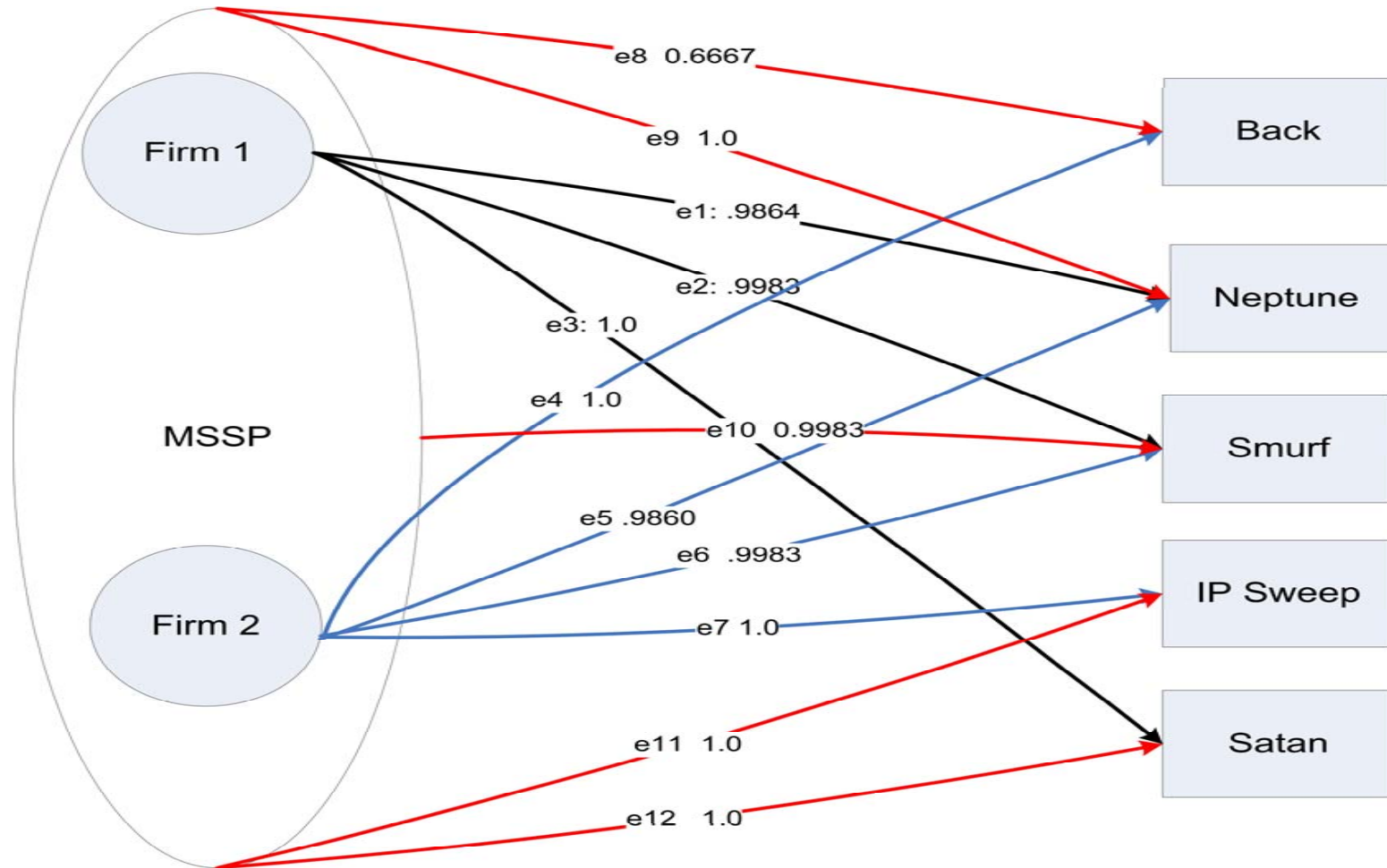
# Forward integration

---



# Reallocation function analysis

---



# Policy recommendations

---

- ▶ If the attributed metagraph indicates that both partners have less than perfect detection capability for a particular attack, they should pool their efforts.
- ▶ The partner with superior detection capability for a particular attack should be responsible for the detection of that attack.
- ▶ In the process of network integration, detection rules generated by individual partners should not be discarded without examination. It is possible that such individual rules are superior to joint rules, and should be retained instead.



# Conclusions

---

- ▶ Metagraphs are appropriate and valuable tools for policy analysis as they combine the visual display properties with formal algebraic structure allowing a wide range of data manipulations
- ▶ Metagraphs may be customized for information security analysis using the definition of balanced system as well as detection-exposure gap
- ▶ Quantitative attributes of metagraphs may be used to analyze alternative approaches to system integration in information security





# Resources

## Resources on the subject

---

- ▶ Workshop on the Economics of Information Security (WEIS): <http://weis09.infosecon.net/>
  - ▶ Includes links to papers from past workshops
- ▶ Economics of Privacy: <http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm>
- ▶ Bruce Schneier on Security: <http://www.schneier.com/blog/>
  
- ▶ Contact me:
- ▶ [Dmitry.Zhdanov@uconn.edu](mailto:Dmitry.Zhdanov@uconn.edu)
- ▶ Phone (860) 486-1578



---

**THANK YOU!**

