Managing the Weakest Link: A Game-Theoretic Approach for the Mitigation of Insider Threats

Aron Laszka [1,2] Benjamin Johnson [3] Pascal Schöttle [4]
Jens Grossklags [1] Rainer Böhme [4]

[1]Pennsylvania State University

[2]Budapest University of Technology and Economics

[3]University of California, Berkeley

[4]University of Münster

Motivation - Cyber-espionage

Will the new device be a phone or not?

Motivation - Cyber-espionage

Will interest rates change or not?

Motivation - Cyber-espionage

Respond to a cyber-attack with conventional warfare?

Motivation - Cyber-espionage

- What is published
  - FBI "estimates that every year billions of U.S. dollars are lost to foreign and domestic competitors who deliberately target economic intelligence in flourishing U.S. industries and technologies" [4]
  - a 2012 report identifies the loss for the German industry caused by industrial espionage to be around 4.2 billion € [2]
  - US and one particular foreign nation in the last four years: "nearly 100 individual or corporate defendants have been charged by the Justice Department with stealing trade secrets or classified information" [5]

Weakest Link: Insider Threats

- FBI: "A domestic or foreign business competitor ... may wish to place a spy into a company in order to gain access to non-public information. Alternatively, they may try to recruit an existing employee to do the same thing." [3]
- 2012 report on Germany: over 70% of losses were caused by members of their own organization [2]
- traditionally: access control

Weakest Link: Insider Threats

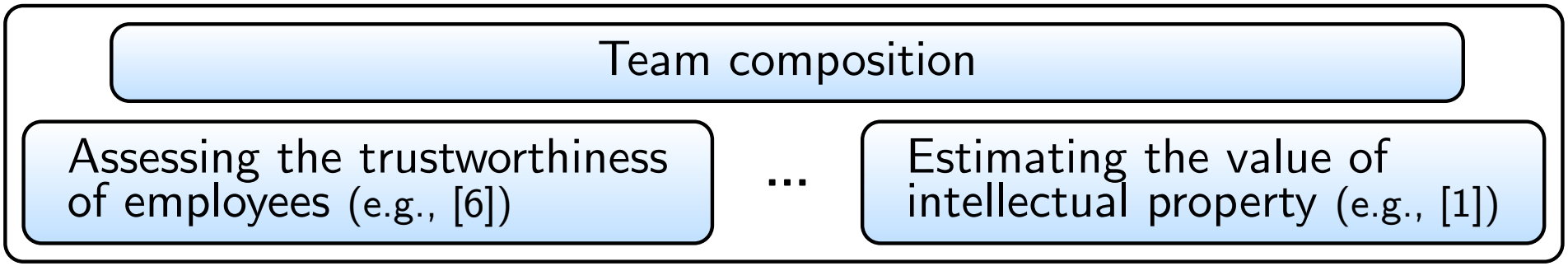
- FBI: "A domestic or foreign business competitor ... may wish to place a spy into a company in order to gain access to non-public information. Alternatively, they may try to recruit an existing employee to do the same thing." [3]
- 2012 report on Germany: over 70% of losses were caused by members of their own organization [2]
- traditionally: access control, but secrets have to be shared with some employees
  - CERT investigation of 23 attacks: "in 78% of the incidents, the insiders were authorized users with active computer accounts" [7]

How can we mitigate these risks?

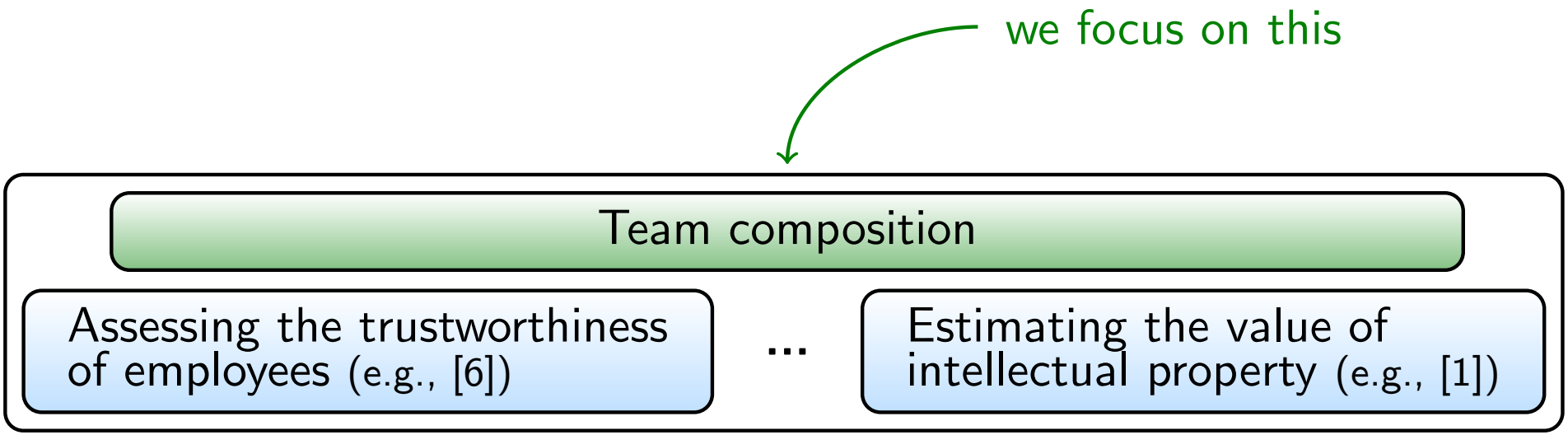
Managing Insider Threats

Managing insider threats

Managing Insider Threats



Managing Insider Threats



Model - Introduction

secret of value S

Model - Introduction

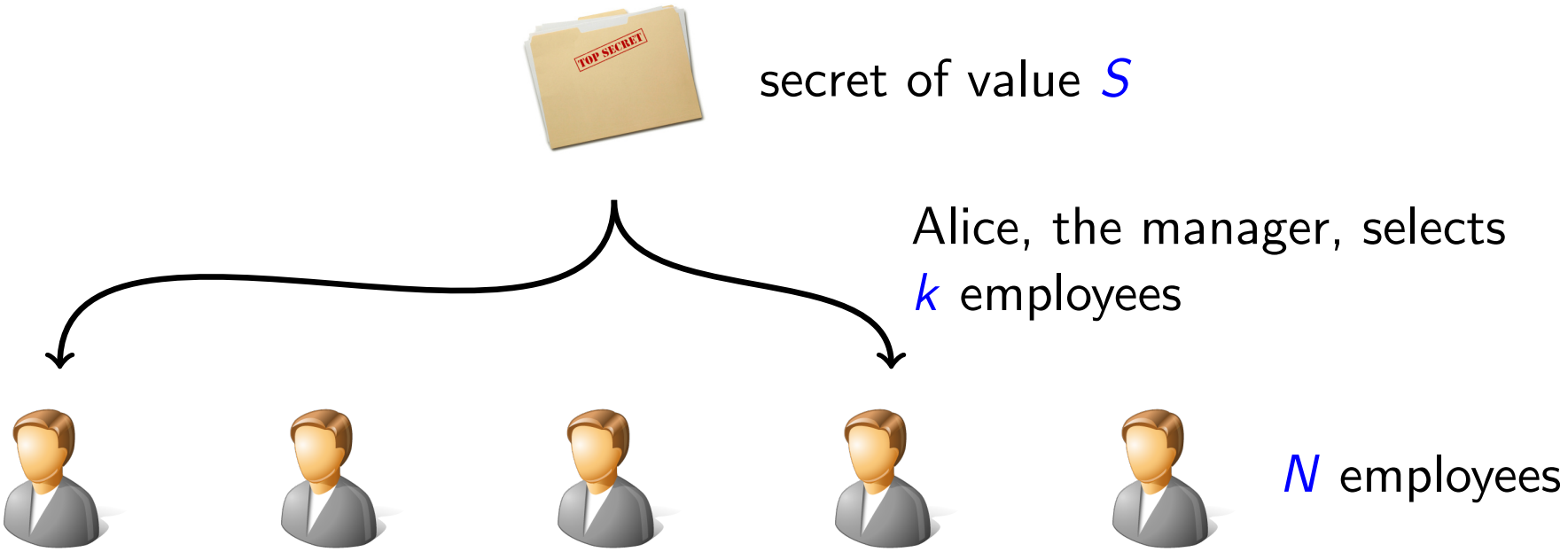
secret of value S





N employees

Model - Introduction



Model - Introduction

secret of value S

Alice, the manager, selects k employees

N employees

Eve, the adversary

Model - Introduction

secret of value S

Alice, the manager, selects k employees

N employees

targets an employee and tries to bribe her with a value of b

Eve, the adversary

Model - Introduction

secret of value S

Alice, the manager, selects k employees

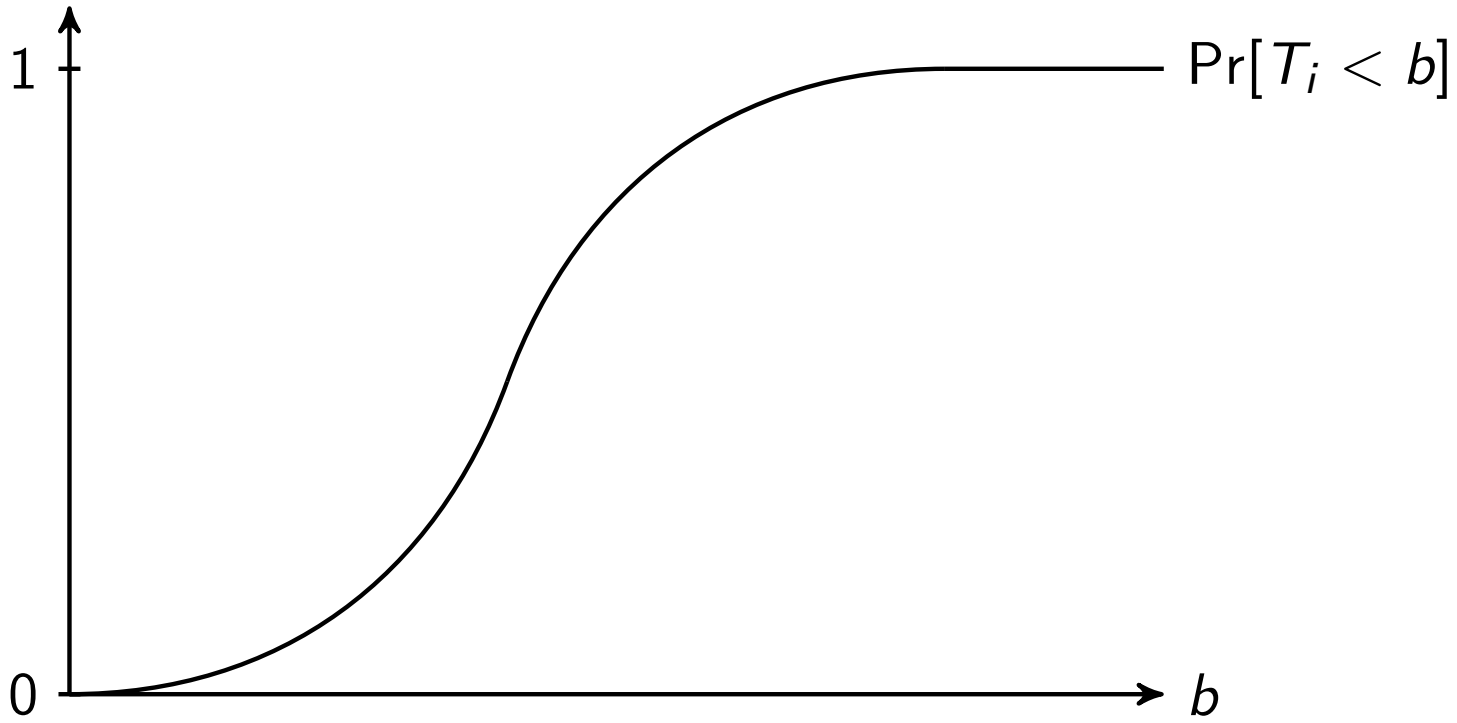
N employees

bribe value b has to be higher than the trustworthiness level T_i of the employee

Eve, the adversary

Trustworthiness Level Distributions

- the probability that the bribe is successful (given that the targeted employee actually knows the secret) is increasing in the bribe value
- we assume that both players can learn the trustworthiness level distributions



Model - Details

Game-theoretic model

- two-player, one-shot game
- Alice, the manager, selects a set I of k employees
  $\rightarrow$ her pure strategies are the k-subsets of N
- Eve, the adversary, targets an employee i and chooses a bribe value b
  $\rightarrow$ her pure strategies are (i, b) pairs
- when Alice selects set I and Eve chooses (i, b)
  - if $i \in I$ and $b \geq T_i$: Eve learns the secret and gains $S - b$, while Alice loses S
  - if $i \notin I$ or $b < T_i$: Eve does not learn the secret and loses b, while Alice does not lose anything
- information available to the players
  - both players know the employees' trustworthiness distributions
  - but they do not know the other players' strategic choice
- mixed strategies
  - Alice: probability a_i of sharing the secret with employee i

Naïve Ideas

- "Select the k most trustworthy employees."

Naïve Ideas

- "Select the k most trustworthy employees."
- "Eve will always target the employees who are the most likely to know the secret."

Naïve Ideas

- "Select the k most trustworthy employees."
- "Eve will always target the employees who are the most likely to know the secret."
- "If the secret has to be shared with more employees (i.e., if k is higher), it is never safer."

Naïve Ideas

- ~~"Select the k most trustworthy employees."~~
- "Eve will always target the employees who are the most likely to know the secret."
- "If the secret has to be shared with more employees (i.e., if k is higher), it is never safer."

THEY

Naïve Ideas

- ~~"Select the k most trustworthy employees."~~
- ~~"Eve will always target the employees who are the most likely to know the secret."~~
- "If the secret has to be shared with more employees (i.e., if k is higher), it is never safer."

THEY ARE ALL

Naïve Ideas

- ~~"Select the k most trustworthy employees."~~
- ~~"Eve will always target the employees who are the most likely to know the secret."~~
- ~~"If the secret has to be shared with more employees (i.e., if k is higher), it is never safer."~~

THEY ARE ALL WRONG!

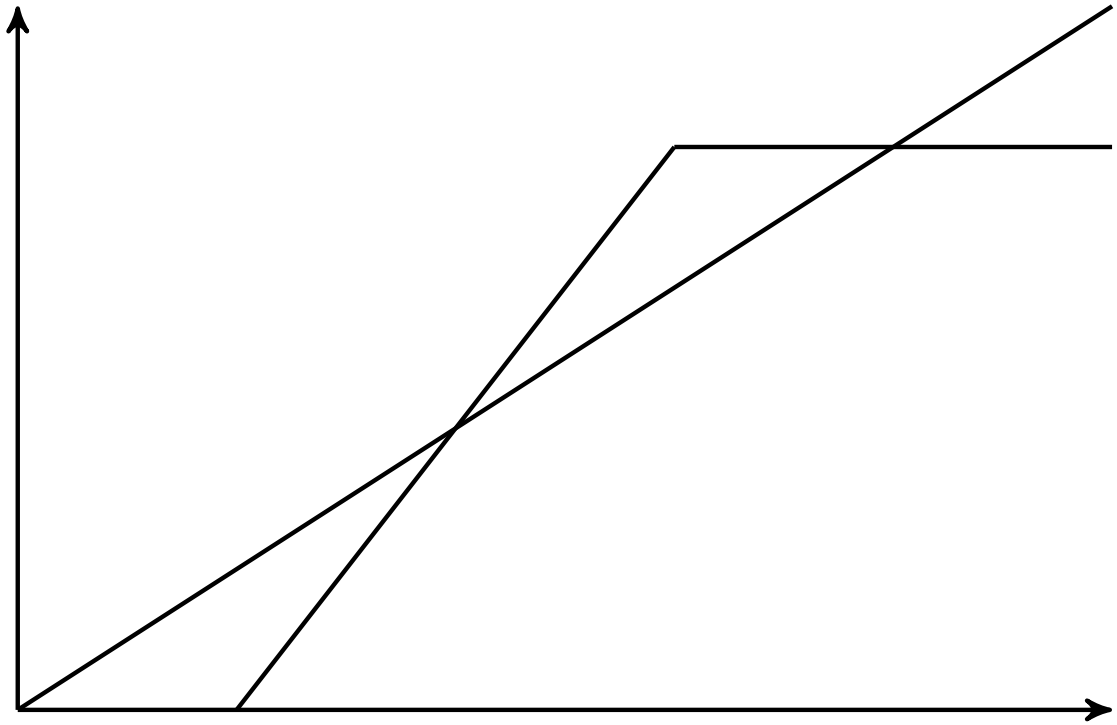
Game-Theoretic Analysis

Outline

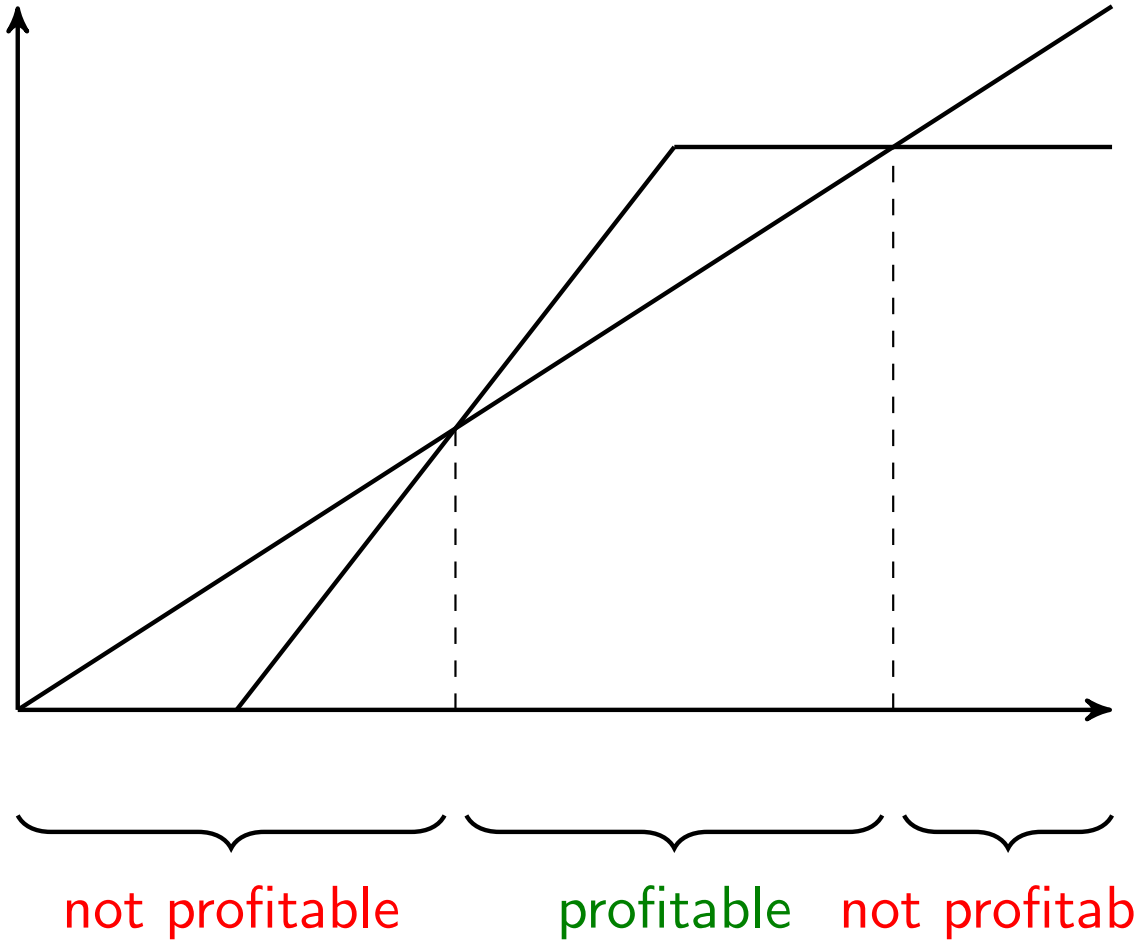
- Eve's expected gain from targeting a given employee
- theorems characterizing Alice's and Eve's equilibrium strategies

(For a more detailed and formal discussion, please see the paper.)

Eve's Gain from Targeting a Given Employee i

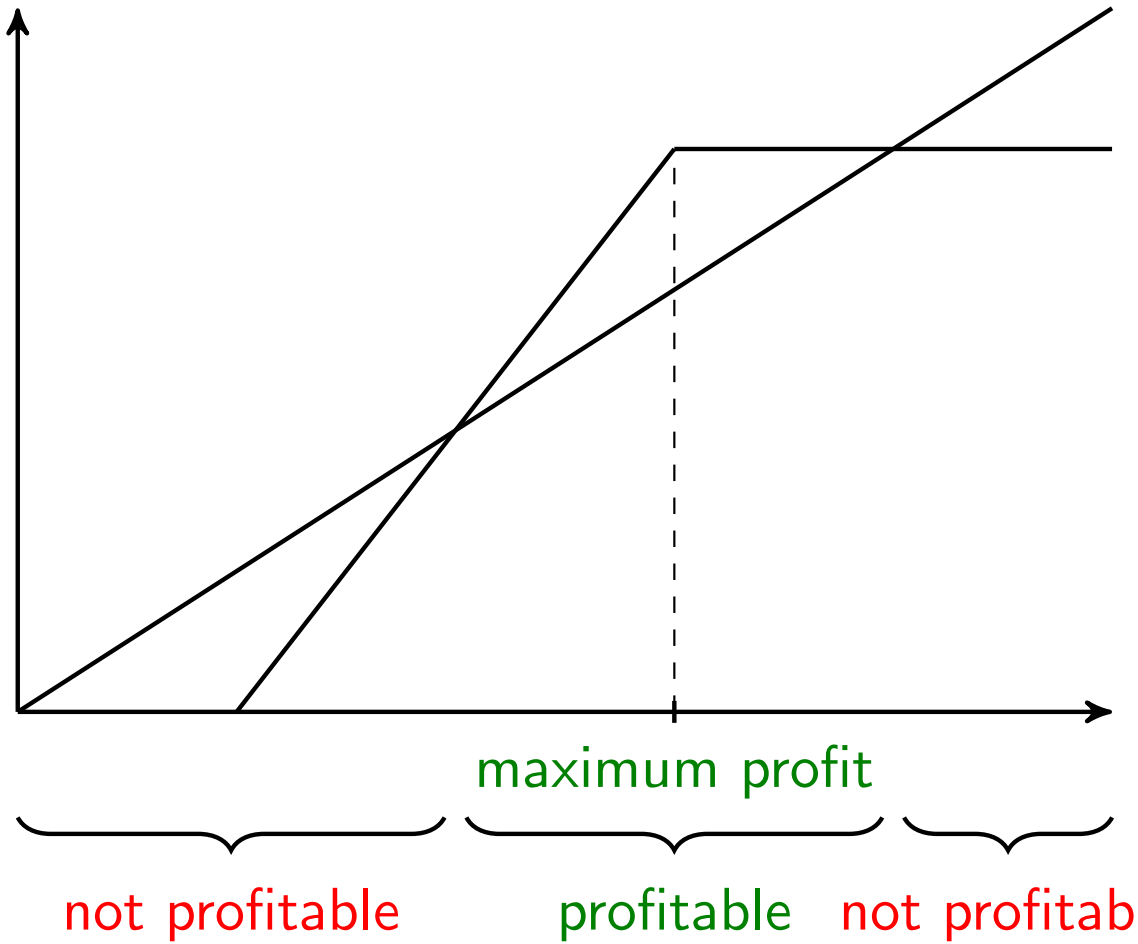


Eve's Gain from Targeting a Given Employee i

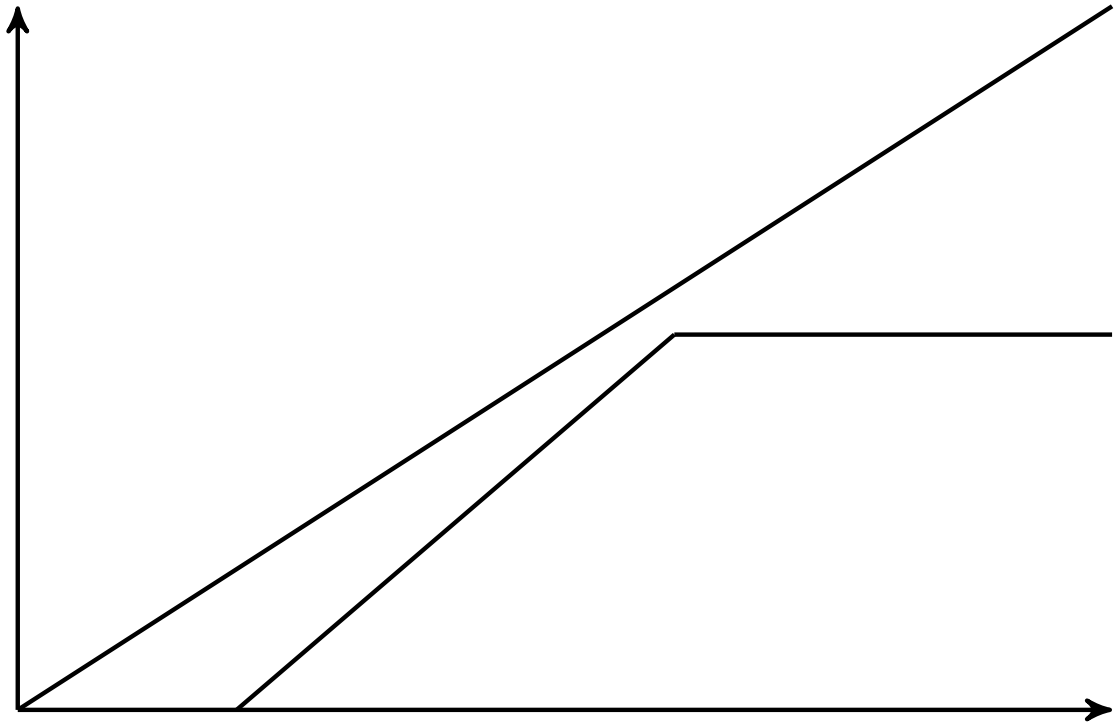


Eve's Gain from Targeting a Given Employee i

$$\text{MaxUE}(\mathcal{T}_i, a_i) > 0$$

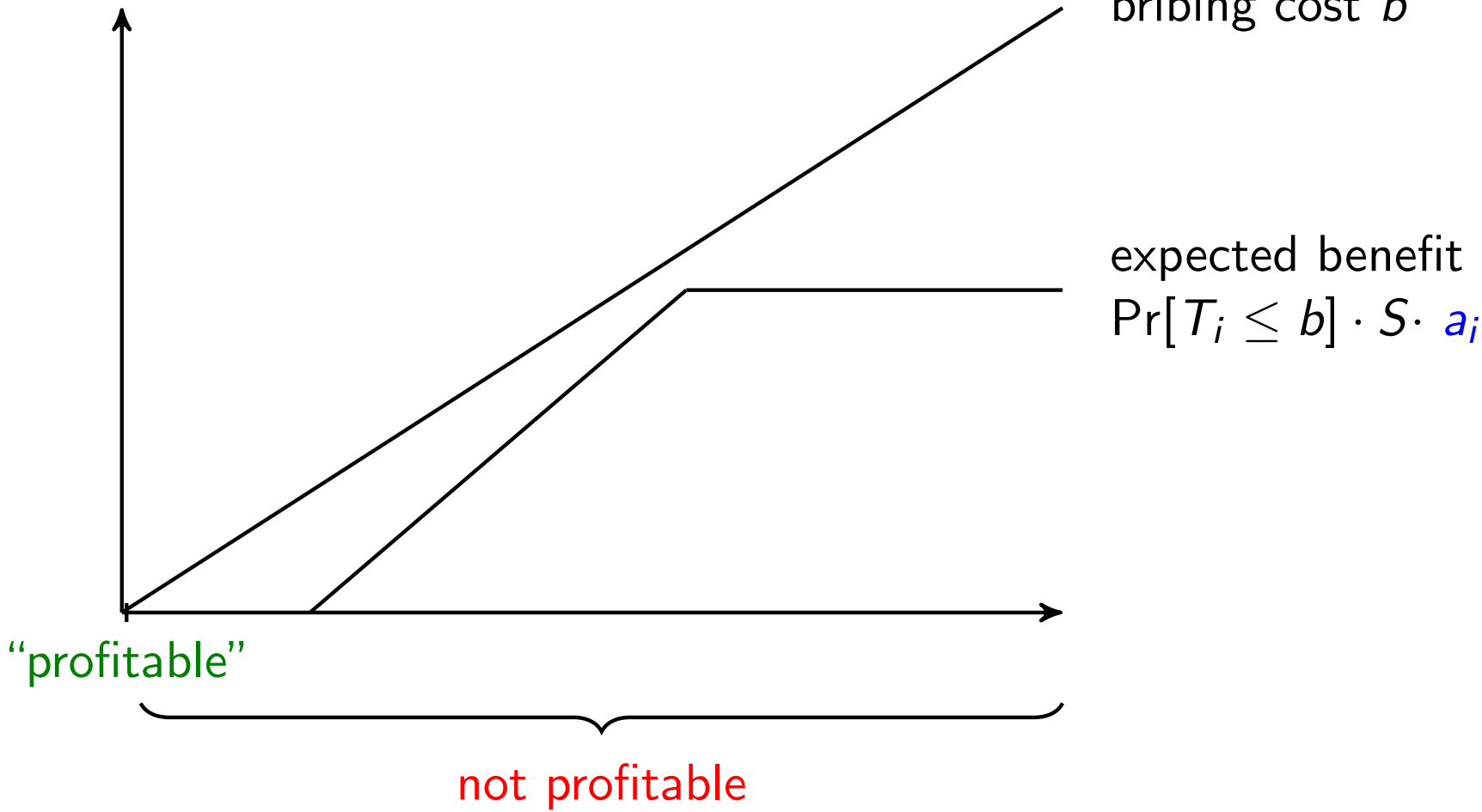


Eve's Gain from Targeting a Given Employee i



Eve's Gain from Targeting a Given Employee i

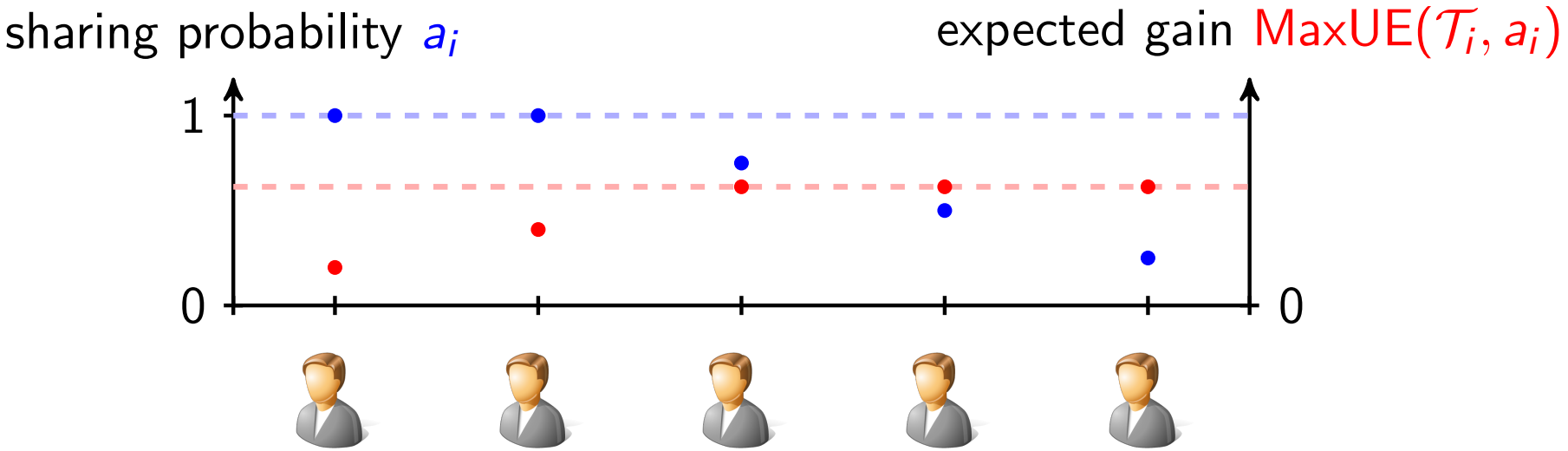
$$\text{MaxUE}(\mathcal{T}_i, a_i) = 0$$



Alice's Strategy in an Equilibrium

Theorem

- *Alice is either secure, that is, Eve has no strategy against her with a positive gain, or she shares the secret with every employee with non-zero probability.*
- *Over the set of employee with whom Alice does not certainly share the secret, Eve's expected gain is uniform. Furthermore, this expected gain is at least as much as the gain from any employee with whom Alice shares the secret certainly.*



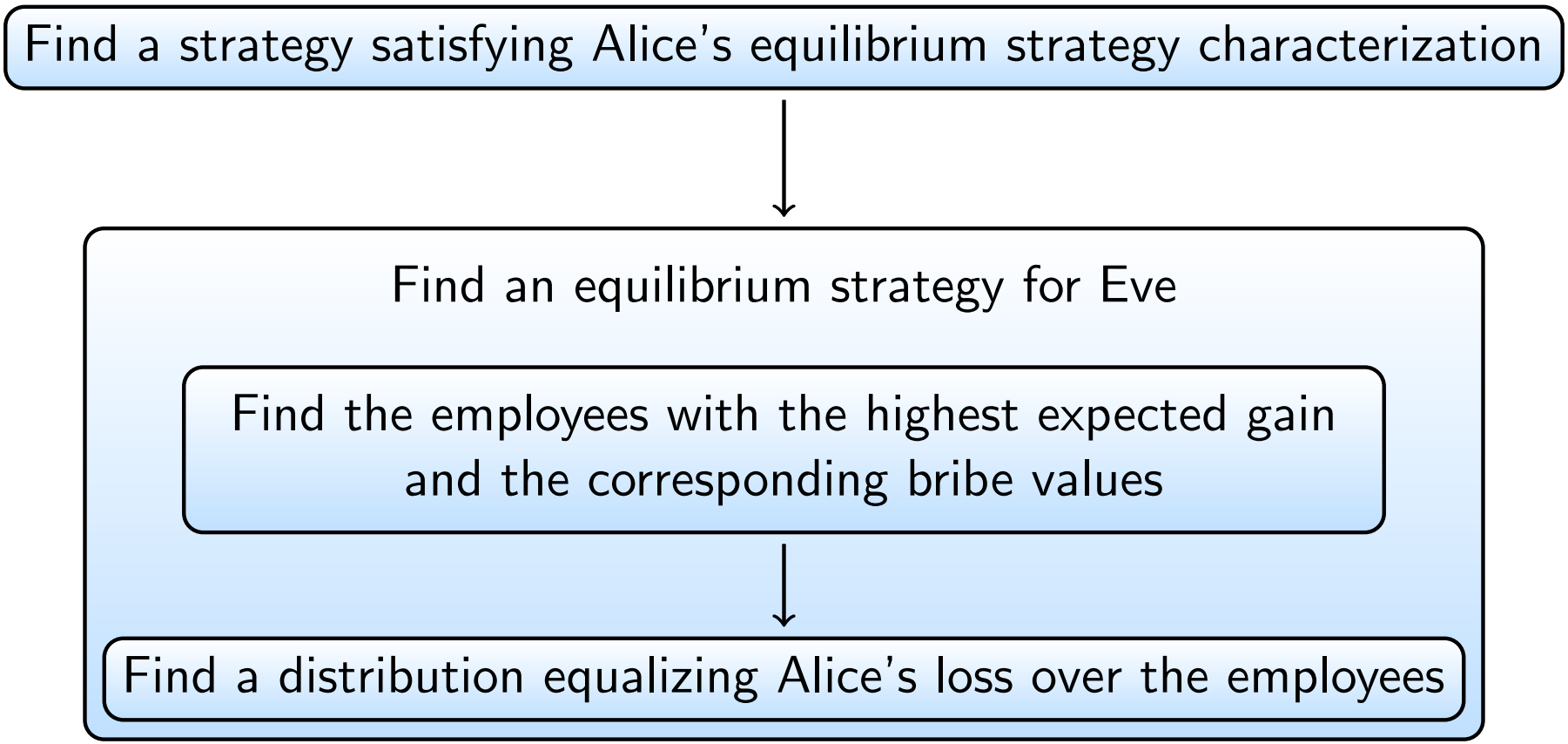
Eve's Strategy in an Equilibrium

Theorem

- *Over the set of employees with whom Alice does not certainly share the secret, the probability that Eve learns the secret from a given employee is uniform.*
- *The employees with whom Alice shares the secret with certainty are at most as likely to be targeted by Eve as the other employees, with whom Alice is less likely to share the secret.*

Computing an Equilibrium

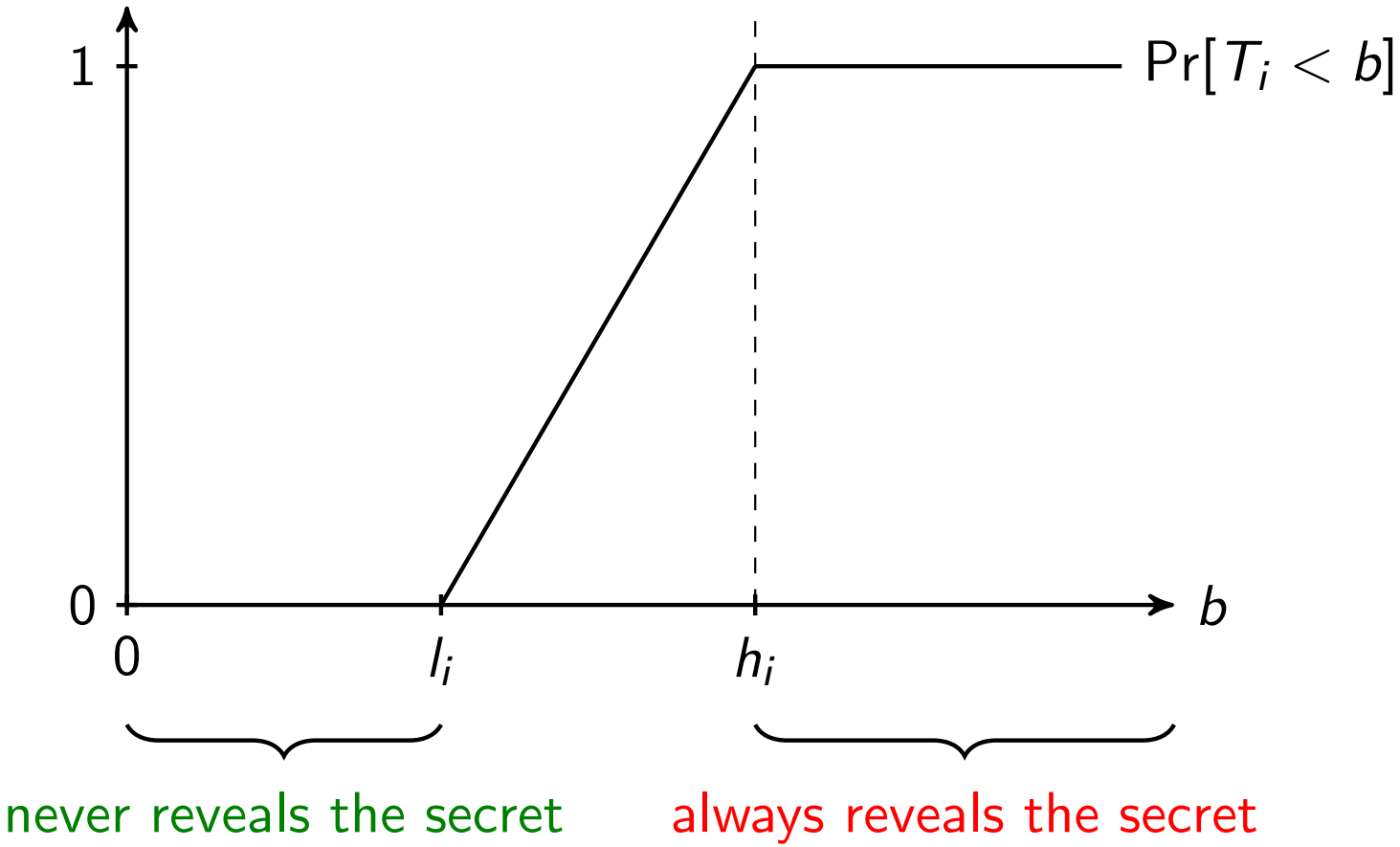
- Our characterizations of the players' equilibrium strategies are not only necessary but also sufficient



- "Find": any multidimensional numerical optimization method (e.g., the Nelder-Mead algorithm)

Uniform Trustworthiness Distributions

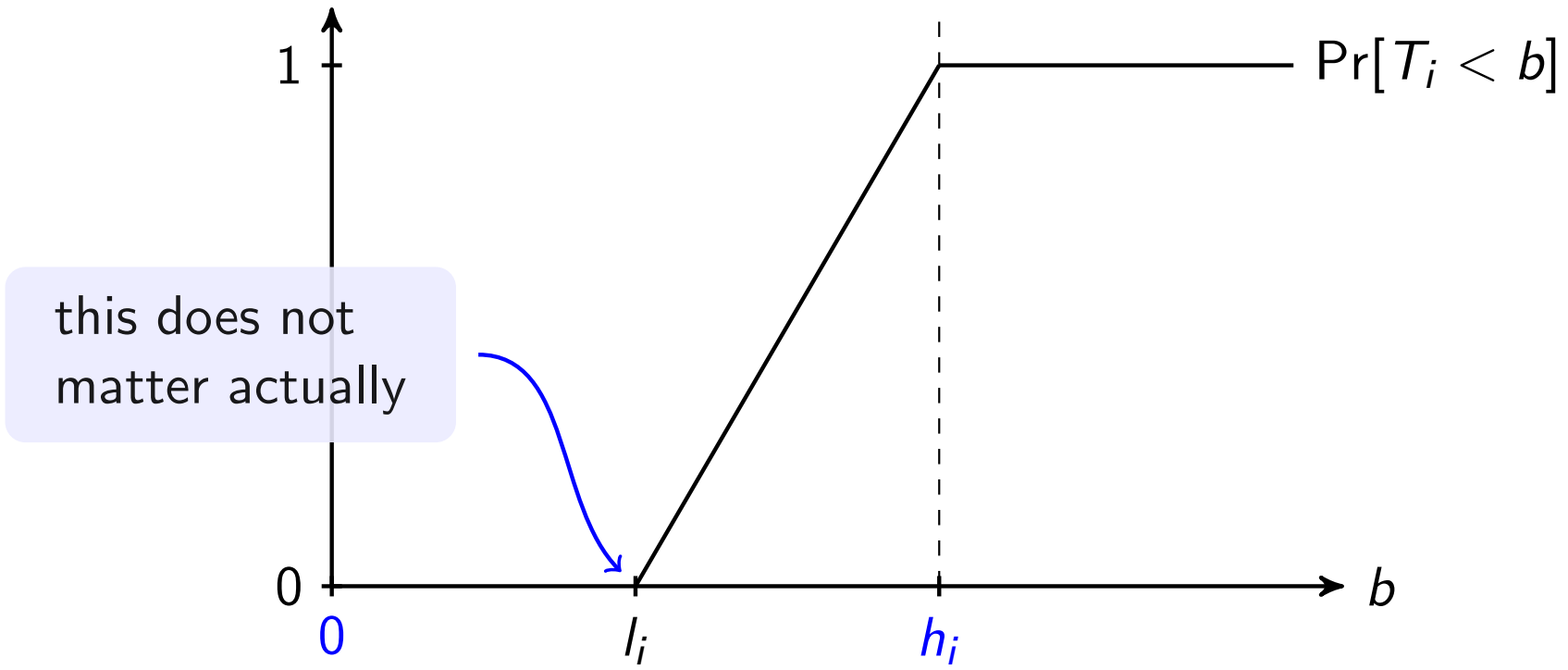
- good approximation when little information is available



Uniform Trustworthiness Distributions

Lemma

For a given employee i, Eve's optimal bribe value is either 0 or h_i (or both).



Uniform Trustworthiness Distributions

Lemma

Let k' be $\sum_i h_i/S$. Then, the equilibrium of the game can be characterized as follows:

- *$k < k'$: Alice is perfectly secure, Eve never bribes any of the employees.*

"There is a critical team size, below which we can be perfectly secure, ..."

Uniform Trustworthiness Distributions

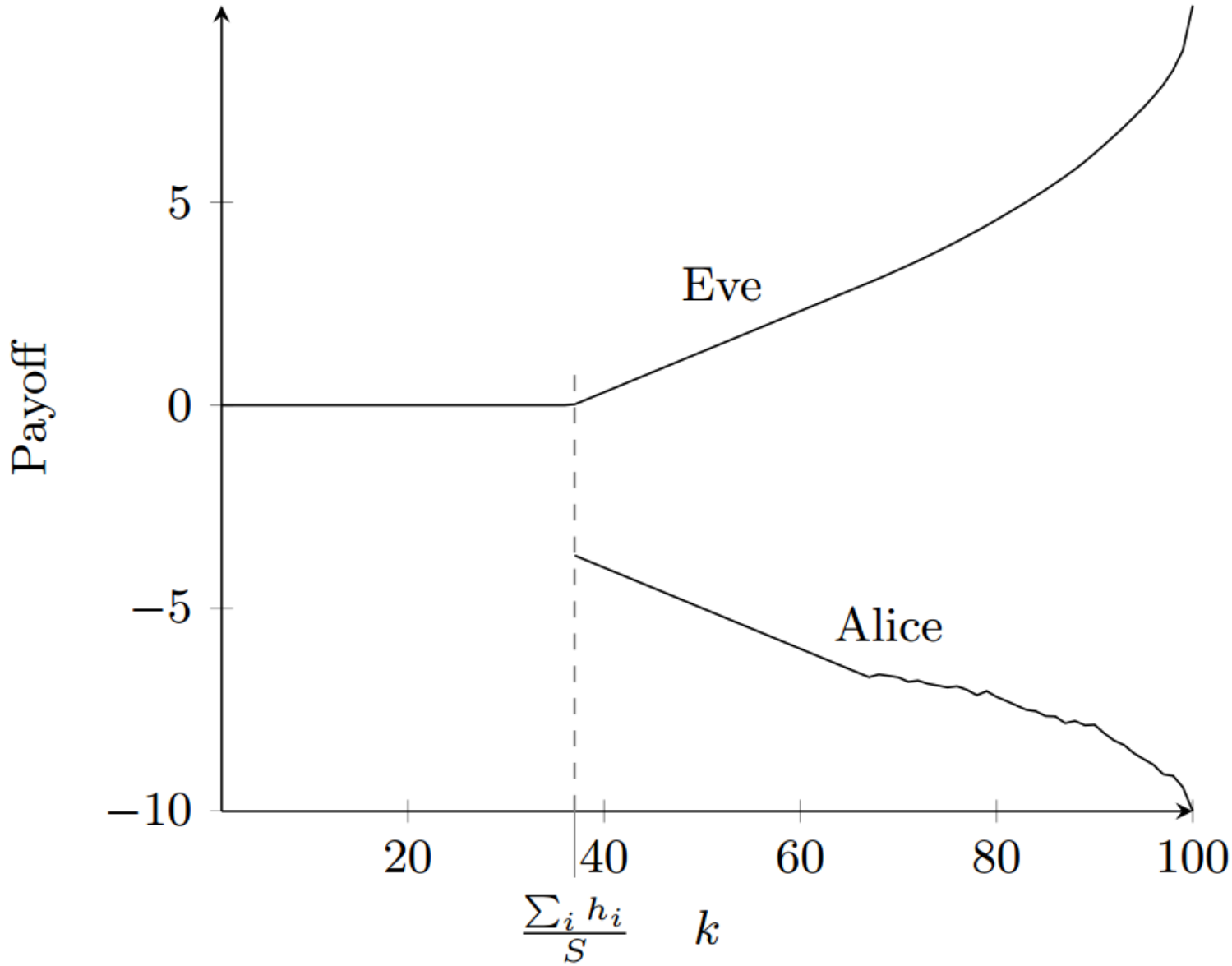
Lemma

Let k' be $\sum_i h_i/S$. Then, the equilibrium of the game can be characterized as follows:

- *$k < k'$: Alice is perfectly secure, Eve never bribes any of the employees.*
- *$k > k'$: Alice is not secure, Eve always chooses a sufficiently high bribe value and learns the secret with non-zero probability.*
- *$k = k'$: Eve can choose one of the above.*

"There is a critical team size, below which we can be perfectly secure, but above which our only chance is randomizing the selection."

Uniform Trustworthiness Distributions - Illustration



Conclusions and Open Problems

- Conclusions & lessons learned
  - game-theoretic model for bribe-resistant team composition
  - do not (always) follow your intuitions
  - a project manager should select every employee with a non-zero probability, unless there is a perfectly secure strategy
  - trusting people is tricky

Conclusions and Open Problems

- Conclusions & lessons learned
  - game-theoretic model for bribe-resistant team composition
  - do not (always) follow your intuitions
  - a project manager should select every employee with a non-zero probability, unless there is a perfectly secure strategy
  - trusting people is tricky
- Open problems
  - study the model instantiated with actual data
  - targeting multiple employees at the same time
  - asymmetric information

Thank you for your attention!

Questions?

laszka@crysys.hu, johnsonb@ischool.berkeley.edu, pascal.schoettle@wi.uni-muenster.de, jensg@ist.psu.edu, rainer.boehme@wi.uni-muenster.de

Acknowledgements

We gratefully acknowledge the support of the Penn State Institute for Cyber-Science. The first author would like to thank the Campus Hungary Program for supporting his research visit. The third author would like to thank the Office of Naval Research (ONR) for supporting his research visit under Visiting Scientists Grant N62909-13-1-V029.

References I

[1] Nick Bontis.
Assessing knowledge assets: A review of the models used to measure intellectual capital.
International Journal of Management Reviews, 3(1):41–60, 2001.

[2] Corporate Trust (Business Risk & Crisis Mgmt. GmbH).
Studie: Industriespionage 2012 - Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar, 2012.

[3] FBI.
The insider threat.
http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure, April 2013.

References II

[4] Federal Bureau of Investigation.
Economic espionage.
http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage.

[5] Peter Finn.
Chinese citizen sentenced in military data-theft case.
Washington Post, March 2013.

[6] Asmaa Munshi, Peter Dell, and Helen Armstrong.
Insider threat behavior factors: A comparison of theory with reported incidents.
In IEEE HICSS 2012, pages 2402–2411, 2012.

References III

[7] Marisa Randazzo, Michelle Keeney, Eileen Kowalski, Dawn Cappelli, and Andrew Moore.
Insider threat study: Illicit cyber activity in the banking and finance sector.
Technical Report CMU/SEI-2004-TR-021, Carnegie Mellon University, June 2005.