Should Cyber-Insurance Providers Invest in Software Security?

Aron Laszka[1] and Jens Grossklags[2]

[1] University of California, Berkeley
[2] Pennsylvania State University

Software Vulnerabilities

- Most software products suffer from vulnerabilities
- Developers have little incentive to invest more into security
  - developers are usually not held liable for incidents
  - investing into security increases costs and may impact time-to-market or create backwards compatibility issues
  - customers rarely reward security immediately
- However, vulnerabilities in widely used software pose a severe risk

What can users do?

- Major technology companies may invest into key software products
  - e.g., Google and Samsung vulnerability reward programs
  - cover only a small set of products, which are critical for their own operations
  - cannot fully address the security risks related to the diverse landscape of widely used software products
- What about companies lacking the resources and/or expertise to effectively invest into security?

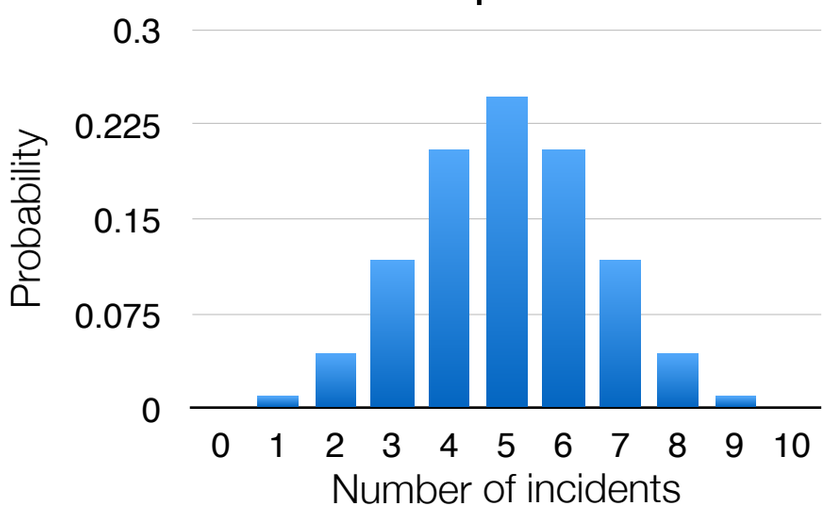
Cyber-Insurance

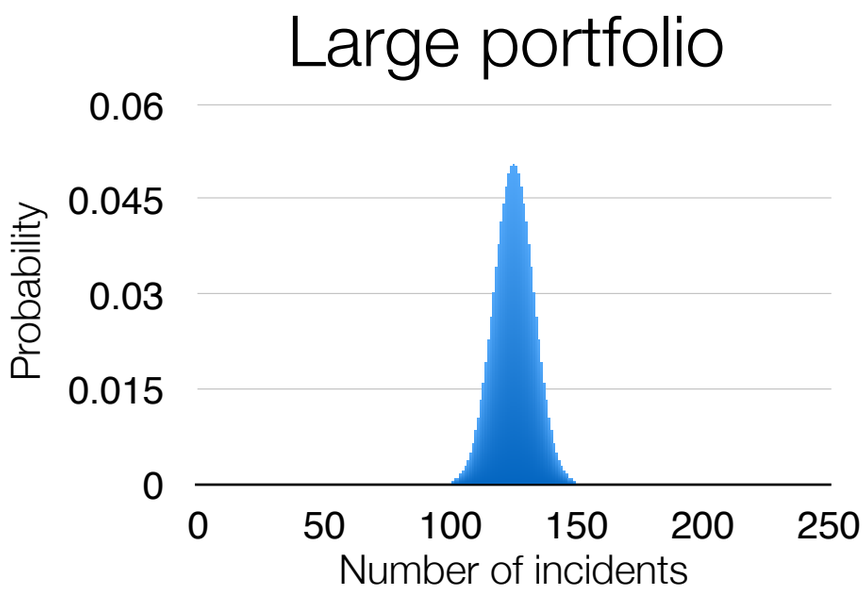
- A company may buy cyber-insurance to transfer its risk to an insurance provider
  - i.e., trading variable losses for a fixed premium
- Supply side of cyber-insurance: insurance provider
  - receives fixed premiums in exchange for variable claims
  - amount of claims to be paid is variable → provider's risk
- How can an insurance provider account for this risk?

  Diversification: *if the provider's portfolio is large enough, then the amount of claims to be paid is almost always close to its expected value*

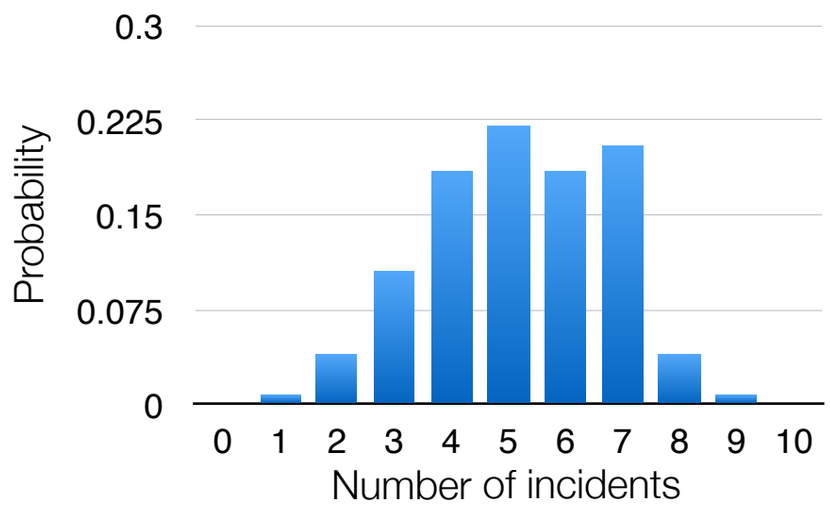
Insurance Claim Distributions

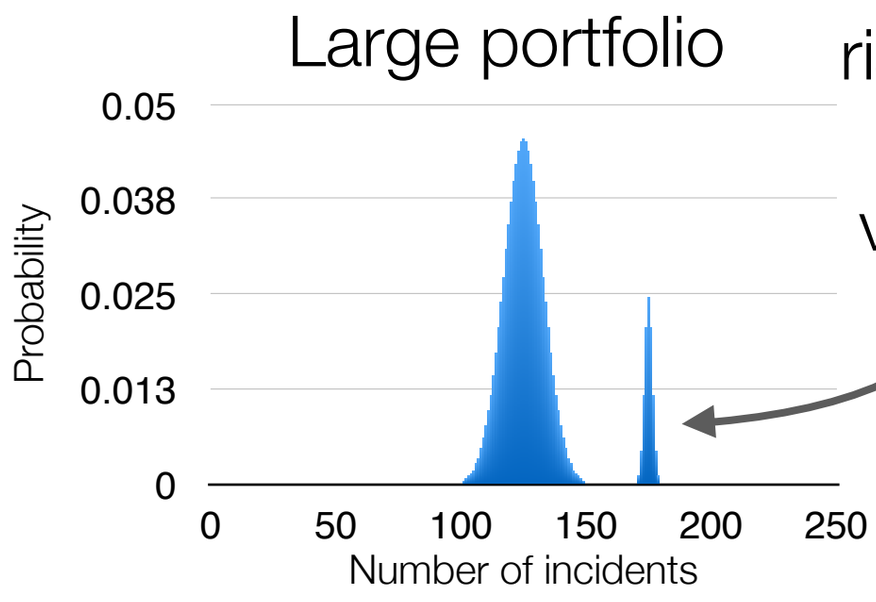
Independent incidents





Cyber incidents





Diversifiable and Non-Diversifiable Risks

Diversifiable risk	**Non-diversifiable risk**
• caused by individual vulnerabilities (e.g., misconfiguration)	• caused (in part) by vulnerabilities in widely used software products
• diminishes as the size of the portfolio increases	• does not diminish with the size of the portfolio
• both provide an incentive for companies to purchase insurance	
• results in predictable insurance claims	• can cause significant fluctuations in the arrival of insurance claims

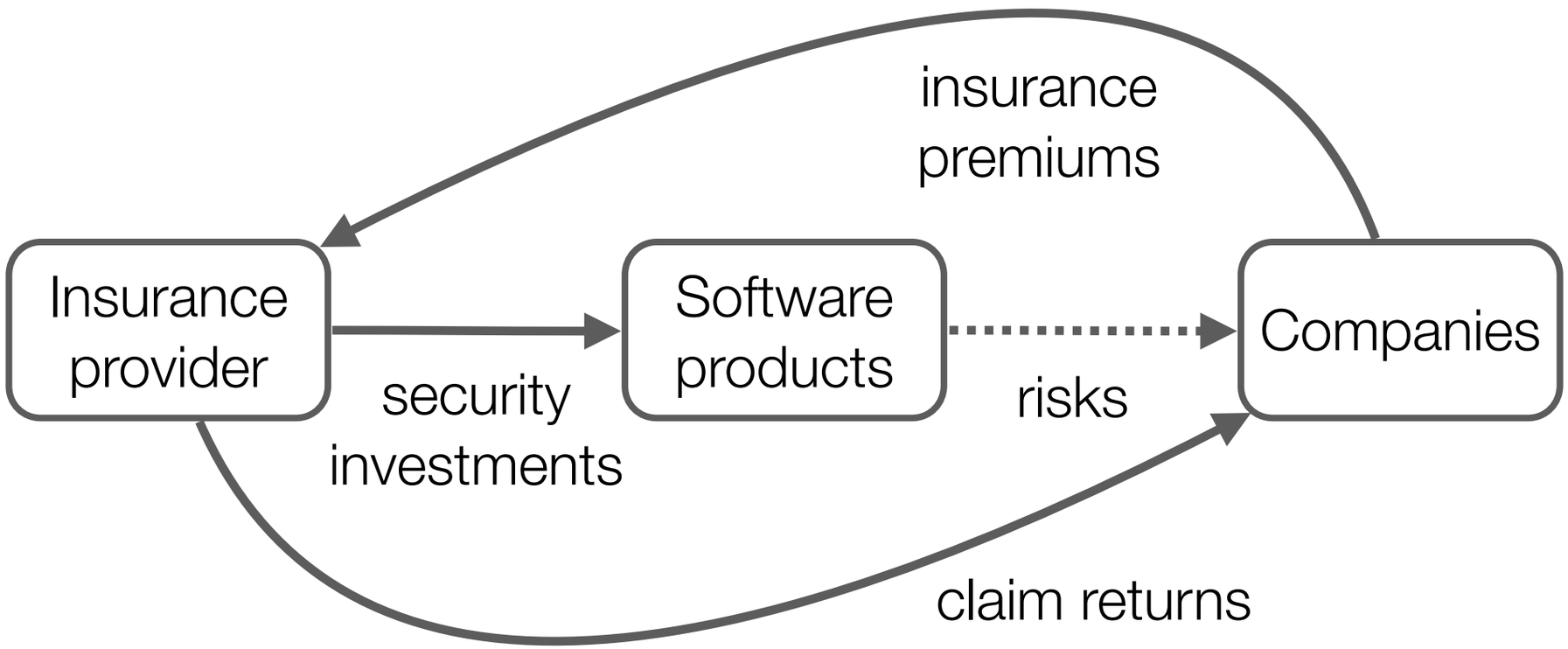
Possible Approaches for Insurance Providers

- Incentivizing customers to invest in security
  - for example, by offering premium reductions for investing in security
  - currently dominant practice
  - typical security investments, such as purchasing security products and hiring auditors, decrease diversifiable risks without decreasing non-diversifiable risks
- Investing in software security
  - for example, by financing vulnerability reward programs for popular software products used by their customers
  - decreases non-diversifiable risks

Can investing in software security be a viable approach?

Model

- Cyber-insurance model incorporating software vulnerabilities and security investments
- Elements:
  - monopolist *insurance provider*
  - *companies* that purchase insurance from the *provider*
  - *software products* that are used by the *companies*



Model: Vulnerabilities and Risks

- Software products

$$V_i(d_i) = BV_i \cdot e^{-\gamma_i d_i}$$

  - V_i : vulnerability level of software i
  - d_i : insurance provider's security investment in software i
  - BV_i : base vulnerability
  - γ_i : efficiency of investment

- Companies

$$R_j = 1 - (1 - IR_j) \prod_{i \in \mathcal{S}_j} (1 - V_i)$$

  - R_j : incident probability for company j
  - IR_j : individual risk of company j
  - S_j : set of software used by company j

Model: Demand-Side of Insurance

- Companies are risk-averse
  - utility for a given amount of wealth w is given by a *Constant Relative Risk Aversion* (CRRA) utility function:

$$\ln(w)$$

- Baseline utility (without insurance) of company j:

$$R_j \ln(W_j - L_j) + (1 - R_j) \ln(W_j)$$

  - W_j : initial wealth
  - L_j : loss in case of an incident

- Insured utility of company j:

$$\ln(W_j - p_j)$$

  - p_j : premium paid by company j

from these, we can compute the insurance premiums for a monopolist provider

Model: Supply-Side of Insurance

- Insurance provider's income:

$$\sum_j p_j$$

- Probability of ruin:
  - probability that the total amount of losses TL (i.e., total amount of claims to be paid) exceeds the provider's safety capital S
  - we assume that the maximal probability of ruin ε is exogenous
- Insurance provider's expenditure:

$$\mathrm{E}[TL] + \sum_i d_i + A + I \cdot S$$

  - $\mathrm{E}[TL]$: expected total amount of losses
  - d_i : security investments
  - A : administrative costs
  - I : interest rate
  - S : minimal safety capital to keep the probability of ruin below ε

Analysis

- Computational complexity of our model
  - hidden complexity from computing the claim distributions
- Provider strategies for investing in security
- Numerical results for evaluating our model and investment strategies

Computational Complexity

Theorem 1. Given a safety capital S and a threshold probability of ruin ε, determining whether the probability of the total amount of losses TL exceeding $S + \mathrm{E}[TL]$ is greater than or equal to ε is NP-hard.

- consequently, it is hard to determine the minimal safety capital and, thus, compute the insurer's profit for a given set of investment values

Theorem 2. Let $TL_1, TL_2, ..., TL_K$ be K independent random variables having the same distribution as TL, and let $\hat{S}$ be the $(1 - \varepsilon)K$-th smallest of these random variables. Then,

$$\Pr[TL > \hat{S}] \leq \varepsilon + \frac{1}{K}$$

- in other words, we can approximate the minimal safety capital using random sampling

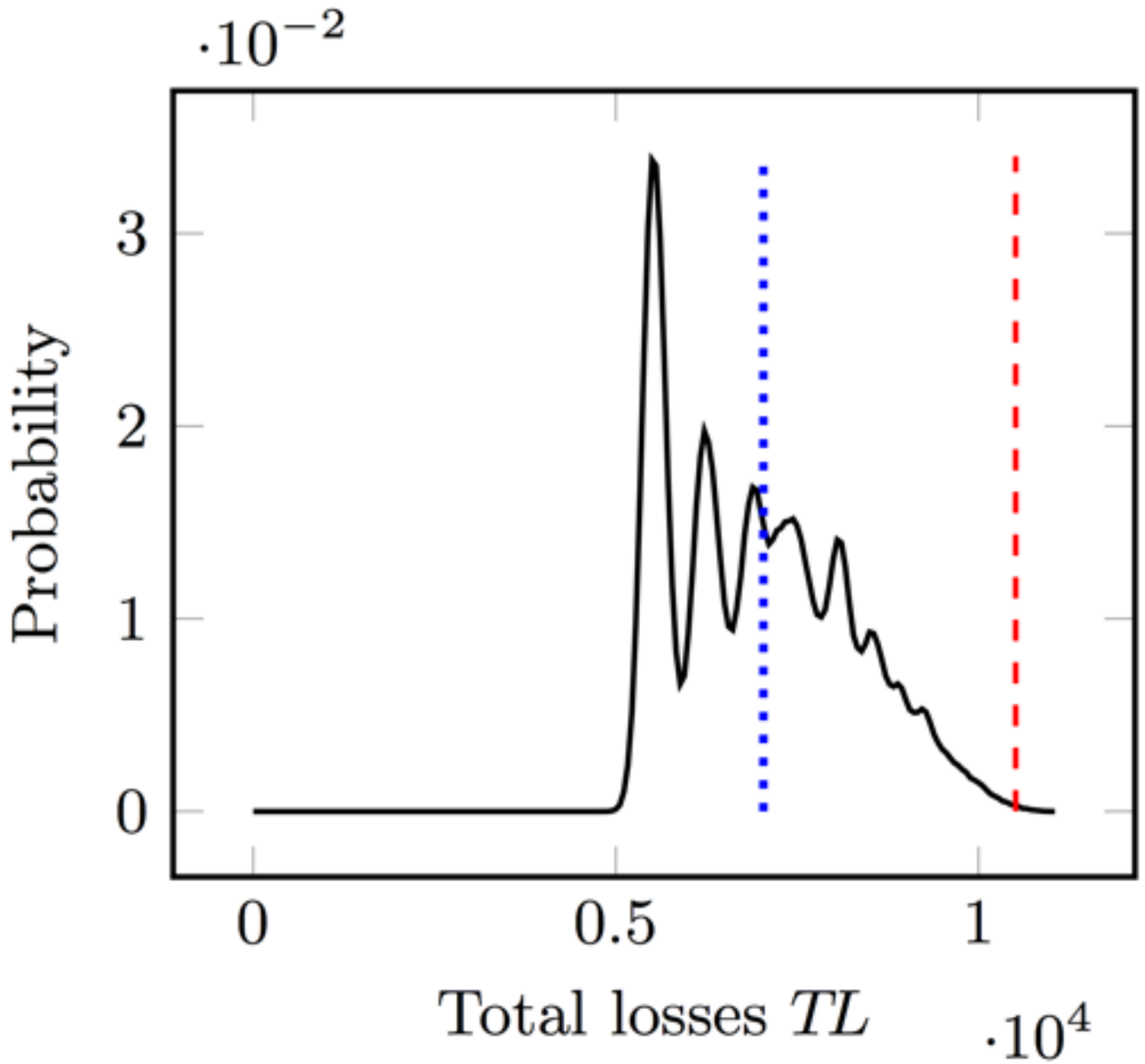
Finding Optimal Security Investments

- *Investment strategy*: given aggregate investment amount $\sum_i d_i$, divide this amount among the software products
- **Uniform strategy**: divide evenly among the software products
- **Most-used strategy**: invest into the software product used by the most companies
- **Proportional strategy**: invest into each software product proportionally to the number of companies using it
- **Greedy strategy**: distribute amount in multiple steps, in each step investing into a software product so that the increase in profit is maximal

Numerical Results

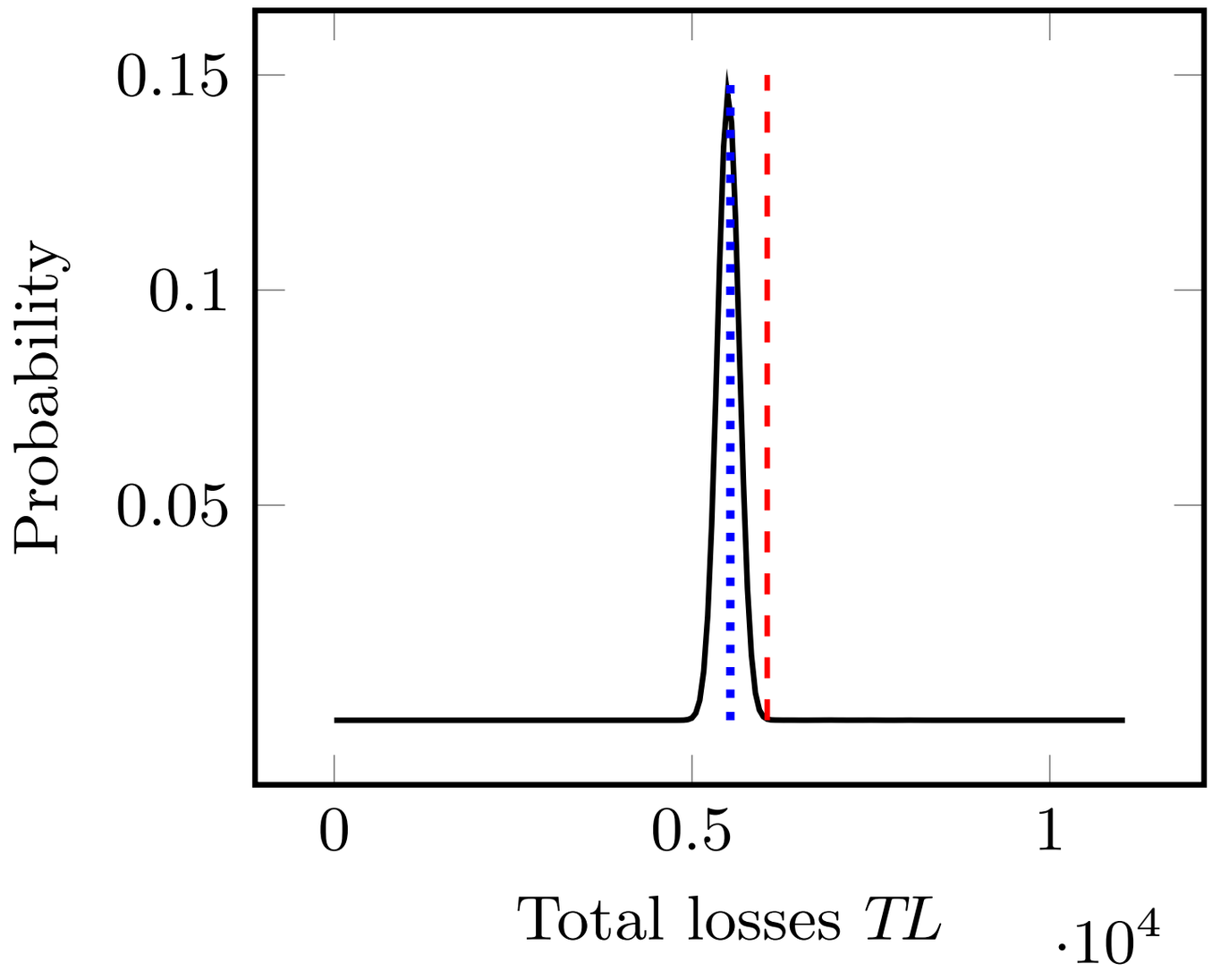
- We instantiated our model with exemplary values to illustrate the relative effect of the investment strategies
- We generated 15 software products with
  - base vulnerability BV_i randomly drawn from [0.09, 0.11]
  - investment efficiency γ_i randomly drawn from [0.9, 1.1]
- We generated 1500 companies with
  - individual risk IR_j randomly drawn from [0.4, 0.6]
  - base wealth W_j randomly drawn from [10, 20]
  - potential loss L_j randomly drawn from [0.25W_j, 0.75W_j]
- For each company, we choose 3 software products using popularity-based preferential-attachment

Insurance Claim Distribution without Investments



- **blue line**: expected value
- **red line**: 99.9% quantile

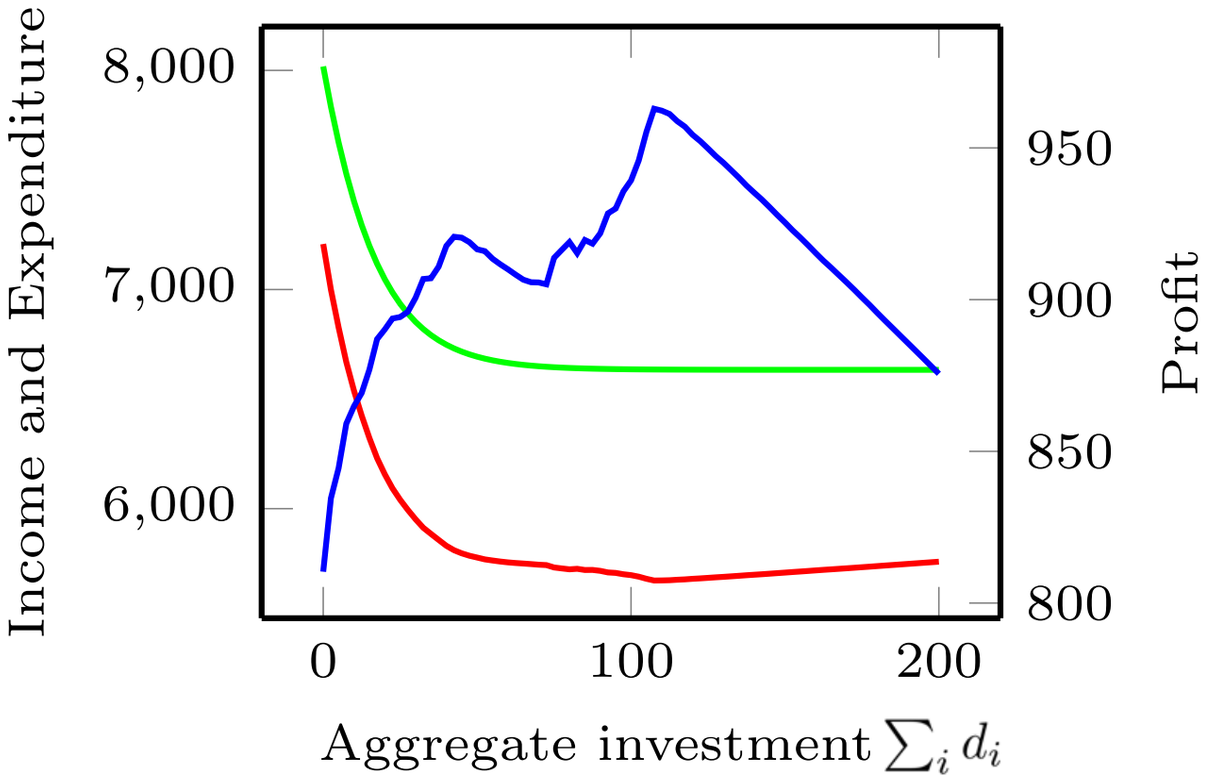
Claim Distribution with Uniform Investments



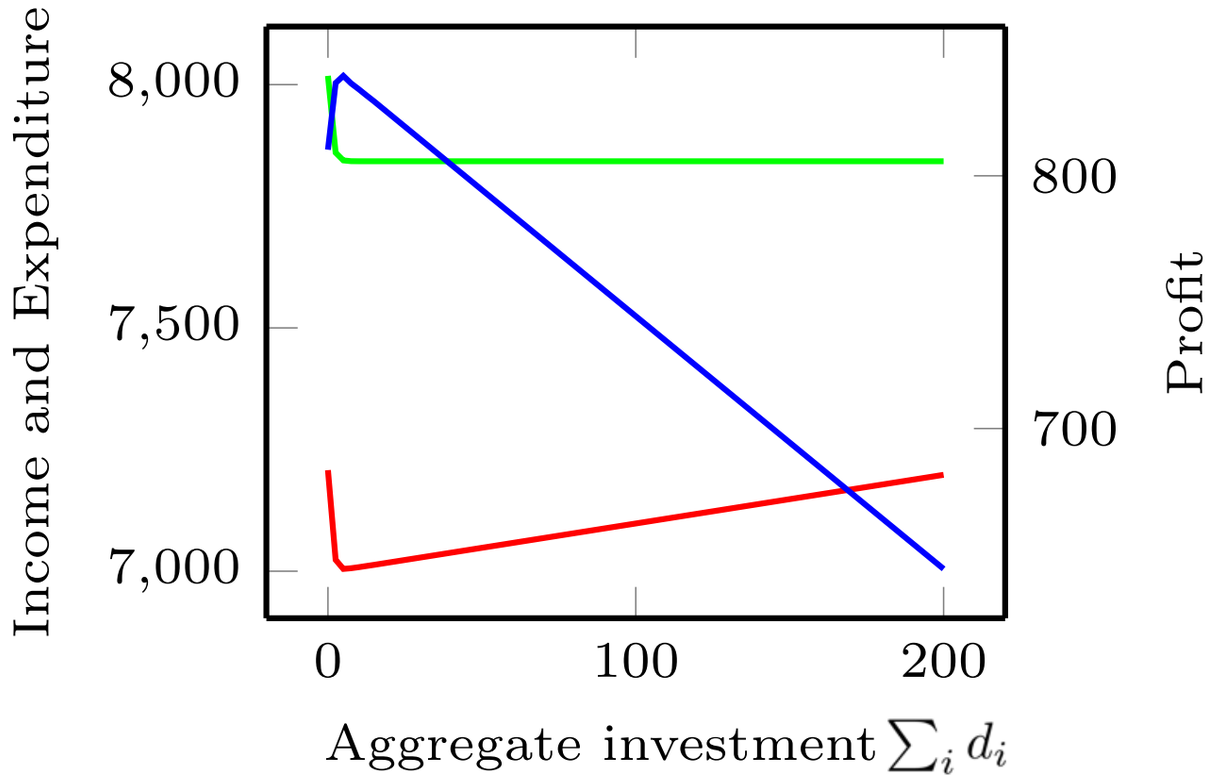
- $d_i = 7.5$ for every software i

Investment Strategies: Uniform and Most-Used

Uniform



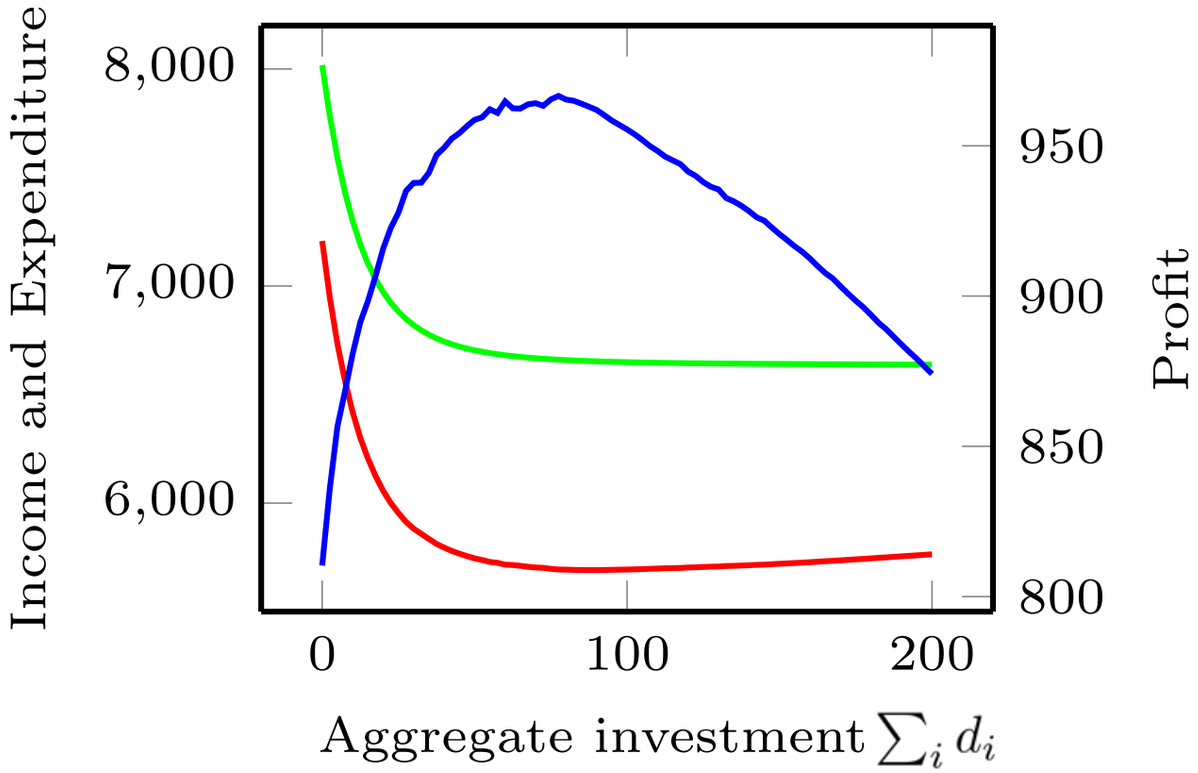
Most-used



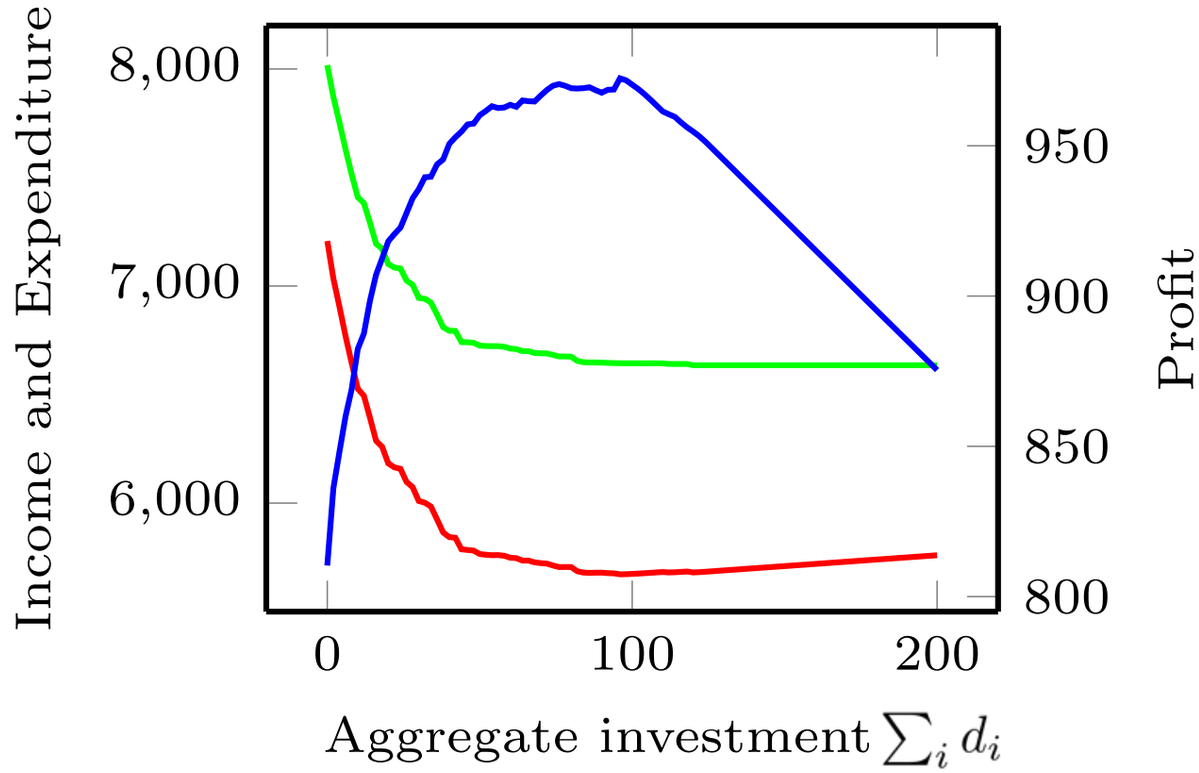
- **green line**: income
- **red line**: expenditure
- **blue line**: profit

Investment Strategies: Proportional and Greedy

Proportional

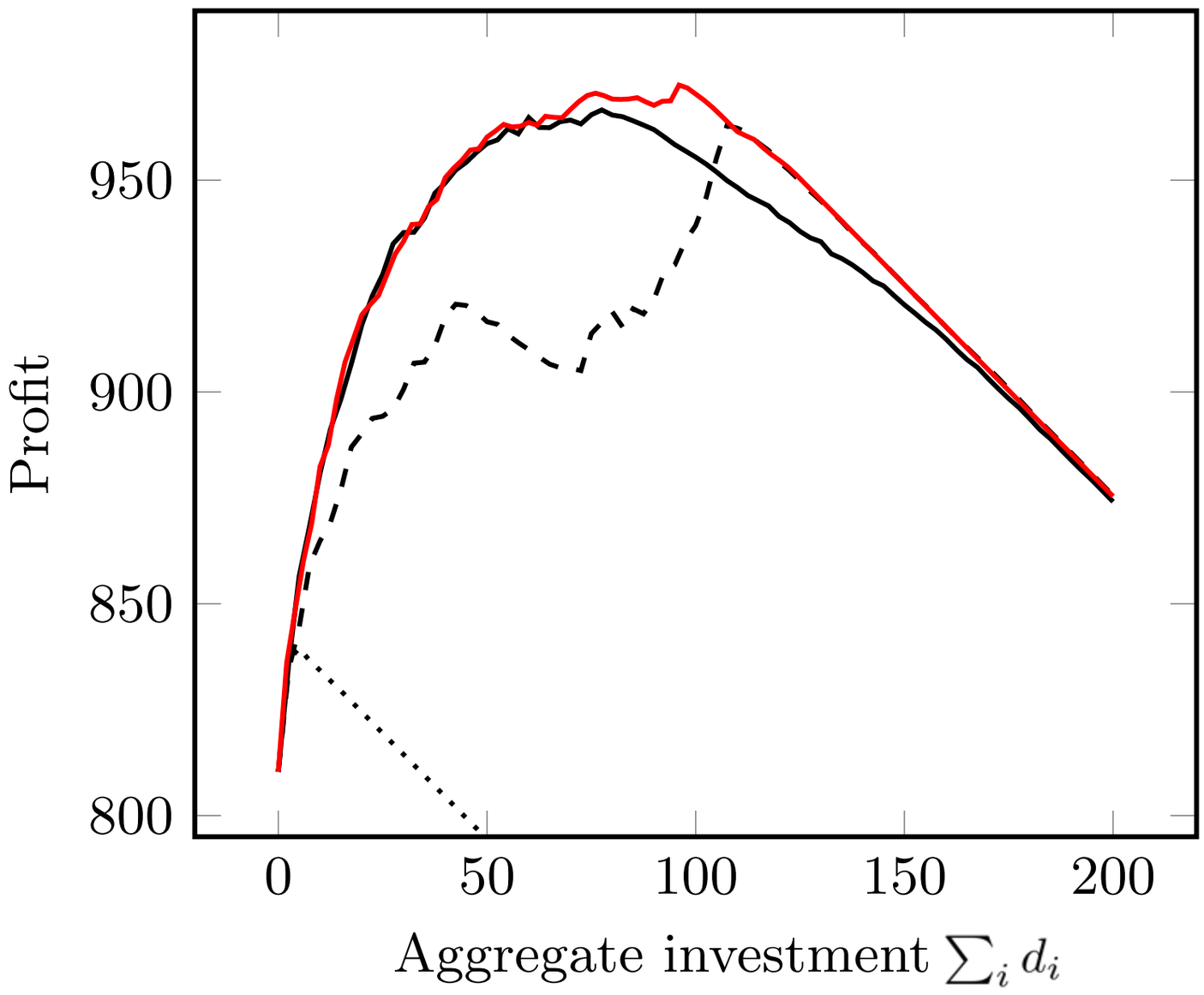


Greedy



- **green line**: income
- **red line**: expenditure
- **blue line**: profit

Comparison of Investment Strategies



- red line: greedy
- solid line: proportional
- dashed line: uniform
- dotted line: most-used

Conclusion and Future Work

- Companies want to buy affordable insurance for cyber-risks, and insurers want to offer profitable insurance policies
  - non-diversifiable risks arising from software monocultures may result in prohibitively high safety capitals or insurance premiums
- Our results show that insurers may have the incentives to invest in software security and thereby reduce non-diversifiable risks
  - in contrast to other approaches which have gained limited traction (e.g., software liability, government involvement)
- Future work:
  - numerical evaluations based on real-world datasets
  - modeling multiple, competitive insurance providers
  - studying positive spillover effects for uninsured entities

Thank you for your attention!

Questions?