The Iterated Weakest Link

A Model of Adaptive Security Investment

Rainer Böhme and Tyler Moore

Institute of Systems Architecture, Technische Universität Dresden
Center for Research on Computation and Society, Harvard University

8th Workshop on the Economics of Information Security
University College London, UK
June 24, 2009

Outline

Motivation

- We read about security breaches in the news almost daily, each bigger and more costly than the last
- Is such unending failure a consequence of flawed technology, policy, or simply ineptitude?
- Or does it reflect rational behavior?
  - Up-front security investment can be expensive
  - Deciding which threats to protect against is hard, and prone to miscalculations and oversights
  - Might it be easier to wait for an attacker to act, and then respond?

The iterated weakest link model

- Information systems are often structured so that a system's overall security depends on its weakest link
  - The most careless programmer introduces a vulnerability
  - Botnet herders run command-and-control from most lax ISPs
  - Varian (WEIS 2004) studied the static case of weakest links
- But what about the dynamic case?
  - Attackers exploit the weakest link; defenders plug the hole; attackers move on to the next-weakest link
  - Our model captures this iterative nature
- In our model, defender uncertainty regarding which links are weakest helps justify reactive, delayed security investment

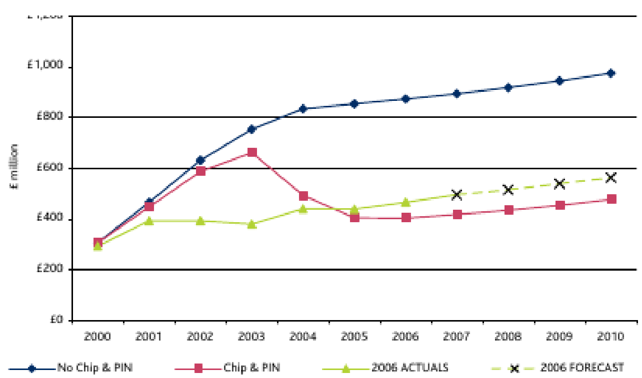
Phishing and online crime

- Due to its open, distributed architecture, the Internet's overall security depends on the weakest link
- Substantial evidence that attackers shift operations from one ISP to the next
  - Once ISPs act to clean up malware-infected webservers, attackers move on to other ISPs (Day et. al WEIS 2008)
  - Bot command and control quickly adapted once protective ISPs/registrars shut down (RBN, McColo, EstDomains, ...)
  - Rock-phish gang iterate over unsuspecting registrars (Moore and Clayton 2007)

Payment card security and the iterated weakest link

- Many security mechanisms have been introduced over the past few decades to combat card fraud
- The latest defense, Chip & PIN, has substantially reduced face-to-face transaction fraud in the UK
- Yet aggregate fraud losses have increased since Chip & PIN's introduction
- Why? Fraudsters have found other weaknesses to exploit

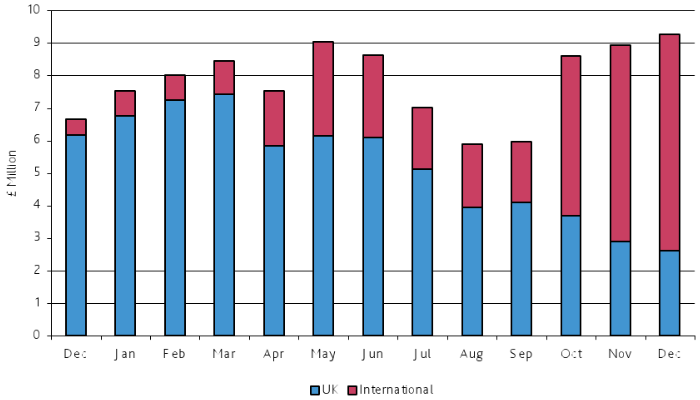
UK total payment card fraud 2000–2010



The rise of card-not-present fraud

Fraud type	2004	2006
Face-to-face retail	£219m	£72m
Card-not-present (UK)	£100m	£138m
Card-not-present (Int'l)	£50m	£78m

ATM fraud shifted overseas once chip verification mandatory in UK



Defender's costs

- Defender considers n threats to protect against
- Cost of countermeasures may be interdependent

$$C = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \qquad C = \begin{bmatrix} 1 & 0 & 12 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -12 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

(a) independent defenses

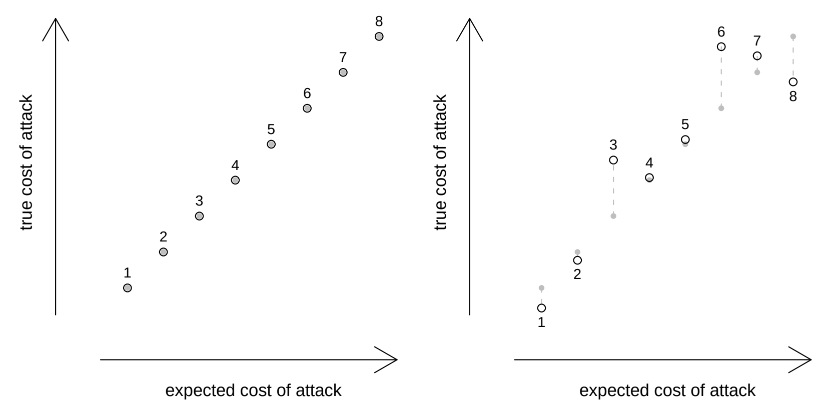
(b) conflicting defenses: 1 and 3
complementary defenses: 3 and 4

- Sunk costs modeled as fraction of the protected asset

Defender's knowledge

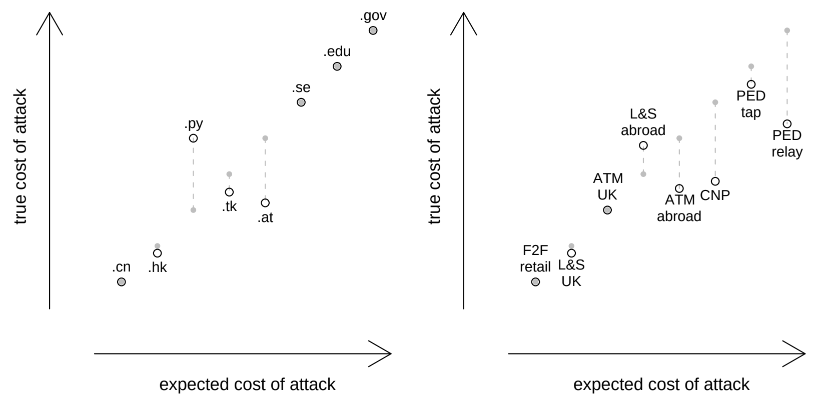
- Order threats by increasing expected cost of attack
  - Expected attack cost for threat i:
    $\overline{x}_i = \overline{x}_1 + (i-1) \cdot \Delta x$
  - True attack cost for threat i:
    $\mathcal{N}(\overline{x}_i, \sigma/\Delta x)$

Modeling uncertainty about true attack costs



certainty: $\sigma = 0$ uncertainty: $\sigma = 1$

Uncertainty in online crime & payment card defense



Rock-phish domain costs

EMV attack costs

Attacker's cost and knowledge

- We assume that the attacker correctly identifies and exploits the weakest link
- Attacker is certain of costs of carrying out each attack
- Only attacks when cost of attack is less than the gain from attacking

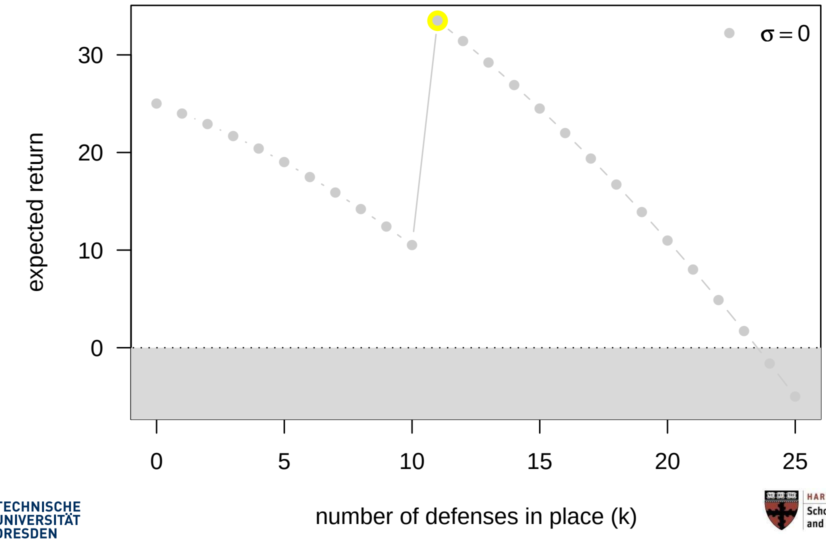
Exploring optimal defense

1. No uncertainty: a static strategy is always as good or better than a dynamic one
2. Static configuration, with uncertainty
3. Dynamic configuration, with uncertainty
4. Dynamic configuration, with uncertainty and sunk costs

Modeling parameters used

- Asset Value: $1 million
- Return on asset: 5%
- Loss given attack: 2.5% of asset
- Minimum expected cost of attack: $15 000
- Gradient of attack cost: $1 000
- Defense interdependence: $\rho = 0.1$
- Number of attacks n: 25

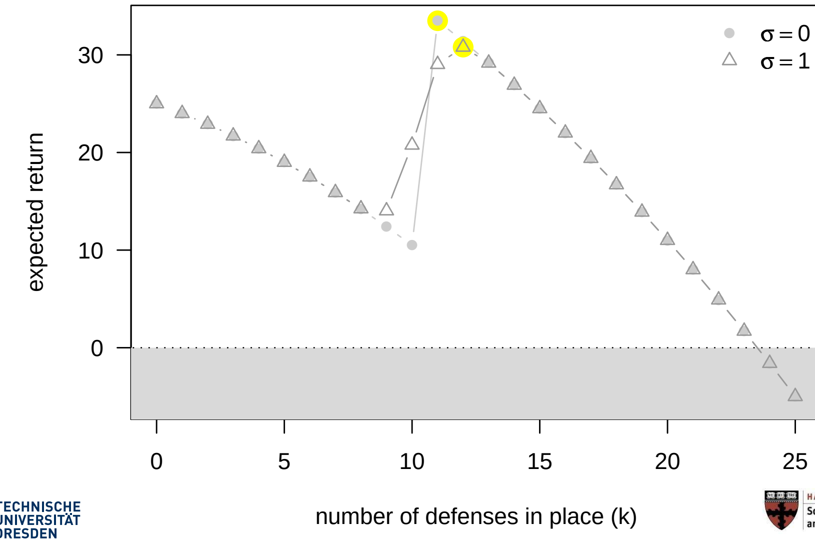
Static configuration, with uncertainty



TECHNISCHE UNIVERSITÄT DRESDEN

HARVARD School of Engineering and Applied Sciences

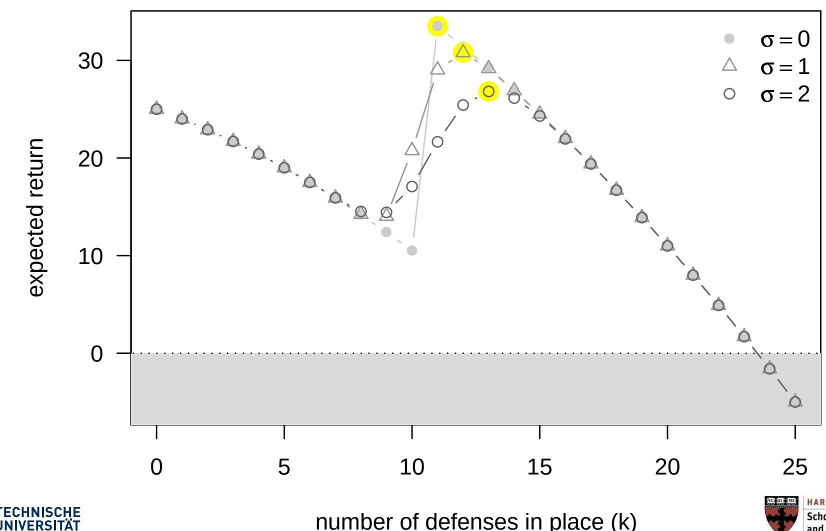
Static configuration, with uncertainty



TECHNISCHE UNIVERSITÄT DRESDEN

HARVARD School of Engineering and Applied Sciences

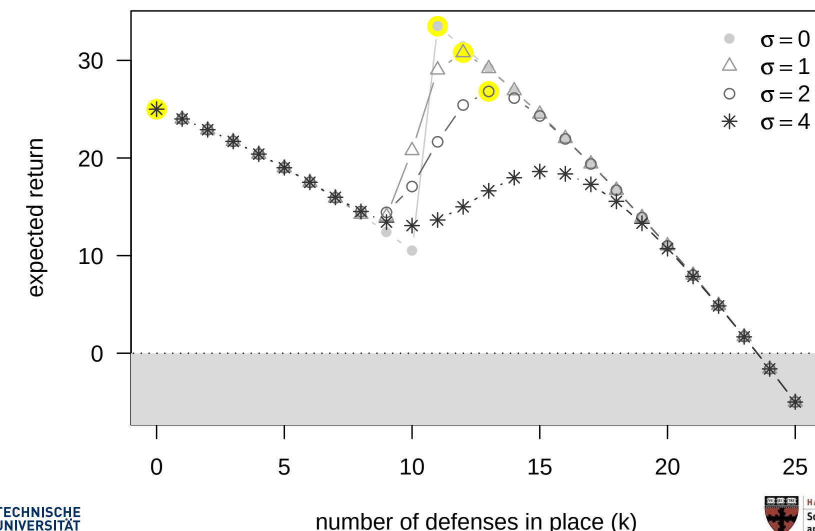
Static configuration, with uncertainty



TECHNISCHE UNIVERSITÄT DRESDEN

HARVARD School of Engineering and Applied Sciences

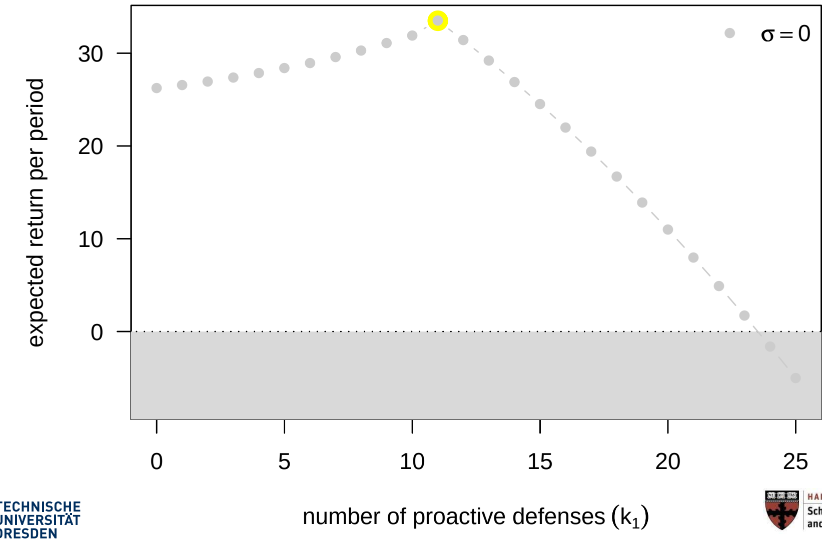
Static configuration, with uncertainty



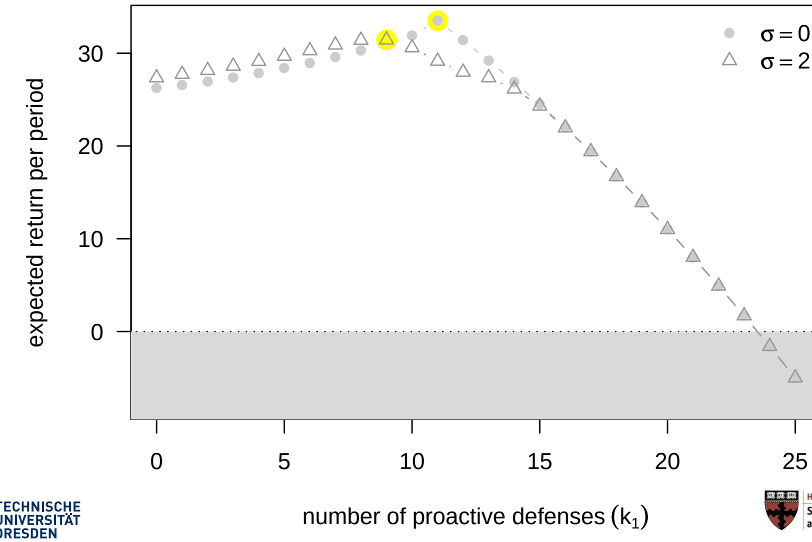
TECHNISCHE UNIVERSITÄT DRESDEN

HARVARD School of Engineering and Applied Sciences

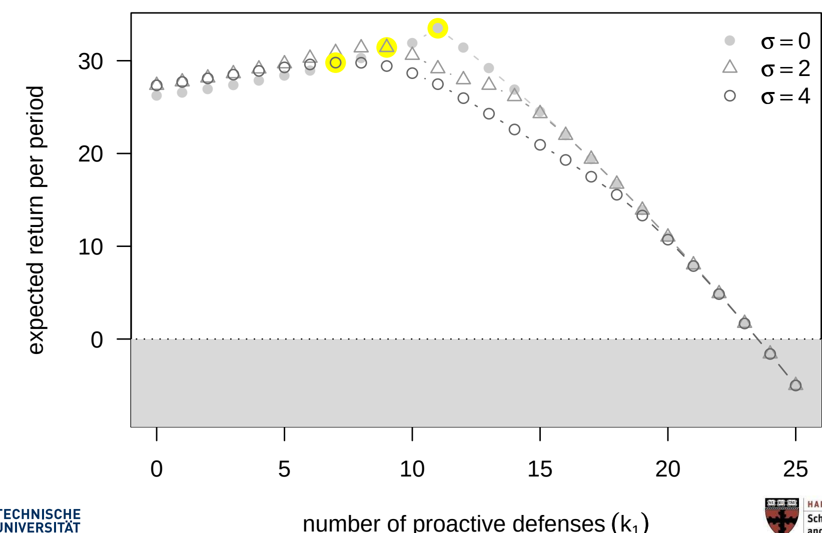
Dynamic configuration, with uncertainty and no sunk costs



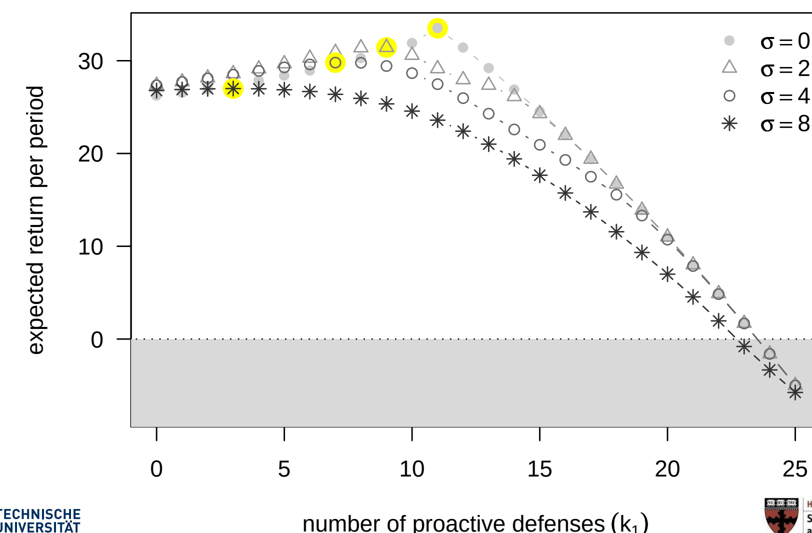
Dynamic configuration, with uncertainty and no sunk costs



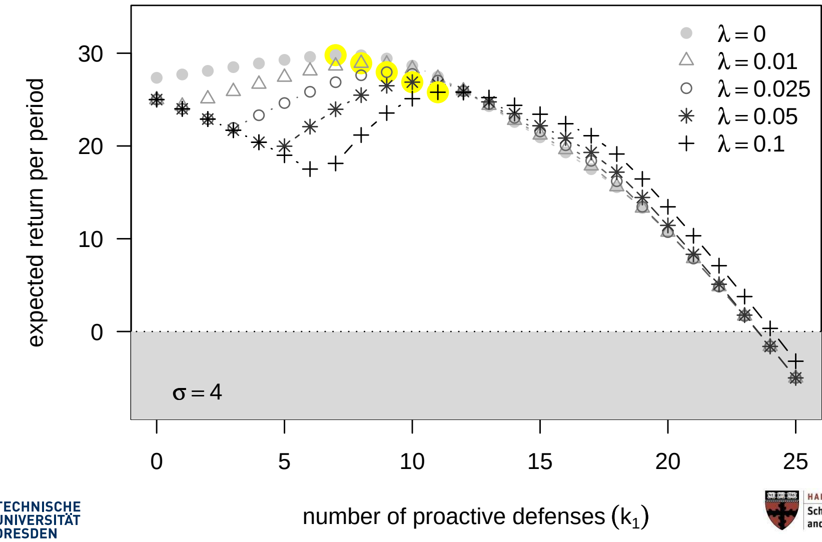
Dynamic configuration, with uncertainty and no sunk costs



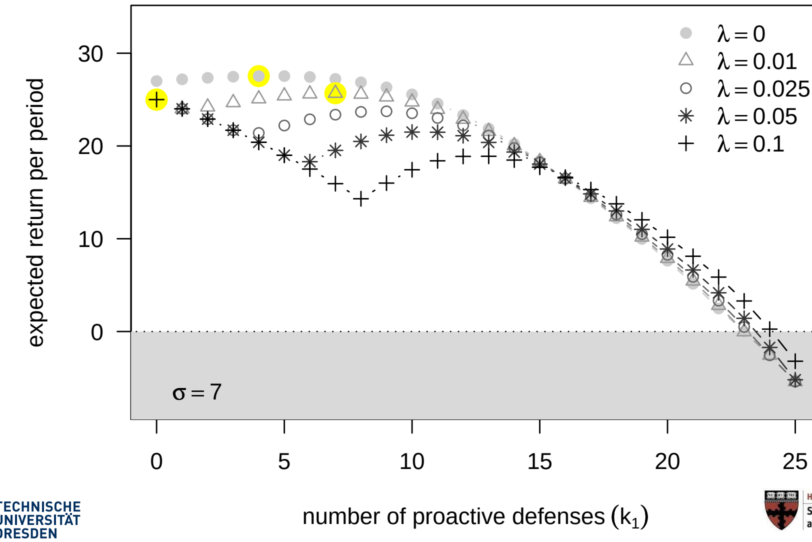
Dynamic configuration, with uncertainty and no sunk costs



Dynamic configuration, with uncertainty and sunk costs



Dynamic configuration, with uncertainty and sunk costs



Iterated weakest link and return on security investment

	Level of uncertainty			
Indicator	$\sigma = 0$	$\sigma = 1$	$\sigma = 4$	$\sigma = 8$
Static defense				
optimal defense k^*	11	12	0	0
attack intensity (% rounds)	0.0	2.4	100.0	100.0
ROSI (% security spending)	51.5	31.2	—	—
Dynamic defense w/o sunk costs				
optimal proactive defense k_1^*	11	9	7	3
attack intensity (% rounds)	0.0	6.1	15.7	32.7
ROSI (% security spending)	51.5	52.8	35.2	18.9
Dynamic defense w/ sunk costs				
optimal proactive defense k_1^*	11	10	9	0
attack intensity (% rounds)	0.0	2.9	9.8	100.0
ROSI (% security spending)	51.5	50.6	15.7	—

Conclusion

- Uncertainty about relative weaknesses explains why reactive security investment is often preferable to proactive measures
- Our model explains security underinvestment independent of impact on others (no externalities required!)
- For more ...
  - My web page
    `http://people.seas.harvard.edu/~tmoore/`
  - Rainer's web page
    `http://www.tu-dresden.de/~rb21/`