Empirical Security & Privacy, for Humans

UPenn CIS 7000-010

8/28/2025

Security – An economic perspective

Readings

Plus: “How to Read a Paper?”

Why Information Security is Hard
– An Economic Perspective

Ross Anderson

University of Cambridge Computer Laboratory,
JJ Thomson Avenue, Cambridge CB3 0FD, UK
Ross.Anderson@cl.cam.ac.uk

Abstract

According to one common view, information security comes down to technical measures. Given better access control policy models, formal proofs of cryptographic protocols, approved firewalls, better ways of detecting intrusions and malicious code, and better tools for system evaluation and assurance, the problems can be solved.

In this note, I put forward a contrary view: information insecurity is at least as much due to perverse incentives. Many of the problems can be explained more clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons.

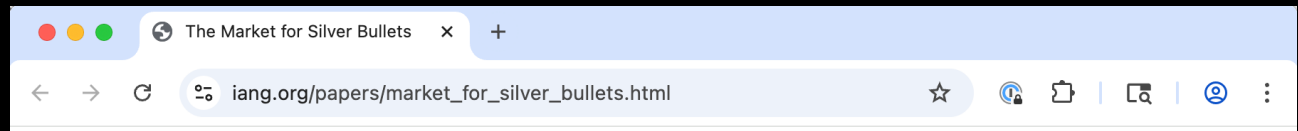
1 Introduction

In a survey of fraud against autoteller machines [4], it was found that patterns of fraud depended on who was liable for them. In the USA, if a customer disputed a transaction, the onus was on the bank to prove that the customer was mistaken or lying; this gave US banks a motive to protect their systems properly. But in Britain, Norway and the Netherlands, the burden

risk of forged signatures from the bank that relies on the signature (and that built the system) to the person alleged to have made the signature. Common Criteria evaluations are not made by the relying party, as Orange Book evaluations were, but by a commercial facility paid by the vendor. In general, where the party who is in a position to protect a system is not the party who would suffer the results of security failure, then problems may be expected.

A different kind of incentive failure surfaced in early 2000, with distributed denial of service attacks against a number of high-profile web sites. These exploit a number of subverted machines to launch a large coordinated packet flood at a target. Since many of them flood the victim at the same time, the traffic is more than the target can cope with, and because it comes from many different sources, it can be very difficult to stop [7]. Varian pointed out that this was also a case of incentive failure [20]. While individual computer users might be happy to spend $100 on anti-virus software to protect themselves against attack, they are unlikely to spend even $1 on software to prevent their machines being used to attack Amazon or Microsoft.

This is an example of what economists refer to as the ‘Tragedy of the Commons’ [15]. If a hundred peas-



The Market for Silver Bullets

Ian Grigg
Systemics, Inc.

2nd March 2008

Abstract: What is security?

As a “good” in the sense of economics, security is now recognised as being one for which our knowledge is poor. As with safety goods, events of utility tend to be destructive, yet unlike safety goods, the performance of the good is very hard to test. The roles of participants are complicated by the inclusion of agressive attackers, and buyers and sellers that interchange.

This essay hypothesises that security is a good with insufficient information, and rejects the assumption that security fits in the market for goods with asymmetric information. Security can be viewed as a market where neither buyer nor seller has sufficient information to be able to make a rational buying decision. Drawing heavily from Michael Spence's “Job Market Signaling,” these characteristics lead to the arisal of a market in *silver bullets* as participants *herd* in search of *best practices*, a common set of goods that arises more to reduce the costs of externalities rather than achieve benefits in security itself.

Introduction

In an investigation into security, Adam Shostack posed the question, *what are good signals in the market for security* [1] [2]? In addressing this apparently clear question we find ourselves drawn to the question of *what is security?* One avenue of potential investigation is to ask what the science of economics can provide in answer to this question. In economics terms, security could be a “good” as it is demanded and traded for value. This essay seeks to cast security as a good, and attempts to classify what sort of good it is?

Security is a silver bullet

The Market for Goods, as described by Information and by Party	**Buyer Knows**	**Buyer Lacks *H1***
Seller Knows	Efficient Goods	Lemons (used cars)
Seller Lacks *H2*	Limes (Insurance)	**Silver Bullets (Security)**

- Security is a good
- Security is hard to assess
  - Leads to information insufficiency
- Investment decisions not based on good metrics, but rather on signals
  - Cf. higher education and the market for hiring – how different than this?
- Security is a negative-sum game
- If cost of breaches > cost of products, all parties herd around the same products
  - Anti-incentive to expand them

Ian Grigg – The Market for Silver Bullets
https://iang.org/papers/market_for_silver_bullets.html

Why Information Security is Hard

An Economic Perspective

- Party best-placed to improve security should be incentivized to do so
  - Liability
  - Tragedy of the commons
  - First-mover and network externalities vs. security
  - 3rd party evaluators paid by seller vs. direct user evaluation
- Costs of attack vs. defense
  - “Even a very moderately resourced attacker can break anything that’s at all large and complex”.
- Market forces: end-user security vs. developer pain
- “In an ideal world, the removal of perverse economic incentives to create insecure systems would depoliticize most issues.”

Ross Anderson

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=991552

END