Security & Economics — Part 9
The upshot of what we studied (and what not)

P.-M. Seidel

Fall 2018
Outline
Summary

Part I: Market of security

- Capital investment in security
Summary

Part I: Market of security

- Capital investment in security
- Computational investment in security

we only did this
Summary

Part II: Security of market

- Market as a computational process
  - auctions
  - matching
  - intermediaries

- Information asymmetry

- Network effects
  - positive: self-fulfilling expectations, tipping point
  - negative: minority game

- Social welfare and social choice
Market process

- Ms Alice Dobbs often goes shopping.
  - She seeks buying deals and opportunities.

- She is looking for goods priced below her utility.
  - The total cost must fit into her budget and maximize her utility.

- The sellers decrease their prices in response to buyers’ choices.
  - They seek to clear the market at maximal prices.
Security process

- Mr Bob Dobbs occasionally hacks into a web site.
  - He seeks hacking deals and opportunities.

- He is looking for cyber assets where the amount of effort needed to hack them is smaller than the potential profit.
  - The total effort must fit into Bob’s budget of computing and programming resources, and maximize his utility.

- Security engineers strengthen their protections in response to attackers’ choices.
  - They seek to keep their assets protected at a minimal cost.
Similarities of market and security

- The buyers and the hackers are seeking to solve the same optimization problem.

- The sellers and the security engineers are seeking to solve *dual* optimization problems.
  - the same methods
  - cf. English vs Dutch auctions
Differences of market and security processes

- The market prices are uniformly expressed in terms of money.

- The strength of security protections is expressed in terms of
  - the computational effort and
  - the programming effort

needed to break them.
Security by cryptography

is based on **computational cost**

- Computational cost is *thought to be* a solid foundation for security
  - Cryptanalysis is hard.
  - Computational hardness is a robust measure of effort
  - One-way functions are a tool to impose pricing in computational effort
Security by cryptography

is based on computational cost

- Computational cost is thought to be a solid foundation for security
  - Cryptanalysis is hard.
  - Computational hardness is a robust measure of effort
  - One-way functions are a tool to impose pricing in computational effort

- Cryptography implements the economy of computational effort
Security by obscurity

is based on **programming cost**

- Programming cost is **not thought to be** a solid foundation for security
  - Reverse engineering is easy.
  - Logical hardness of attack derivations is not robust, or not well understood.
Security by obscurity

is based on **programming cost**

- Programming cost is not thought to be a solid foundation for security
  - Reverse engineering is easy.
  - Logical hardness of attack derivations is not robust, or not well understood.

- Nevertheless, the economy of programming cost plays a substantial role both for the hackers and for the security engineers.
Economy of cryptography

balances diverse types of values

- value of secured assets
- computational strength of security protections
- value of the applied cryptographic protections
Claims

- Security is **not** an aspect of economics
- Economics is **not** an aspect of security
Claims

- Security is **not** an aspect of economics
- Economics is **not** an aspect of security

- Economics **is** security
  - An asset is an asset only if it can be secured.

- Security **is** economics
  - A protection is effective only if it is cost effective.
Conclusion

- Security and cryptography are governed by the same forces as the market of goods and services.
Conclusion

- Security and cryptography are governed by the same forces as the market of goods and services.

- It is up to our governments to reconcile their views of security and cryptography with their views of the market:
  - Are they efficient and self-balancing, or inefficient and depression prone?
  - Are the values and technologies global or local?
  - Are centralization and regulation beneficial or harmful?
Diverse answers to these questions can be reasonably supported.

The same answers must be supported for security and for the market.
Tasks

Security: Protect the organization from the world
Economy: Protect the world from the organization