The Economics of Cybersecurity — Lecture 6 Notes

Adam Hastings

January 23, 2024

Project Topics

Have each group briefly describe their class project

Doctrine for Cybersecurity

Three prior doctrines proposed:

- Prevention
- Risk Management
- Deterrence through Accountability

Each with flaws though. What are they?

"Cybersecurity is non-rivalrous and non-excludable" is the justification for the public goods model. *Is this correct though? Since it underpins much of the argument.*

How is (cyber)vaccination a "tragedy of the commons"?

Does "herd immunity" really apply to security these days?

Public health can serve as a guide. Not always a 1-to-1 mapping but can inspire methods:

- Education of professionals/Certification—*How do you do this in a domain that is constantly changing? Attackers are often one step ahead. Kind of dismissed by the industry*
- Law, e.g. introducing liability—*What are the different types?*
- Standards—*What about security theatre?*

0.1 Pros

- Introduces idea of doctrine as a guiding principle

0.2 Cons

- Too much coercion
- Too much loss of privacy
- Security not a public good in many regards
- This paper was pre-Snowdon. Public opinion on government surveillance is different now.
- Patching — sysadmins might not even know about all the systems on their network or how to patch
- Info sharing with government orgs—what do private sector companies get in return? Nothing? Are they supposed to report out of goodness?

Coercion in cybersecurity: What public health models reveal

Interesting to read in light of COVID, which started 3 years after this paper was published.

0.3 Summary

- Review: Doctrines are high-level conceptual frameworks. E.g. MAD during cold war—had goals (deterrence) means (second strike capability), and desired outcomes (prevention of war)
- Doctrines have issues though because unlike in nuclear war, where there is a shared desired outcome (no war), in cybersecurity, there are different parties with meaningfully different goals. E.g. is protection of free speech a cybersecurity outcome? Do we want to still be able to attack other countries? No agreement on means.
- Public health has been proposed as an analogous doctrine for security by many.
- Three points of contention to this view: 1) Security not exactly a public good, 2) Heavily relies on government intervention; many questions about what appropriate government interventions are 3) May involve significant coercion.

    1. Is security really a public good at all?
        - Gives 2x2 matrix of goods which we discussed in first week of class
        - Nature determines rivalrousness but not excludability, which is determined by policy choices. Security (and health) are maybe better described as club goods (excludable, non-rival) via e.g. vaccine passes and quarantines.
    2. Public health model glosses over the key role of government in providing public goods.

    - Public goods are often underprovisioned in the marketplace (free riding, tragedies of the commons).
    - Governments are often seen as the ones to ensure proper production of public goods. This can be done via education, monitoring, or coercion.
    - E.g. mandatory reporting
    - What level of coercion should be exerted? Not clear.
    - Economic models exist, but rely on variables that are hard or impossible to measure in practice.

  3. Neglects how important coercion has been in major public health achievements
    - Examines how disease control, automobile safety, smoking, and obesity have been addressed through various levels of coercion.
    - Health offices have requires mandatory reporting (of e.g. tuberculosis), mandatory vaccination, surveillance, enforced quarantines
    - Justified by literal saving of lives. Very quantifiable. Might not be the case in cybersecurity!
    - Levels of coercion in e.g. automobile safety (seatbelts, BAC limits) are already a restrained balance. But were eventually accepted because less coercive measures (e.g. public education) failed to have adequate impact.

- To summarize: public health has been proposed as a doctrine for security, but Weber claims these deteriorate under scrutiny. If we want to follow these metaphors, it's going to require a greater coercive authority.

0.4 Pros

- Adds to the discourse. Challenges common assumptions.

0.5 Cons

- Rambling! Doesn't forcefully state the point. Needs to summarize sections or something
- No data to back up points (but fun citations—Rosseau 1762!)

A New Doctrine for Hardware Security