CE879 - Information Security Mng. & Eng.

Lecture 10: Introduction to Cybersecurity Governance

Seyedeh Atefeh Musavi / Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology
Spring 1404

S4Lab

Acknowledgments: Some of the slides are fully or partially obtained from other sources. A reference is noted on the bottom of each slide to acknowledge the full slide or partial slide content.

Internet, smart or dumb?

S4Lab

- “Smart” networks offer sophisticated services that can be delivered to very simple end-user devices on the “edge” of the network.
- Other networks are “dumb” — they offer only a very basic service and require that the end-user devices are intelligent.
- Centralized innovation means slow innovation. It also means innovation directed by the goals of a single company. As a result, anything that doesn’t seem to fit the vision of the company that owns the network is rejected or even actively fought.
- Surprisingly, then, “dumb” networks are the smart choice for innovation and freedom.

[Why Dumb Networks Are Better, Andreas M. Antonopoulos, Medium, 2016]

Permission less model

S4Lab

- The Internet is a dumb network, which is its defining and most valuable feature.
  - The Internet's protocol (transmission control protocol/Internet protocol, or TCP/IP) doesn't offer "services." TCP/IP acts as an efficient pipeline
  - It doesn't make decisions about content.
  - It doesn't distinguish between photos and text, video and audio.
  - It doesn't have a list of approved applications.
  - It doesn't even distinguish between client and server, user and host, or individual versus corporation.
  - Every IP address is an equal peer.
- So the dumb network becomes a platform for independent innovation, without permission, at the edge.
- Simultaneously this permission less design certainly affects the security.

[Why Dumb Networks Are Better, Andreas M. Antonopoulos, Medium, 2016]

Ownership challenge

S4Lab

- Complicated legal “edge cases” around ownership of (e.g. IP addresses) are minor exceptions.
- What risks are mitigated, accepted or externalized is driven first and foremost by the incentives of the owner.
  - So institutional mechanisms might constrain or otherwise shape these incentives.
- One could basically call this a property rights approach to security governance.
  - Ownership is a conceptually straightforward starting point for thinking about governance.
- So why governance is so complicated, or in some ways, absent:
  - Because ownership is extremely distributed across an interdependent global ecosystem of resources, systems, and services.

[Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. Van Eeten, M., Digital Policy, Regulation and Governance, 2017]

Ownership challenge

S4Lab

- Complicated legal “edge cases” around ownership of (e.g. IP addresses) are minor exceptions.

A common belief:

Internet is a “global digital commons” or “public good”.

The fact:

Nearly every resource, system or service is someone’s private property.

- So why governance is so complicated, or in some ways, absent:
  - Because ownership is extremely distributed across an interdependent global ecosystem of resources, systems, and services.

[Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. Van Eeten, M., Digital Policy, Regulation and Governance, 2017]

Shifting property rights

S4Lab

from users to internet intermediaries

Schneier has observed that two recent developments are impacting the authority of owners of nodes:

- The rise of cloud computing.
- More of our data and computing takes place on the networks of others, rather than on our own node.
- Obvious examples are Gmail, Salesforce, Amazon elastic cloud compute, Facebook, Uber, Spotify, Office 365, Dropbox, etc.

- Vendor-controlled platforms.
- More and more of our devices are closed down, or at least less open than general-purpose computers, and controlled by vendors.
- Vendors limit what users can do with their devices, i.e. What code they can run.

[Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. Van Eeten, M., Digital Policy, Regulation and Governance, 2017]

Shifting property rights

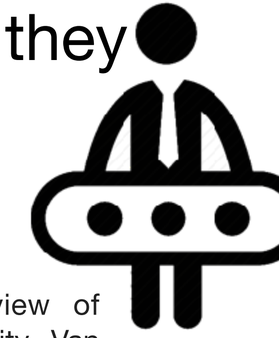
S4Lab

from users to internet intermediaries

Schneier has obs… are impacting the authority …

- The … s.
- M… s are … pen … rs,
- … Al… do with Face… ode they Dropbox, …

- Sometimes these companies are referred to as internet intermediaries.
- Their security practices determine to an increasing degree the security of everyone.
- In many cases, we do not really have a good way to evaluate what they are doing.



[Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. Van Eeten, M., Digital Policy, Regulation and Governance, 2017]

Feudal security

S4Lab

- Now that the IT industry has matured, we expect more security “out of the box.”
- We cede control of our data and computing platforms to these companies and trust that they will treat us well and protect us from harm.
  - We become their vassals; or, on a bad day, their serfs.
- Feudal security also has its risks. Vendors can act arbitrarily, against our interests.
- The feudal relationship is inherently based on power.
- In Medieval Europe, people would pledge their allegiance to a feudal lord in exchange for that lord’s protection. This arrangement changed as the lords realized that they had all the power and could do whatever they wanted. Vassals were used and abused; peasants were tied to their land and became serfs.

[You Have No Control Over Security on the Feudal Internet, Bruce Schneier, Harvard Business Review, 2013]

Feudal security 2

S4Lab

- How do we survive?
- Increasingly, we have little alternative but to trust someone, so we need to decide who we trust — and who we don't — and then act accordingly.
- On the policy side, we have an action plan.
  - In the short term, we need to keep circumvention — the ability to modify our hardware, software, and data files — legal and preserve net neutrality.
  - In the longer term, we all need to work to reduce the power imbalance. Medieval feudalism evolved into a more balanced relationship in which lords had responsibilities as well as rights.
- Regulations do change the scene.

[You Have No Control Over Security on the Feudal Internet, Bruce Schneier, Harvard Business Review, 2013]

Limitations on property rights of owners

S4Lab

- Another trend is the growing number of regulatory constraints on the property rights of device owners.
- This is mainly happening in sectors that were already strongly institutionalized and regulated, such as health, energy, financial services, and transportation.
- Slowly but surely, though, security standards are being recommended or mandated in these sectors.
- Many of these standards are process-based (“adopt adequate safeguards”), rather than mandating specific technical security measures.

[Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. Van Eeten, M., Digital Policy, Regulation and Governance, 2017]

Limitations on property rights of vendors

S4Lab

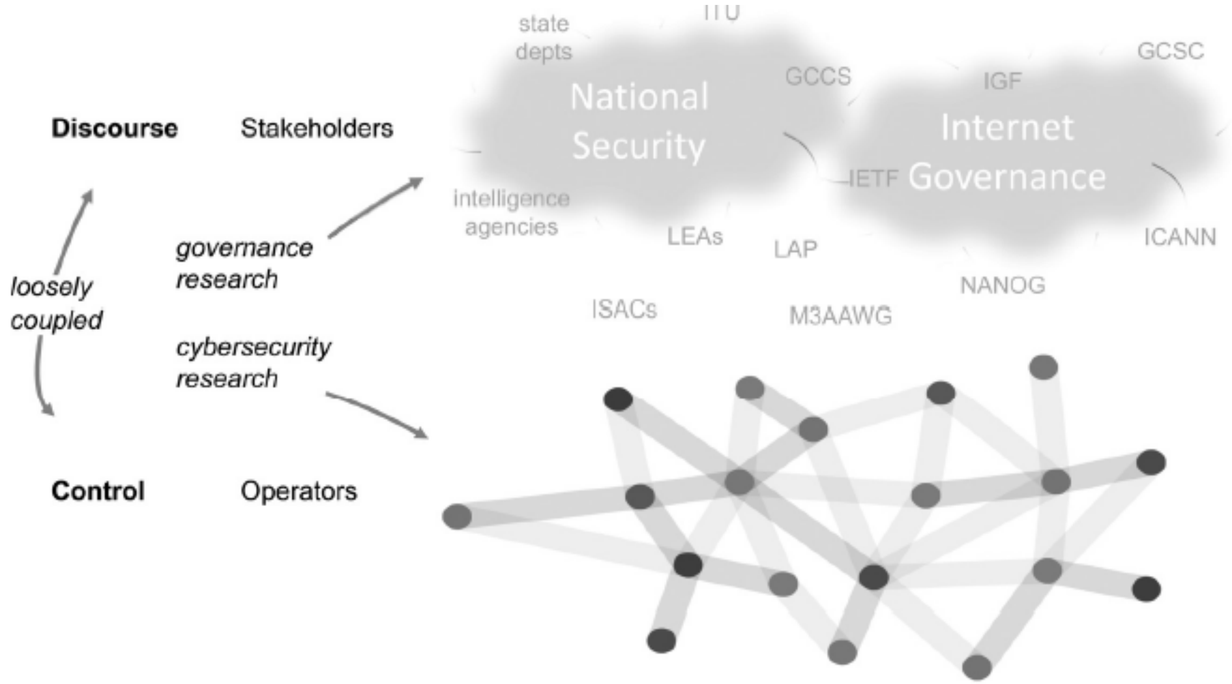
- The last shift in security governance to highlight here is changes in the property rights of vendors.
- Conventionally, software and hardware vendors put their products into the market without requirements in terms of how they were secured.
- Users, whether corporate or consumer, have to accept End User License Agreements (EULAs) to be able to use the product.
- This is not without benefits in terms of innovation (“go fast and break things”), but the downside is that time-to-market and other economic incentives have often trumped security.
- Some cases for such trend are:
  - Dutch consumer union (Consumentenbond) took Samsung to court for failing to release security patches for even recent phones.
  - Another case, Samsung rolled out a software update that prevented the phones not returned in the “Note 7 recall” from charging, rendering it completely unusable.

[Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. Van Eeten, M., Digital Policy, Regulation and Governance, 2017]

Multiple players

S4Lab

- There isn't a complete coupling between governance institutions and operation at resources connected to the internet.
  - ICANN and OpenDNS
  - IETF and ignored RFCs
- Governance research is heavily focused on the top of the figure, cybersecurity research on the bottom.
- The discourse and control are only loosely coupled reflects a particular political economy, where many states have not imposed wide-ranging hierarchical control.
- This particular arrangement is contingent and might change over time.

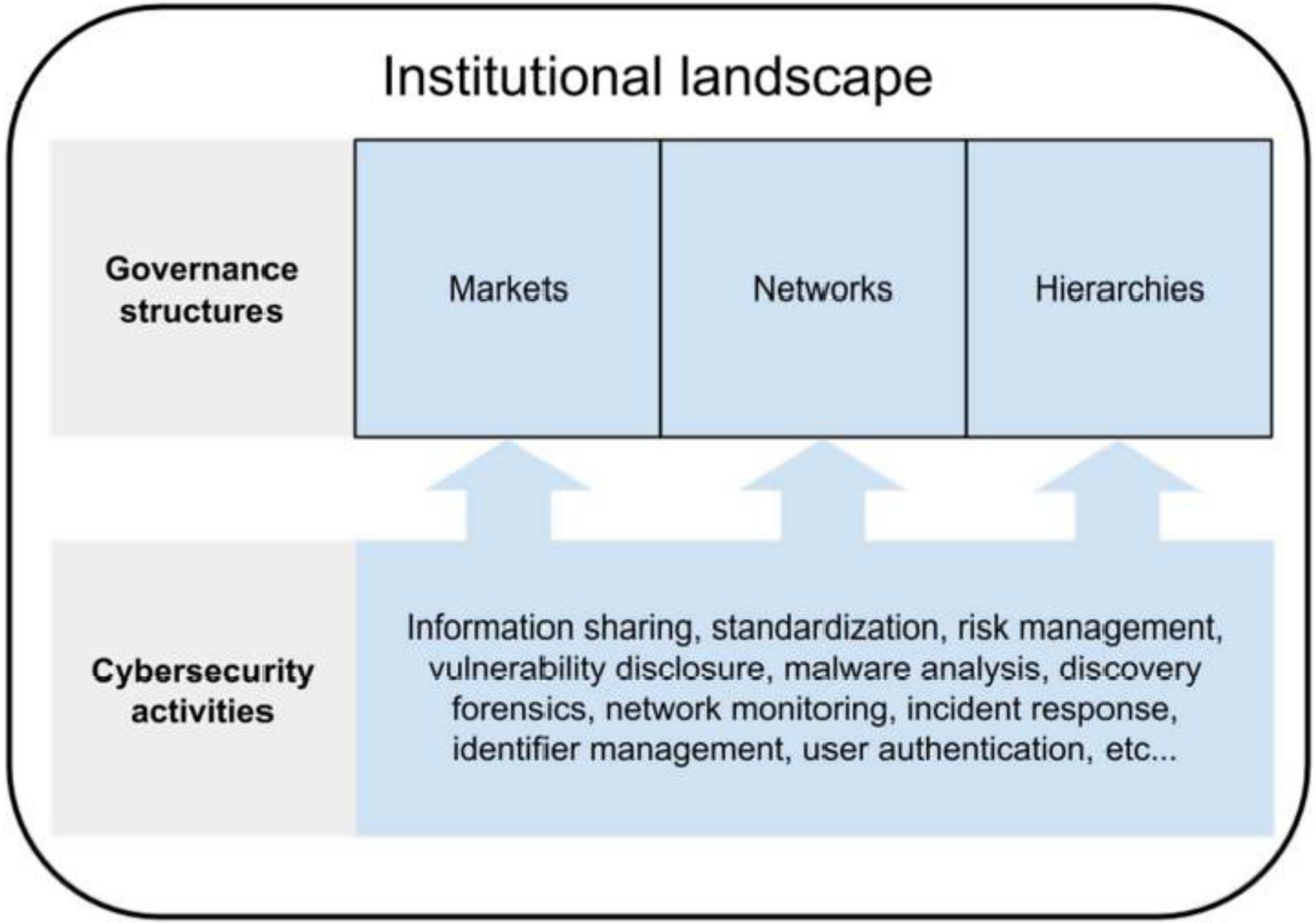


[Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. Van Eeten, M., Digital Policy, Regulation and Governance, 2017]

A general overview to cyber security governance

S4Lab

- We will talk more on these structures in the following lectures.



[Mapping the cybersecurity institutional landscape, Kuerbis, B., & Badiei, F., Digital Policy, Regulation and Governance, 2017]