Architecture, Economics and the Value of Security for Things

Jari Arkko
Senior Expert
Ericsson Research

What this talk is and is not

- We could talk about the details of IOT protocols and systems
- But we’re not going to — trying to focus on the big picture instead:
  - Reasons for working with security
  - What generates the value of IOT systems for the user
  - Or the mankind
  - What generates the downsides, e.g., value for an attacker

Picture source: ioti

Reasons for security?

- This?

- This?

- Or this?

Picture sources: datafloq, thehackernews, study

Reasons for Security?

- The traditional perspective on this relates to, e.g., guaranteeing that your systems are available for your use and your data is kept confidential
  - And limiting how many entities have control over you

- But the Internet is an interconnected system and its vulnerable parts may be used in attacks to harm other parts of the Internet

- We need to look at the impacts on not just individuals but also the commons, i.e., the Internet as whole.

Economics of Networking

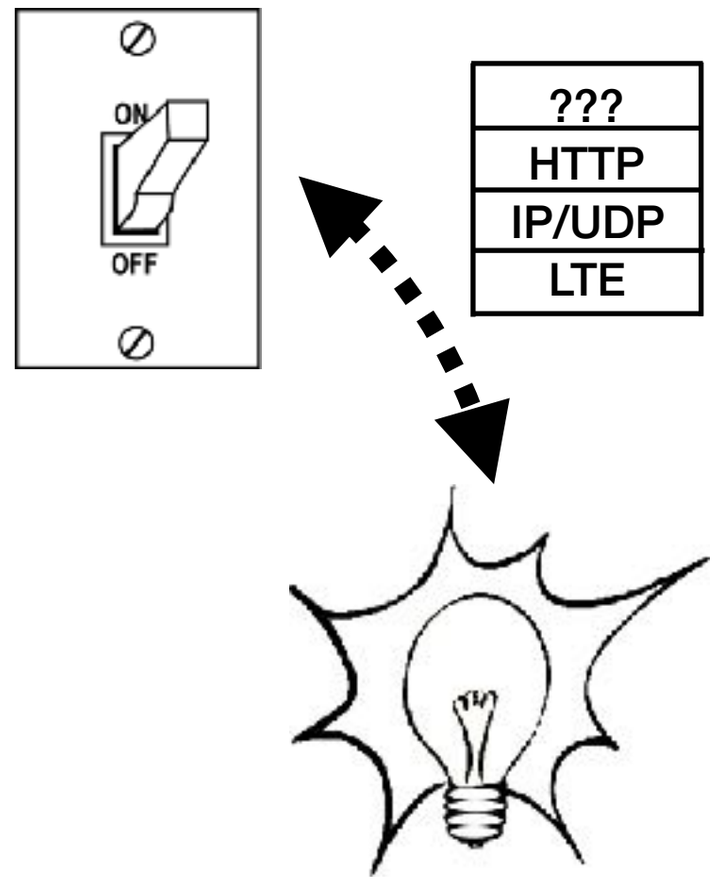
- **Metcalfe's law** states that the value of a network is proportional to the square of the number of connected users of the system

- **Reed's law** suggests that the utility of a network scales even exponentially with the number of users, on the grounds that there is an exponential number of possible subgroups of users

- **Beckström's law** looks at the added value that transactions performed over the network generate, minus costs related to securing the system and attacks that happened despite the security.

Do These Apply to IOT?

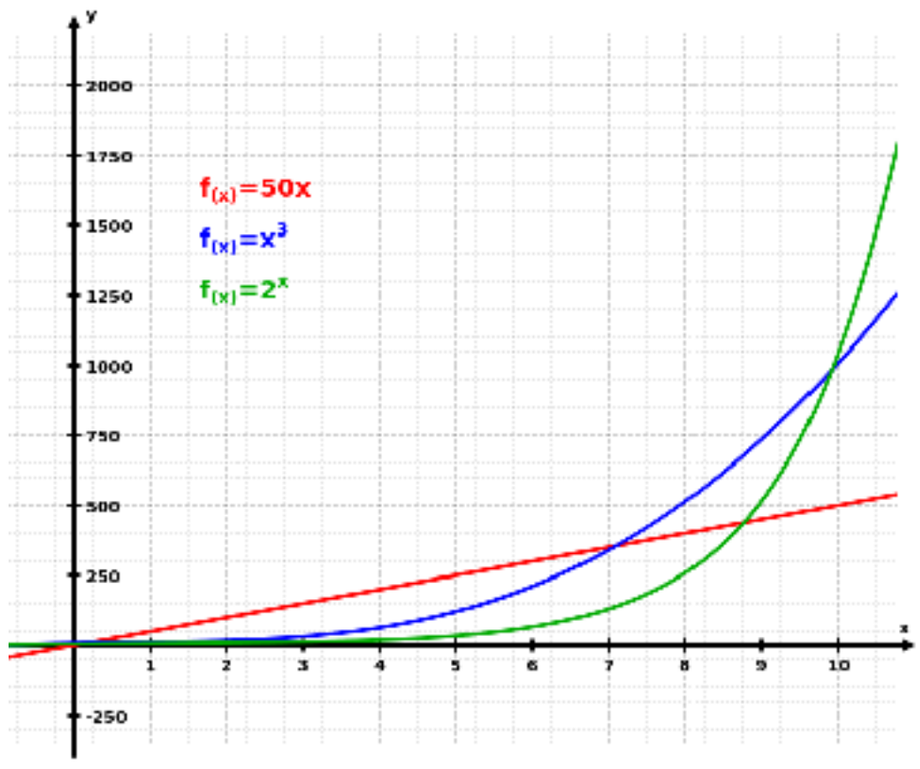
- Not clear generic laws apply to closed IOT systems
- Having the ability to use one network for all these different systems is an example of the network effects, however
- Metcalfe's law and humans interacting with each other vs. silos of IOT applications
- Interoperability and open data increase value for the humankind



What about Economics of IOT Security?

- Even assuming full interoperability, not all IOT devices may have a reason to talk to each other

- But I fear that for attackers, the economics are far more attractive — a hijacked device can be used to attack anything



What about Economics of IOT Security?

- **Law I (Eflactem's law) — value for attacker**: The cost of attacks from a group of nodes grows proportional to the size of the group times the nodes in the entire Internet

- **Law II — value of interoperable IOT**: The value of a network of application nodes grows proportional to the square of nodes having an ability to participate

- Value needs to exceed cost!

    - Costs and and value may go to different entities

    - Decrease # of vulnerable nodes, limit ability to take down centralised Internet services, increase value

Minimal Security Requirements for IOT Nodes

- Protect the Internet commons, new devices should not be an additional burden in terms of vehicles of attack towards the rest of the Internet
  - Not hackable e.g., via default passwords (duh!)
  - Not usable as reflectors; updatable; maintained through lifetime
- Requiring that devices are safe for the purpose of the application they were made for

You Are Going to Order Us to Do WHAT???

- Can anyone set requirements? Standards organisations?
- Internet is based on voluntary co-operation
- We can document best practices and recommendations
- Self-interest needs to drive the rest, and there are good reasons for manufacturers to avoid recalls, higher insurance premiums, even liability

Summary

- It is very easy to add more nodes to the Internet
- Sometimes that comes back to bite us
- IOT security is not just about the protecting the application and user, it is also about protecting the rest of the Internet
- Sticking to some basic minimal security requirements for IOT devices would take us a long way for avoiding these problems