(How) Does Internet Policy Influence Innovation?

Jari Arkko*

Chair, Internet Engineering Task Force (IETF)

Expert, Ericsson Research

*) Speaking as an individual & this presentation contains forward looking statements

Outline

- The role of the engineers & innovators
- Examples of influence and other reactions
  - Past, present, and future
  - Pervasive monitoring as an example
- Conclusions

Role of the Innovators – the Theory

- Engineers and businesses create new possibilities
- Individuals and organisations decide how to employ those possibilities
- Standards should be largely indifferent to policy choices (e.g., DNS protocol vs. gTLD allocations)

But ...

- Engineers need to be aware of different deployment models and policies
- Those who set policies should be aware of technical limitations and implications of their policy choices

Add a Dose of Reality…

- Interaction between parties is often insufficient
- Various entities have different opinions
- Engineers routing around policy damage
- Policies routing around technical deficiencies

Example: Pervasive Monitoring

Pervasive = all encompassing
Monitoring = surveillance

Last year's allegations about NSA etc.
(but also a wider issue around the world)

Not a surprise as such, but the scale and tactics have been surprising

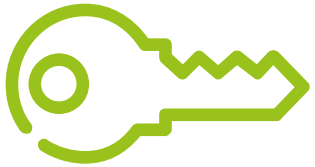
An interesting case study where policy matters have caused technology changes, yet there has been significant disagreements about policies

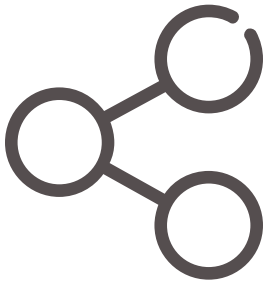
The Allegations Painted a Depressing Picture

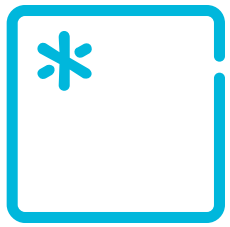
- Store-everything-and-search-later surveillance
- Everything that anybody does is recorded
- Encrypted traffic can be read as well as cleartext
- Agents plant vulnerabilities in standards

Likely Vulnerabilities To Be Exploited

- Unprotected communications (duh!)
- Communications within cloud
- Direct access to the peer
- Direct access to keys (e.g., lavabit?)
- Third parties (e.g., fake certs)
- Implementation backdoors (e.g., RNGs)
- Vulnerable standards (e.g., Dual_EC_DBRG)







Reactions

- Many reactions from all directions
- Many useful discussions – but I will only talk about the reaction from the technical community
- (Note that there has also been reactions that have no direct relationship to monitoring activities)

How Should the Engineers React?

We've Been Here Before

Various entities and agreements pushed for no or weak encryption in 1990s and 2000s, but IETF discussion led to:

- 1996 – encryption is an important tool: RFC 1984
- 2000 – not consider wiretapping: RFC 2804
- 2002 – use strong encryption: RFC 3365

Role of Engineers

- The technical community is not the place to have a political discussion
- And there are differing opinions in the political world
- But engineers MUST understand what dangers in general face Internet traffic
- And SHOULD have an idea how Internet technology can become more secure

Engineering View of Current Issues

- We think of monitoring as a technical attack, or at least indistinguishable from one
- Retrieved information could be used for good or bad
- It is difficult to leave security vulnerabilities into technology for just some entities
- Vulnerabilities tend to “democratize” over time

Ongoing Technical Activity

Many online services are deploying secure service at an accelerated pace (cf. EFF report)

There is general desire in the IETF to employ more and better security technology

Of course, balanced with the need to manage and operate networks

Limits of Technology

- Technology may help - to an extent - although it does not help with communications to an untrusted peer
- Prevent some attacks, make getting caught more likely, shift attacks from wholesale to targeted, …
- Attention makes this an opportunity as well

Some Directions for Protection

- Protect unprotected communications!
- Math and good crypto
- Standards
  - New technology
  - Public, broad review of standards
- Implementation backdoors
  - Diversity
  - Open source

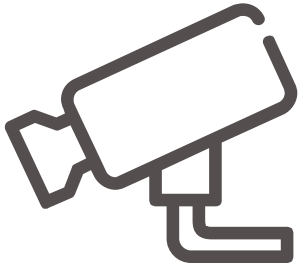
What Is the IETF Doing?

- Discuss the topic - openly
  - E.g., IETF-88 technical plenary
- Work on the problem & threats
- Specific proposals, such as TLS algorithms & PFS
- Ongoing bigger efforts (started earlier)
- Starting to understand the difficulties as well

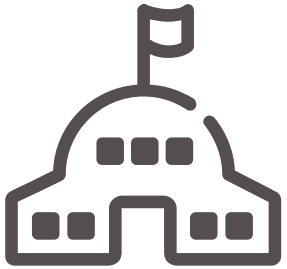
Some High-Interest Efforts

- Various services turning on TLS far more in recent years than before -- this trend will now accelerate
- Role of security in HTTP 2.0
- Applications (IM, E-mail; UTA WG)
- TLS 1.3

Challenges



- E-mail: end-to-end security
- Web: proxies and CA lists
- Endpoint and operating system security
- “National Internet” model for the Internet future

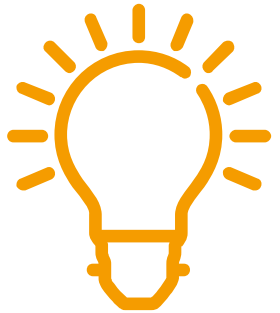


Opportunities

Internet technology is evolving fast - future is defined today

An opportunity to improve the security of the Internet

Initial actions are mostly about deploying already existing technology, but could be a need for deeper changes as well



Other Examples of Interaction Between Policy and Innovation

- Whitespace radio frequency management
- Emergency call technology
- Secure VoIP caller identification

Typical Interaction Issues

- The Internet and regulator/policy worlds need to discuss with each other
- Understanding the requirements
- Global vs. local solutions
- Ability to refer to Internet-age standards

Other Examples of Interaction Between Policy and Innovation

- Whitespace radio frequency management
  - PAWS working group
  - Interface from an access point to a regulatory body
  - Need for regulators and the IETF to interact

Other Examples of Interaction Between Policy and Innovation

- Emergency call technology
  - ECRIT working group
  - Emergency communication is highly regulated
  - Need one technology for the world

Other Examples of Interaction Between Policy and Innovation

- Secure VoIP caller identification
  - STIR working group
  - Important for reducing robocalls, vishing, swatting
  - Another highly regulated area
  - Also needs more policy – engineer interaction

Potential Future Questions

- Could new technology remove policy bottlenecks?
- Signed data vs. trustworthy data distributors
- Single authority vs. cryptographic authority (e.g., k-of-n)
- Engineers should not drive policy, but should make technology available
  - DNSSEC, DANE, TLS, …

Final Words

- Interaction between policy, governance, and technical worlds is not easy
- Most fruitful interaction runs both ways
- Difficult policy questions and conflicts are painful, but also an opportunity
- Engineers have a role in some policy/society issues
- IETF is realizing a need to talk to the policy world

Welcome to London!
March 2-7, 2014

HTTPBIS, TLS, UTA, IAB STRINT workshop, STIR, PAWS, ECRIT, and many other interesting meetings

Thank you