Tackling Internet Challenges

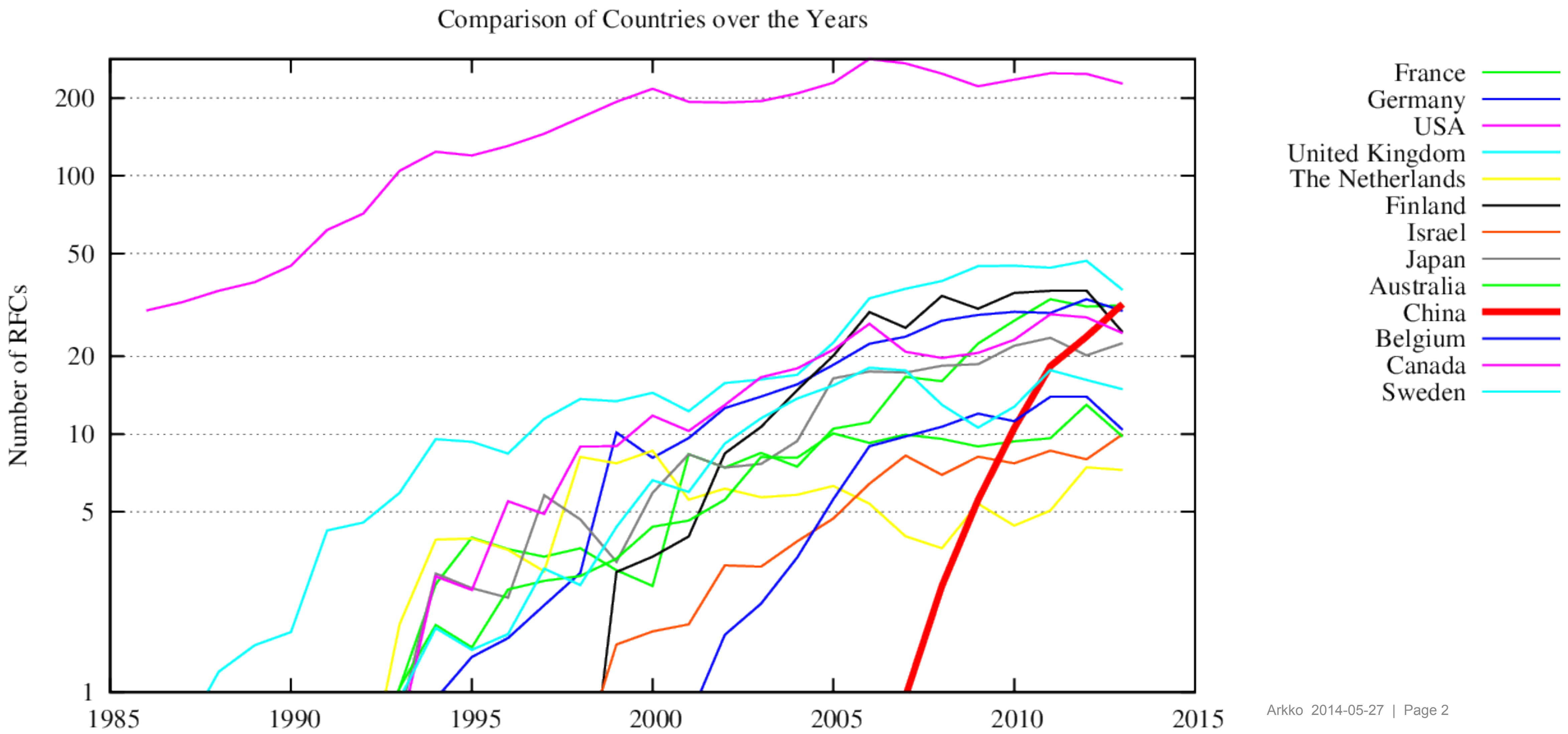
Jari Arkko

Chair, IETF

Expert, Ericsson Research

Kauniainen, Finland

A Small Side-Tour: Sources of Internet Standards



Goals for This Talk

- Understanding the trends in Internet evolution
- Learning from the history
  - Why did the Internet succeed?
- Current challenges and changes
  - Surveillance, smart objects, real-time communications, …
- Evolution of the web protocol stack

Current Challenges

- Internet privacy
- Networked society
- Real-time communications

IETF’s role in remaking the web protocol stack

Questions Around the Challenges

- Can we protect privacy better?
- How is technology evolving due to security worries?
- How can the Internet scale to connecting all things?
- How is technology evolving to support smart objects?
- How can we integrate real-time communications to the rest of the Internet experience?

Some Technology Trends Related to These Challenges

- The web is a key component
- Faster evolution of the web
- Web as a platform for small devices
- Increased use of secure web connections (https, TLS)
- Internet address space (IPv6)

☑

Privacy

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

Targeted vs. wholesale surveillance
Database vs. communications access

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

[these are all claims, of course – may not be true]

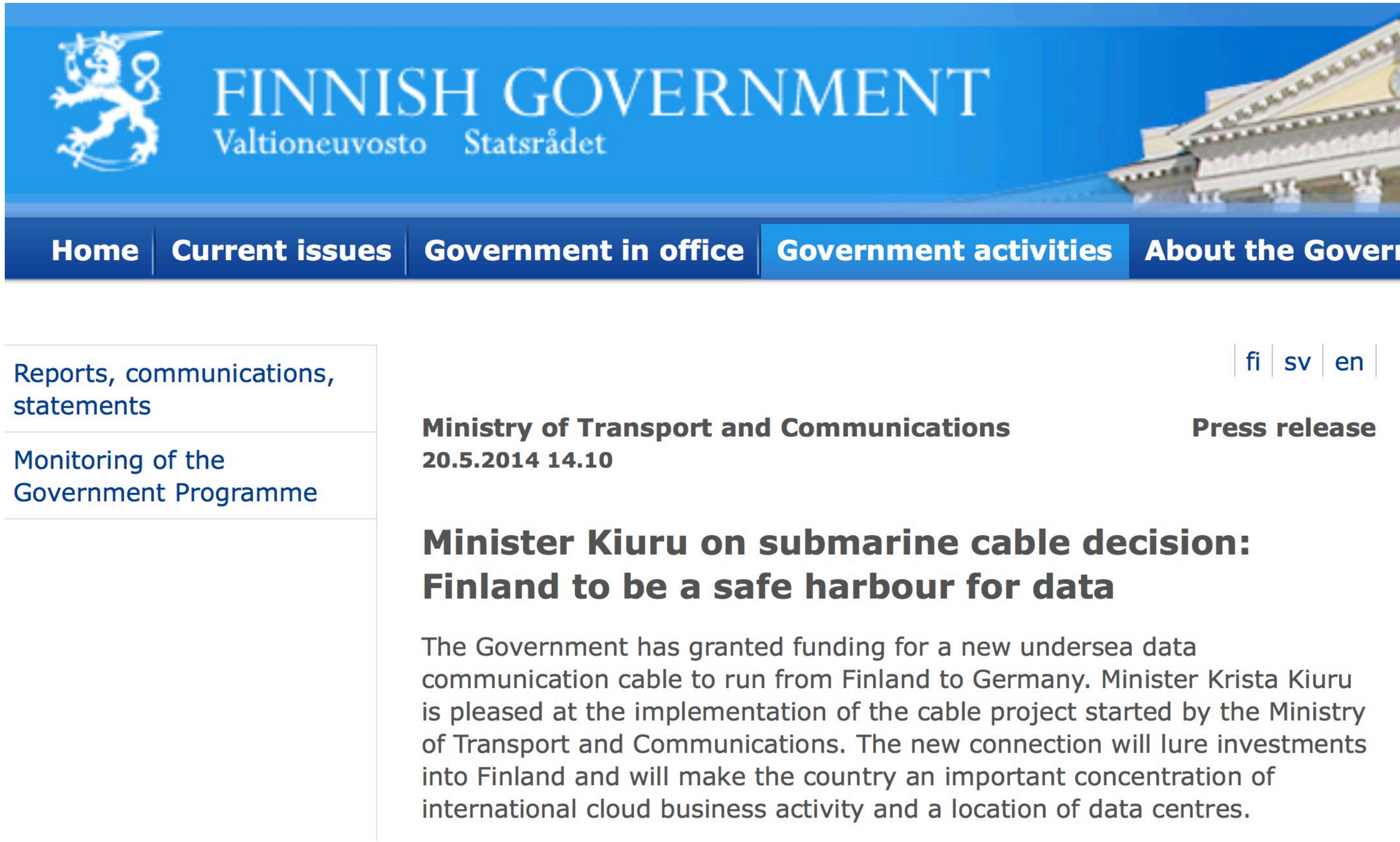
Likely Vulnerabilities To Be Exploited

- 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)

Example Reactions

- Initiatives for operational improvements
- Calls for more “national” Internets
- NSA-envy
- Service providers showing they are secure
- Engineers wondering what they should do

Initiatives for Operational Improvements



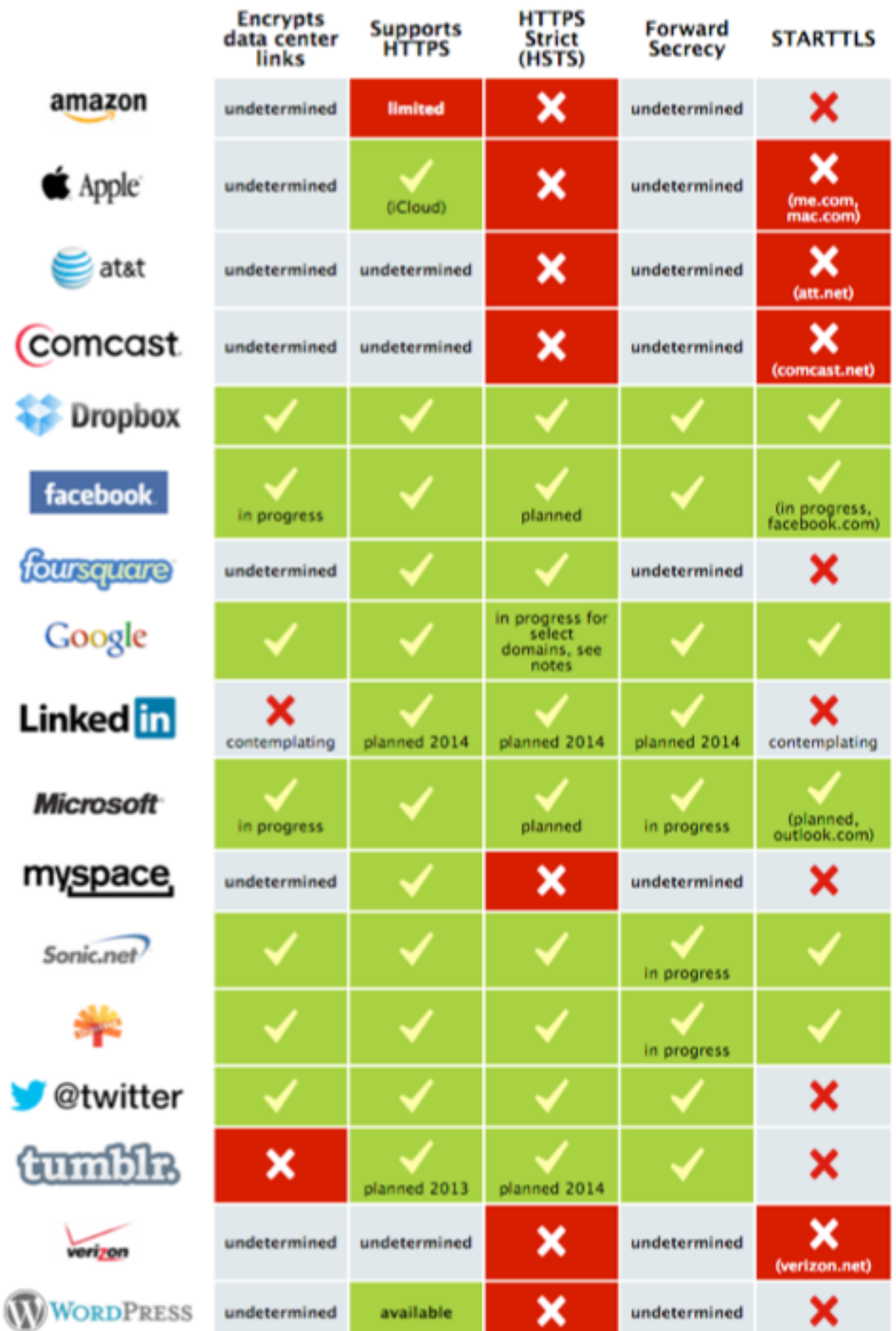
Ministry of Transport and Communications **Press release**
20.5.2014 14.10

Minister Kiuru on submarine cable decision: Finland to be a safe harbour for data

The Government has granted funding for a new undersea data communication cable to run from Finland to Germany. Minister Krista Kiuru is pleased at the implementation of the cable project started by the Ministry of Transport and Communications. The new connection will lure investments into Finland and will make the country an important concentration of international cloud business activity and a location of data centres.

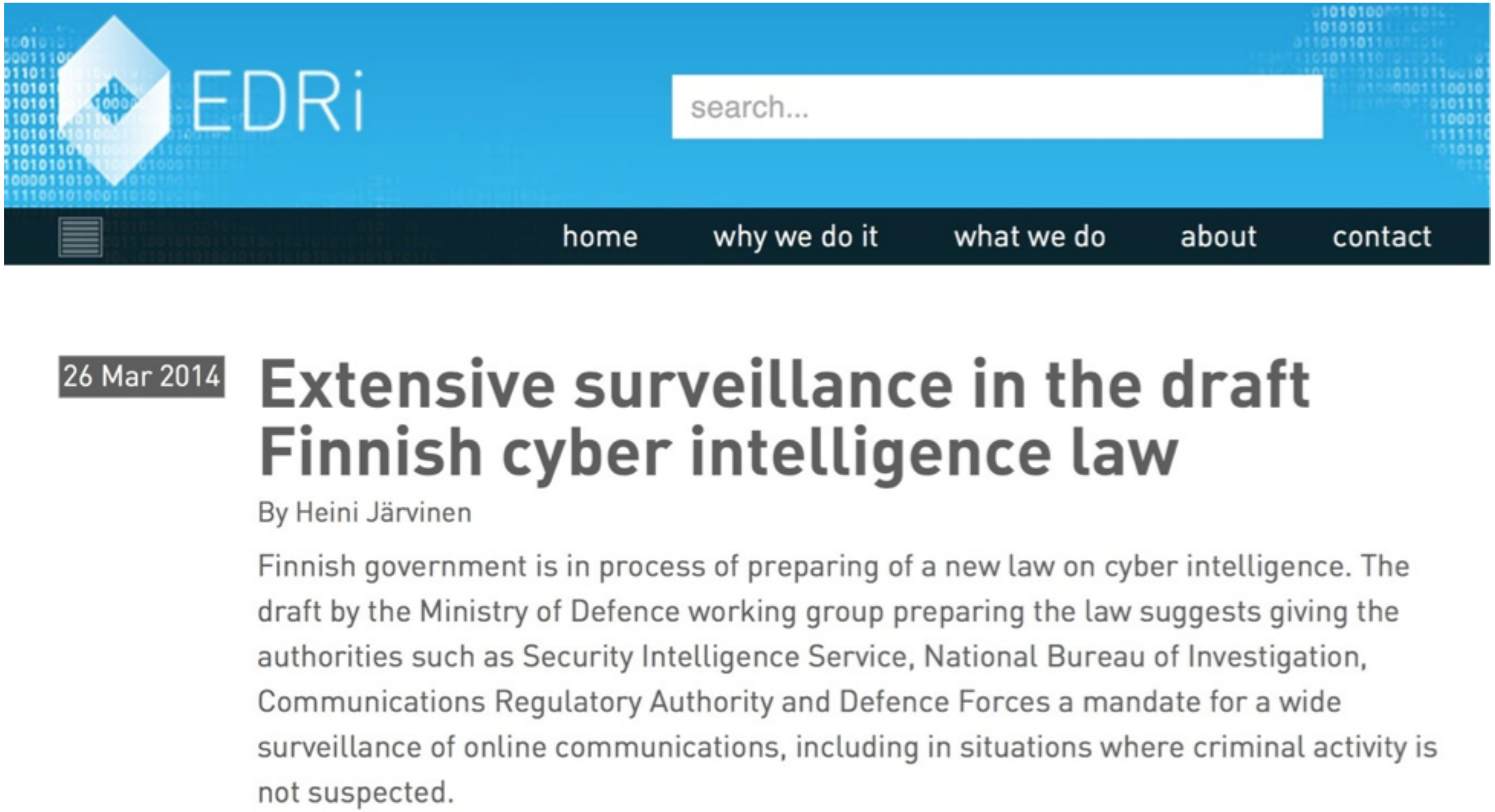
Service Providers Showing They Are Secure

The “https:” trend



	Encrypts data center links	Supports HTTPS	HTTPS Strict (HSTS)	Forward Secrecy	STARTTLS
amazon	undetermined	limited	✗	undetermined	✗
Apple	undetermined	✓ (iCloud)	✗	undetermined	✗ (me.com, mac.com)
at&t	undetermined	undetermined	✗	undetermined	✗ (att.net)
comcast	undetermined	undetermined	✗	undetermined	✗ (comcast.net)
Dropbox	✓	✓	✓	✓	✓
facebook	✓ in progress	✓	✓ planned	✓	✓ (in progress, facebook.com)
foursquare	undetermined	✓	✓	undetermined	✗
Google	✓	✓	in progress for select domains, see notes	✓	✓
LinkedIn	✗ contemplating	✓ planned 2014	✓ planned 2014	✓ planned 2014	✗ contemplating
Microsoft	✓ in progress	✓	✓ planned	✓ in progress	✓ (planned, outlook.com)
myspace	undetermined	✓	✗	undetermined	✗
Sonic.net	✓	✓	✓	✓ in progress	✓
	✓	✓	✓	✓ in progress	✓
@twitter	✓	✓	✓	✓	✗
tumblr.	✗	✓ planned 2013	✓ planned 2014	✓	✗
verizon	undetermined	undetermined	✗	undetermined	✗ (verizon.net)
WordPress	undetermined	available	✗	undetermined	✗

NSA-Envy



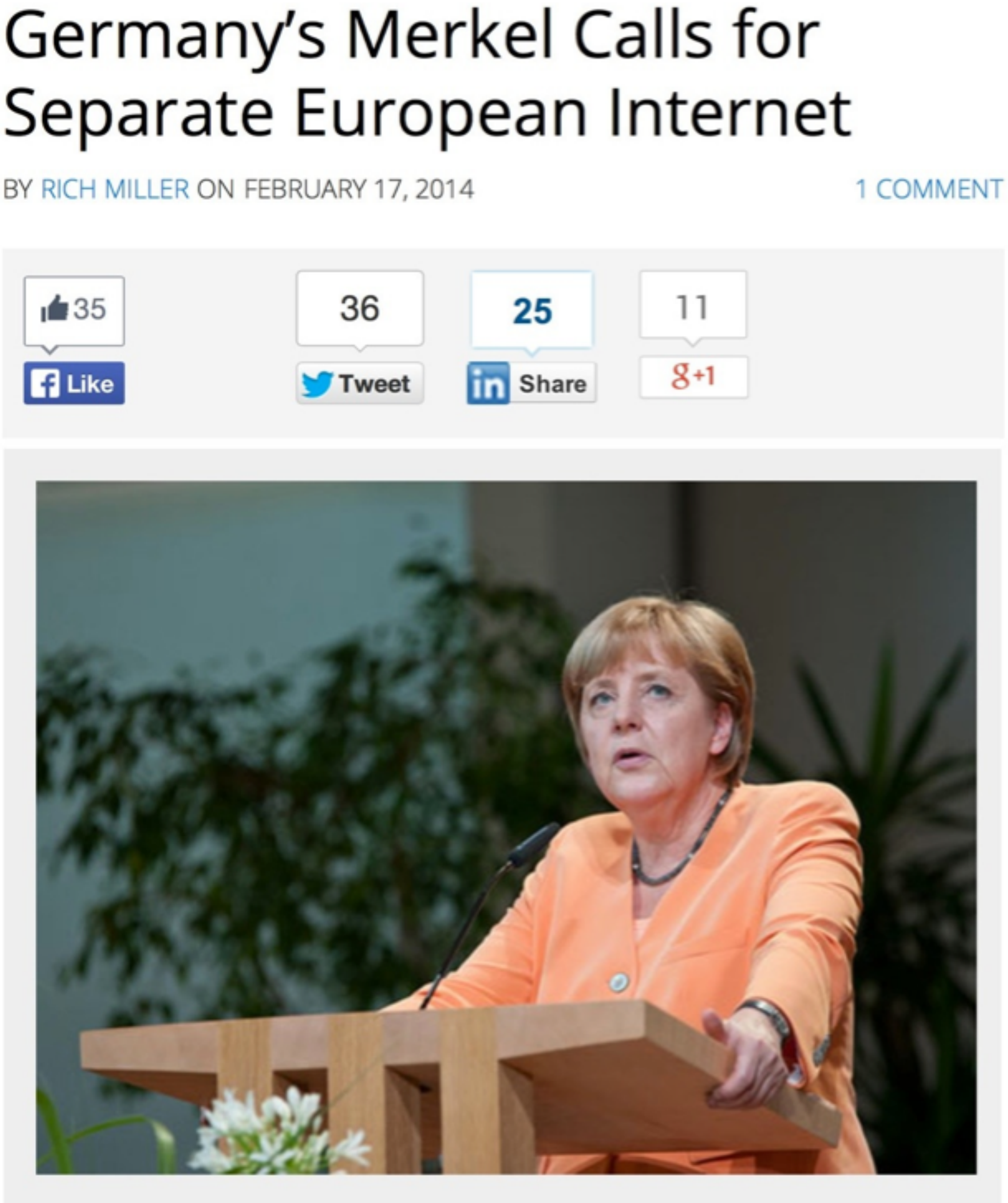
26 Mar 2014

Extensive surveillance in the draft Finnish cyber intelligence law

By Heini Järvinen

Finnish government is in process of preparing of a new law on cyber intelligence. The draft by the Ministry of Defence working group preparing the law suggests giving the authorities such as Security Intelligence Service, National Bureau of Investigation, Communications Regulatory Authority and Defence Forces a mandate for a wide surveillance of online communications, including in situations where criminal activity is not suspected.

Calls for National “Internets”



Germany’s Merkel Calls for Separate European Internet

BY RICH MILLER ON FEBRUARY 17, 2014 1 COMMENT

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 @ IETF

- We think of monitoring as a technical attack, or at least indistinguishable from one (RFC 7258)
- 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

Limits of Technology

- Technology may help - to an extent - although it does not help with communications to an untrusted peer
- Pervasive monitoring worries have energized IETF folk to work on security & privacy issues

Some Directions for Protection

Protect unprotected communications!

Math and good crypto

Standards

- New technology
- Public, broad review

Implementation backdoors

- Diversity
- Open source

What Is the IETF Doing?

- Various services turning on https 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

New in HTTP/2.0

- Key goal is to provide better efficiency
- And to promote more TLS usage
- TLS not mandatory but some browsers require it
- May allow the use of TLS for http:
  - Does the TLS mode for http reduce https deployment?
  - The trend for more https/TLS decreases the ability to do caching/scanning as well as spying

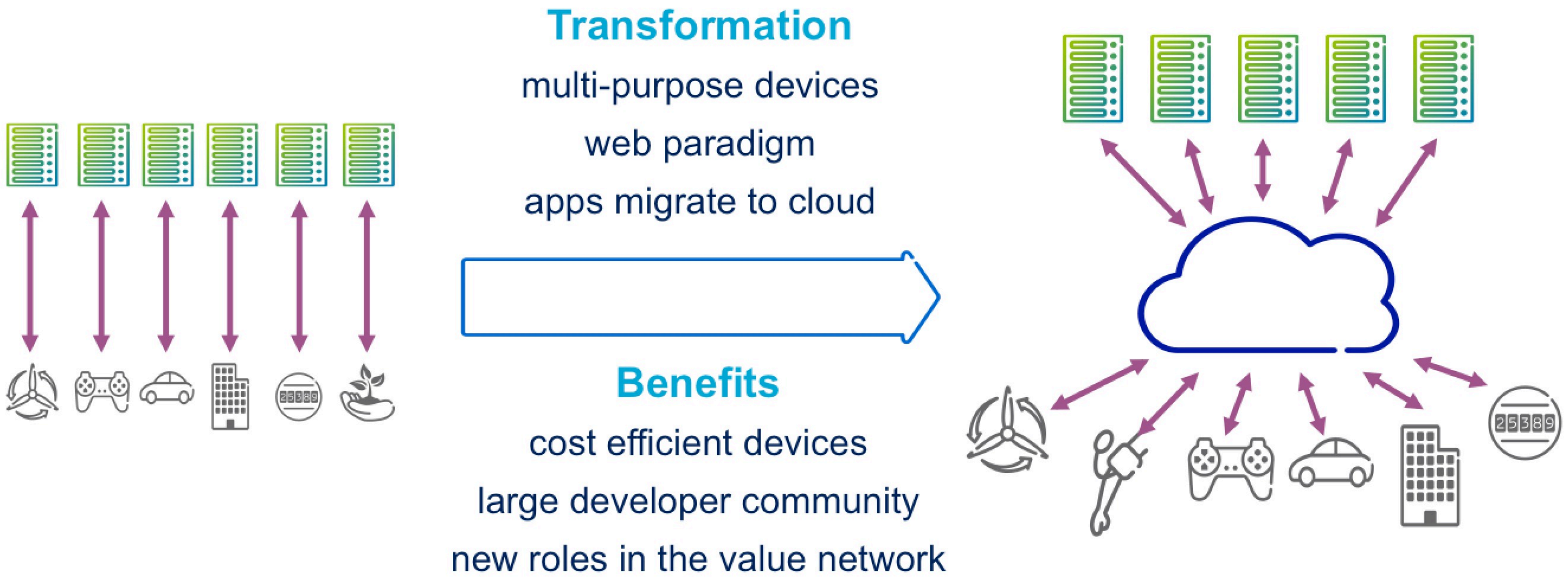
Networked Society

Networking the Society

- Everything that benefits from being connected, will be
- Gadgets, cars, buildings, equipment, even clothes and materials, …
- 50B or 500B devices?
- How to do this?

Trends in Smart Objects

- Vertical applications are very expensive to build
- Legacy devices are moving to IP
- The key is general purpose technology (4G, WLAN, web)



Transformation

multi-purpose devices

web paradigm

apps migrate to cloud

Benefits

cost efficient devices

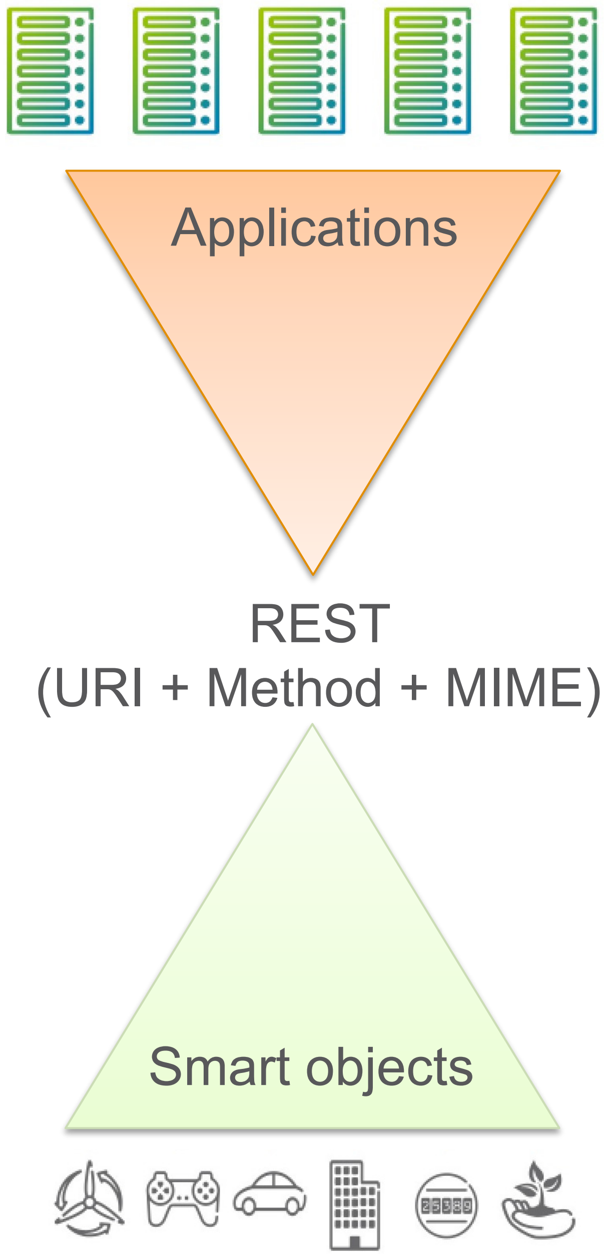
large developer community

new roles in the value network

The Web of Things

An attractive development model:

- Very successful elsewhere
- Widely available tools
- Millions of programmers
- Simple and well-defined
- “Permissionless innovation”



The IP API as the common open interface to the network

Permissionless Innovation

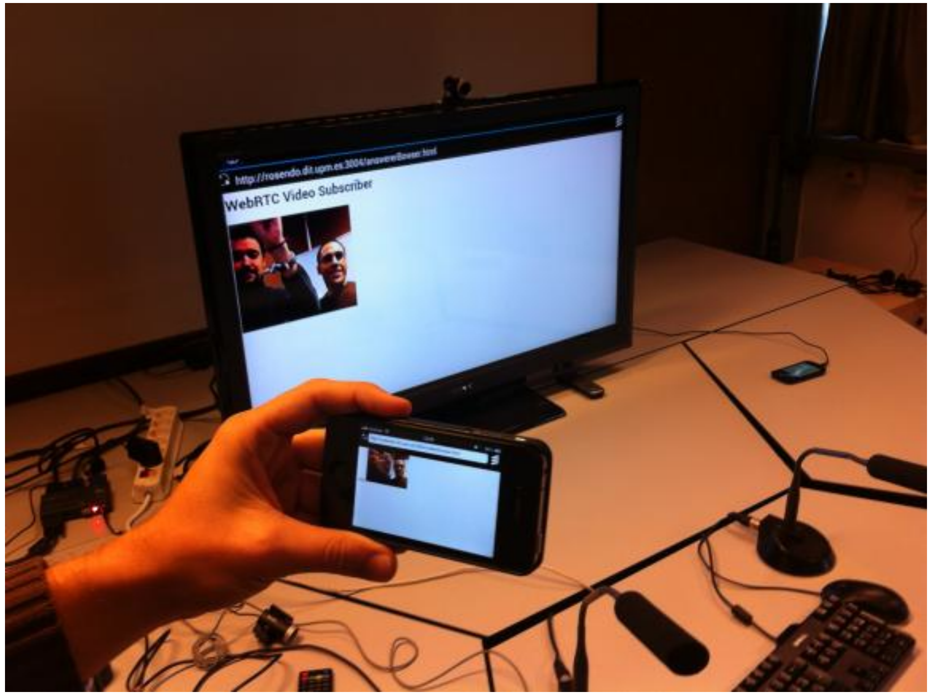
Mini note: HTTP is more and more the de-facto substrate

What Is the IETF Doing?

- Tailoring the web tools for small devices
- Lightweight HTTP (CoAP, HTTP/2.0)
- TLS for small devices (DTLS, DICE, ACE)
- Helping IP run on new link technologies

Real-Time Communications

Real-Time Communications



- Internet multimedia has freed us from circuits and pure voice
- But can we free ourselves from purpose-built applications? Can we make anyone a VoIP provider?
- WebRTC enables voice and video apps in browsers
- Integration to the rest of the web experience

What Is the IETF Doing?

With W3C:

- Working on the browser APIs
- Working on the protocols

Conclusions

Evolving Web Technology

- New types of applications – real-time multimedia, smart objects
- Https becoming far more common
- Basic protocols are evolving
- The web becomes central to everything

☑ Why? Because anyone can build on it

Thank you

谢谢