

# The Effect of Surveillance Revelations to Internet Technology

Jari Arkko

Chair, IETF

Expert, Ericsson Research



**I E T F**®



# Outline

- › IETF
- › Surveillance and the revelations
- › Likely attack vectors
- › World (re)actions
- › What can the techies do?
- › IETF (re)actions
- › Conclusions

# Evolving Internet Technology

“Perfect storm of 2014”

- › Pervasive monitoring
- › HTTP 2.0
- › Transport Layer Security (TLS) 1.3
- › WebRTC
- › Evolution of transport protocols



# Surveillance

HOME PAGE TODAY'S PAPER VIDEO MOST POPULAR U.S. Edition

**The New York Times** U.S.

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION

POLITICS EDUCATION TEXAS

## N.S.A. Able to Foil Basic Safeguards of Privacy on Web

By **NICOLE PERLROTH**, **JEFF LARSON** and **SCOTT SHANE**  
Published: September 5, 2013 | 1466 Comments

darkREADING SECURITY  
Protect The Business Enable Access

Advanced Threats Applications Attacks & Breaches Compliance Database Endpoint Insider Threat Management  
Mobile Monitoring Perimeter Risk Security Analytics Services SMB Threat Intel Vuln Management Vulns & Threats  
More

Security that's healthy from head to toe. **Lumension**  
IT Secured. Success Optimized.

NEWS

## Latest NSA Crypto Revelations Could Spur Internet Makeover

Kelly Jackson Higgins  
See more from Kelly | Connect directly with Kelly: Bio | Contact

Concerns over backdoors and cracked crypto executed by the spy agency is prompting calls for new more secure Internet protocols, IETF will address latest developments at November meeting

2 Comments 11 Likes 76 Tweets 5 +1s 20 Shares Submit 17

**Lumension**  
IT Secured. Success Optimized.

theguardian Google Custom S

News Sport Comment Culture Business Money Life & style Travel Environment

News World news The NSA files

Series: Glenn Greenwald on security and liberty Previous Next Index

## Revealed: how US and UK spy agencies defeat internet privacy and security

- NSA and GCHQ unlock encryption used to protect emails, banking and medical records
- \$250m-a-year US program works covertly with tech companies to insert weaknesses into products
- Security experts say programs 'undermine the fabric of the internet'

Share 30992 Tweet 11.3K +1 3.6k Pin it 57 Share 873 Email

Q&A: submit your questions for our privacy experts

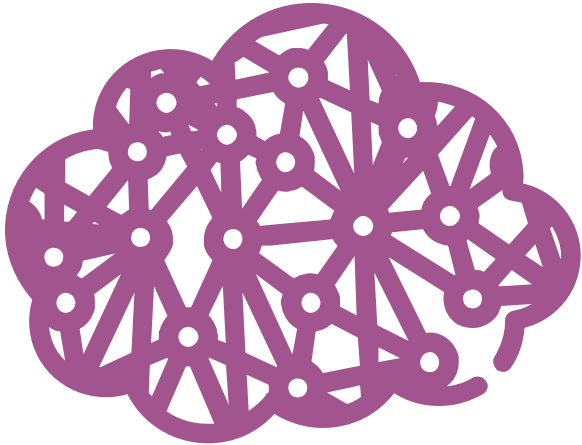
theguardianAlpha

Home UK World Comment Sport Football Life & style Culture Business Travel Technology E

comment is free

The US government has betrayed the internet. We need to take it back

# 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

# Some Basic Terms



Legal interception

Surveillance

Communications vs. database access

Targeted vs. wholesale surveillance

Intelligence/military activities vs. police/courts

# The Allegations Painted a Depressing Picture

- › Store-everything-and-search-later surveillance
- › Everything that anybody does is recorded
  - with the help of co-operating countries, if needed
- › Encrypted traffic can be read as well as cleartext
- › Service providers forced into silence
- › Agents plant vulnerabilities in standards

# Likely Vulnerabilities To Be Exploited

Unprotected communications (duh!)

Communications within cloud

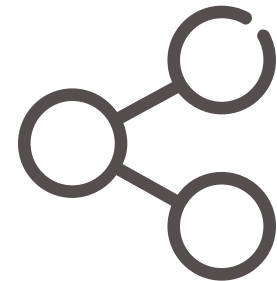
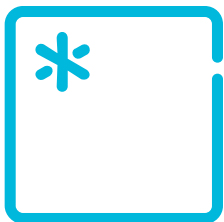
Direct access to the peer

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)





# Example Reactions

- › Various political reactions
- › Initiatives for operational improvements
- › Calls for more “national” Internets
- › The spark for Internet Governance discussions
- › NSA-envy
- › Service providers showing they are secure
- › Engineers wondering what they should do
- › More attention to security of software



# Initiatives for Operational Improvements

KONESALIT

## Nyt riemastui ministerikin: Suomeen tulee uusi miljardin euron konesali ja merikaapeli Saksaan

Talouselämä

23.5.2014 07:50

päivitetty 23.5.2014 07:51

 Suosittele 75

 Jaa

 Twiittaa 7

 +1 0

 Share 0

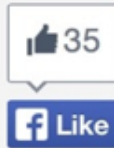


"Viime viikolla korviin kantautui iloinen viesti. Helsingin Roihupeltoon kaavaillaan miljardiluokan teollista investointia. Edellisestä teollisesta investoinnista Helsinkiin on kulunut jo aikaa", iloitsee omistajaohjausministeri [Pekka Haavisto](#) (vihr) [blogissaan](#).

# Germany's Merkel Calls for Separate European Internet

BY RICH MILLER ON FEBRUARY 17, 2014

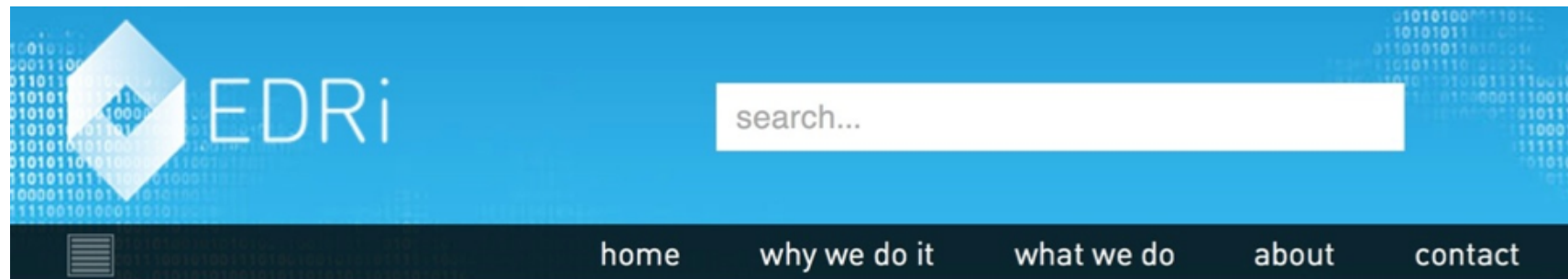
1 COMMENT



# Calls for National “Internets”



# 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.

# The Spark for Internet Governance Discussions

(At least in the eyes of some – but in reality, Internet governance and, e.g., domain name or address maintenance has nothing to do with surveillance. Changes in IANA are largely due to hard work over several years in bringing the system to a state where USG no longer needs to be involved.)

**CNN Money**  
A Service of CNN, Fortune & Money

FORTUNE Money

Home Video Business News Markets My Portfolio Investing Economy Tech Personal Finance

Brainstorm Tech | Mobile | Security | Social | Innovation | Enterprise | Apple 2.0 | Tech30

This is the Microsoft C

## The U.S. is relinquishing control of domain names. Here's why.

FORTUNE

March 17, 2014: 2:10 PM ET

Recommend 95

The United States has long planned to give up its unique role as steward of the Internet's domain name system, but it's unclear what kind of entity will replace it.

By Sam Gustin


















PHOTO: DALE E BOYER/GETTY

This post is in partnership with Time, which offers the latest news from around the world. The article below was originally published at [Time.com](#)

Page 13

# Service Providers Showing They Are Secure

The “https:” trend

	Encrypts data center links	Supports HTTPS	HTTPS Strict (HSTS)	Forward Secrecy	STARTTLS
	undetermined	limited	✗	undetermined	✗
	undetermined	✓ (iCloud)	✗	undetermined	✗ (me.com, mac.com)
	undetermined	undetermined	✗	undetermined	✗ (att.net)
	undetermined	undetermined	✗	undetermined	✗ (comcast.net)
	✓	✓	✓	✓	✓
	in progress	✓	planned	✓	✓ (in progress, facebook.com)
	undetermined	✓	✓	undetermined	✗
	✓	✓	in progress for select domains, see notes	✓	✓
	✗ contemplating	✓ planned 2014	✓ planned 2014	✓ planned 2014	✗ contemplating
	in progress	✓	planned	in progress	✓ (planned, outlook.com)
	undetermined	✓	✗	undetermined	✗
	✓	✓	✓	in progress	✓
	✓	✓	✓	in progress	✓
	✓	✓	✓	✓	✗
	✗	✓ planned 2013	✓ planned 2014	✓	✗
	undetermined	undetermined	✗	undetermined	✗ (verizon.net)
	undetermined	available	✗	undetermined	✗

# More Attention to the Security of Software



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
- › 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



Internet Engineering Task Force (IETF)  
Request for Comments: 7258  
BCP: 188  
Category: Best Current Practice  
ISSN: 2070-1721

S. Farrell  
Trinity College Dublin  
H. Tschofenig  
ARM Ltd.  
May 2014

## Pervasive Monitoring Is an Attack

### Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

### Status of This Memo

This memo documents an Internet Best Current Practice.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on BCPs is available in Section 2 of RFC 5741.

# Ongoing Technical Activity



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?

- › Pervasive monitoring worries have energized IETF folk to work on security & privacy issues in general
- › July 2013 – side meeting
- › November 2013 – big topic
- › March 2014 – doing the practical work, workshop
- › Early results coming in, more in the summer



# Some Specific IETF Topics

- › UTA WG formed - how to use TLS in applications
- › RFC 7258 published after major discussion
- › Recent new ideas: DNS Privacy and TCP encryption

# 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

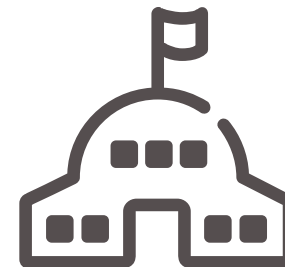
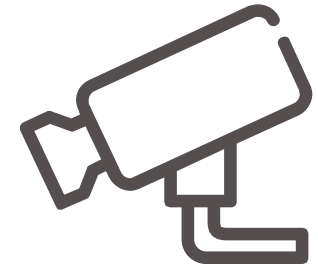


# TLS 1.3 and HTTP/2.0

- › TLS 1.3 in development, aiming for better handshake encryption properties and learning from previous TLS problems
- › HTTPBIS WG developing HTTP/2.0, aiming for better efficiency but also for TLS protection of more web traffic

# Challenges

- › **E-mail**: end-to-end security
- › **Web**: proxies and CA lists
- › **Endpoint** and **operating** system security



# HTTP/2.0 Challenges

- › Does **not** have mandatory encryption
- › But some implementations 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

# 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



# Final Words

- › Initial excitement followed by hard work
- › No one ever said Internet security is easy...
- › But communities are energized to do the hard work
  - both specifying and deploying more security
  - while debating the difficult trade-offs
- › The Internet should not be taken for granted
  - open & global & source of benefits for the humankind

Thank you