Strengthening the Internet Against Pervasive Monitoring

Jari Arkko Stephen Farrell Richard Barnes

IETF {Chair, SEC AD, RAI AD} - speaking as individuals

Outline

What has happened since RIPE-67?

IETF Activities

Challenges

What can you do?

RIPE-67 Discussion Items

- Considering surveillance as one attack among others

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.

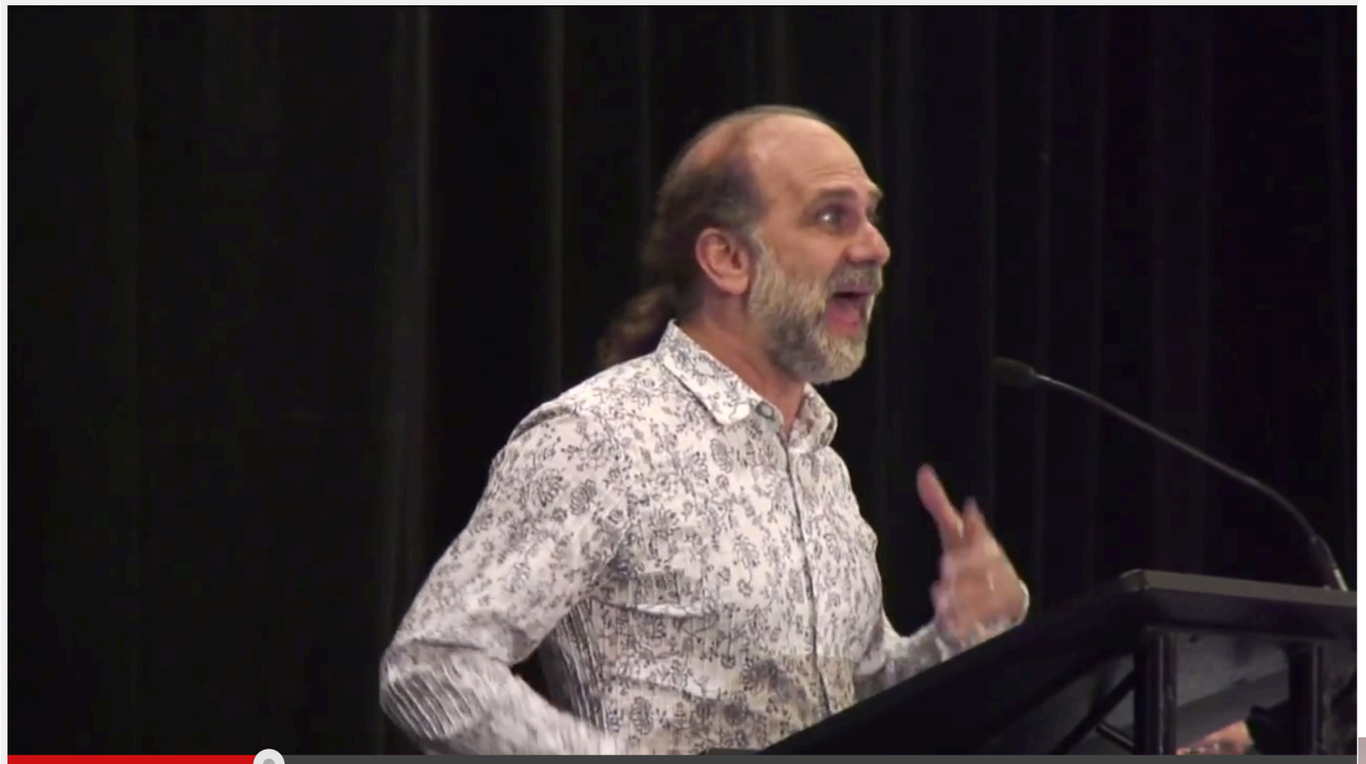
This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on BCPs is available in Section 2 of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

RIPE-67 Discussion Items

- Discuss the topic openly in the IETF plenary, IAB workshop, WGs, ...

YouTube

ietf technical plenary



IETF 88 Technical Plenary: Hardening The Internet

IETF - Internet Engineering Task Force · 46 videos

Subscribed

11,429 views

108 0

WG Action: Formed Using TLS in Applications (uta) — Inbox – IETF Announce

The IESG <iesg-secretary@ietf.org>

December 11, 2013 7:33 PM

Hide Details

To: IETF-Announce <ietf-announce@ietf.org>

Cc: uta WG <uta@ietf.org>

Reply-To: ietf@ietf.org List

WG Action: Formed Using TLS in Applications (uta)

A new IETF working group has been formed in the Applications Area. For additional information please contact the Area Directors or the WG Chairs.

Using TLS in Applications (uta)

Current Status: Proposed WG

Chairs:

Leif Johansson <leifj@sunet.se>

Orit Levin <oritl@microsoft.com>

RIPE-67 Discussion Items

- Start encrypting unprotected communications

	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	✗
YAHOO!	✓	planned 2014: default for mail, available for all services	✗	undetermined	✗ (yahoo.com)

RIPE-67 Discussion Items

- Vulnerable standards - call for additional public review, update/decommission old algorithms

[ietf-privacy] Draft report on IETF89 PM review lunch meeting report

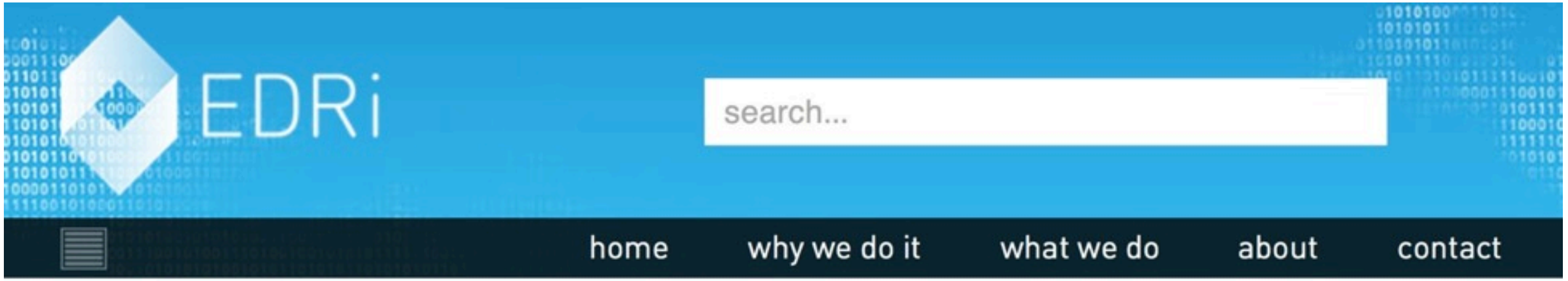
- *From*: Avri Doria <avri at acm.org>
- *To*: ietf-privacy at ietf.org
- *Date*: Wed, 12 Mar 2014 06:19:51 -0400
- *List-id*: Internet Privacy Discussion List <ietf-privacy.ietf.org>

```
Draft Meeting report.

A set of notes created by Scott Brim (thanks!) can be found at:
https://docs.google.com/document/d/1GwD5m09p42fS3OWucYwPZ0lWcVN8Y_HIN0yp2BzYYYI/edit?usp=sharing

Those who were at the meeting should feel free to add their comments. A text view of their current state is attached
to this message.

In terms of the meeting, we discussed several issues and I believe we came up with the following:

- Volunteers will be begin to work on reviews of existing standards track RFCs

- While the reviews will be primarily for Pervasive Monitoring (PM) risks and issues, privacy issues will also be in
scope for the reviews.
```

- Contact Stephen Farrell if you want to volunteer

RIPE-67 Discussion Items

- NSA-envy in other intelligence agencies



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.

RIPE-67 Discussion Items

- Implementation backdoors - diversity, open source, review

LibreSSL

RIPE-67 Discussion Items

- A more diverse Internet (IXPs, cables, services), good!
- Calls for more nationally controlled Internets, bad!

Germany's Merkel Calls for Separate European Internet

BY RICH MILLER ON FEBRUARY 17, 2014 1 COMMENT

Back to 2014

Scope for This Discussion

- We should not have a political discussion
- But we MUST understand, in general, threats to Internet traffic and how the real Internet evolves
- And we SHOULD have an idea how Internet technology can better support security and privacy
- Particularly for those who want it (like us!)

Some History

- 1990's crypto wars - RFC 1984
- 2000's wiretap/lawful interception - RFC 2804
- Today's equivalent is pervasive monitoring

Being a Part of the Problem

- IETF and others should see themselves as part of the problem as well as part of the solution
  - Too hard to use secure protocol variants
- Did BULLRUN have an effect? Unlikely... IMO
- Likely: Complex requirements, lack of deployment experience, hard problems
- We can and will improve though by focusing on real, large deployments

IETF (Re)Action

- Overall: snowdonia has re-energised folks to do better on security and privacy in general (and not solely in response to PM)
    - Side meeting in Berlin @ IETF-87
    - Tech plenary, major discussion @ IETF-88
    - STRINT workshop before IETF-89
- Topic at many meetings/BoFs @ IETF-89
- Wanting to see results from IETF-90

New IETF Work

- UTA WG formed, update BCPs on how to use TLS in applications
- WG has to do work now of course
- draft-farrell-perpass-attack becomes RFC 7258 (BCP) after major IETF LC debate – sets the basis for further actions
- BoFs at IETF-89: DNS Privacy and TCP encryption

Other Relevant IETF Work

- 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

Hot Topics in HTTP 2.0 TLS

- HTTP 2.0 specification does **not** have mandatory encryption
  - Some implementations may 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 is decreasing the ability to do caching/scanning as well as spying

What To Do (I)

- Turn on crypto
  - For applications and between data-centres
    - Current tools: TLS, IPsec, DNSSEC
    - Future tools: DNS-priv, TCPCrypt, ... ?
- Data minimisation
  - E.g. DNS QNAME minimisation
  - More to learn here

What To Do (II)

- Better implementations
  - Update/check/audit crypto support
    - https://cryptech.is/ and similar
    - Make security/privacy admin easier
- Users
  - Target diversity - don't all use the same services

What To Do (III)

- Discuss the issue openly
  - In whatever fora are relevant for you
- Go and be responsible engineers/computer scientists and take the broader implications of your work into account
  - Before, while and after doing it

Final Words

- Initial excitement followed by hard work
- No one said that Internet security is easy :-)
- But the community seems energized to do the hard work, and is both deploying and specifying more security
    - While debating the hard tradeoffs
- The high rate of change in the web world makes some changes easier

Please join the work if you are willing and able!

Send feedback to TLS, HTTPBIS WGs on your use cases
Join TCP and DNS efforts to ensure they are deployable

Next meeting: IETF-90 July 20-25, 2014 in Toronto
(hosted by Ericsson)

Thank You

Backup Slides for Reference

Likely Attack Vectors

- Unprotected communications (duh!)
- 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)

Vulnerable Standards?

- Bad random number generators (case Dual_EC_DBRG withdrawn NIST)
- Weak crypto (case RC4 & TLS)
- Some claims about other vulnerabilities in IETF standards (IPsec) and elsewhere but personally we believe this to be unlikely

What Can the Engineers Do?

- Technology may help - to an extent - but does not help with communications to an untrusted peer
- Prevent some attacks, make getting caught more likely, ...
- We need to do and be seen doing as much as we can - this **is** about the security of the Internet - and the time window is **now**

Vulnerable Standards?

- Bad random number generators (case Dual_EC_DBRG withdrawn NIST)
- Weak crypto (case RC4 & TLS)
- Some claims about other vulnerabilities in IETF standards (IPsec) and elsewhere but personally we believe this to be unlikely

What Can the Engineers Do?

- Technology may help - to an extent - but does not help with communications to an untrusted peer
- Prevent some attacks, make getting caught more likely, ...
- We need to do and be seen doing as much as we can - this **is** about the security of the Internet - and the time window is **now**