Using Applications with TLS (UTA)

IETF 89, London

March 7th, 2014

By chairs:

Leif Johansson <leifj@sunet.se>
Orit Levin <oritl@microsoft.com>

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function
- All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Channels

- Mailing list
  - uta@ietf.org
- Jabber
  - uta@jabber.ietf.org
- audio stream
  - http://ietf89streaming.dnsalias.net/ietf/ietf896.m3u
- meetecho
  - http://www.meetecho.com/ietf89/uta

Agenda

9:00 – 9:15	Welcome by chairs and getting organized
9:15 – 9:30	Discussion
9:30 –10:00	Applicability to a generic application presented by Peter Saint-Andre https://datatracker.ietf.org/doc/draft-sheffer-uta-tls-attacks/ https://datatracker.ietf.org/doc/draft-sheffer-tls-bcp/
10:00-10:10	XMPP over TLS presented by Peter Saint-Andre https://datatracker.ietf.org/doc/draft-saintandre-xmpp-tls/
10:10–10:20	Prohibiting RC4 presented by Orit Levin https://datatracker.ietf.org/doc/draft-popov-tls-prohibiting-rc4/
10:20-10:50	E-mail over TLS presented by Keith Moore and Chris Newman https://datatracker.ietf.org/doc/draft-newman-email-deep/
10:50-11:00	TLS certificates for email presented by Alexey Melnikov https://datatracker.ietf.org/doc/draft-melnikov-email-tls-certs
11:00-11:10	Opportunistic TLS Summary from STRINT presented by chairs
11:10-11:20	Opportunistic TLS terminology draft presented by Joe Hildebrand https://datatracker.ietf.org/doc/draft-hoffman-uta-opportunistic-tls/
11:20-11:30	Open Mic/Discussion

Problem Statement

- Many application protocols have defined methods for using TLS
- These definitions are often confusing, incomplete, and inconsistent among different (application) protocols
- This has led to lack of interoperability and/or lack of TLS deployment

Mission Statement

As a part of the IETF broader agreement to increase the security of transmissions over the Internet, UTA's goal is to increase usage of TLS by applications through

- Improved TLS interoperability by clarifying and simplifying existing implementation and deployment choices
- Hardening security and confidentiality of application connections by using secure ciphers and possibly new modes of operation (e.g. Opportunistic Keying) with TLS

Working Assumptions

- Make no changes to TLS itself
- Ensure that no changes will be required to current versions of popular TLS libraries
- Strive that as few changes as possible might be required to the applications using TLS
- Collaborate closely with other IETF WGs (e.g., TLS and DANE)

Deliverables

1. A threat analysis document containing a collection of known security breaches to application protocols due to poor use of TLS (Likely an Informational RFC)
2. Applications' independent document recommending best existing and future practices for using TLS (Likely a BCP or a Proposed Standard RFC)
3. A set of documents, each describing best existing and future practices for using TLS with a specific application protocol, i.e., SMTP, POP, IMAP, XMPP, HTTP 1.1, etc. (Case-by-case likely a BCP or a Proposed Standard RFC)
4. A document discussing (and potentially defining) how to apply the “opportunistic keying” approach to TLS. (Category TBD)
5. A UTA WG Wiki page summarizing the state of TLS implementations

Back to the Agenda

9:00 – 9:15 Welcome by chairs and getting organized

9:15 – 9:30 Discussion

9:30 –10:00 Applicability to a generic application presented by Peter Saint-Andre

https://datatracker.ietf.org/doc/draft-sheffer-uta-tls-attacks/

https://datatracker.ietf.org/doc/draft-sheffer-tls-bcp/

10:00-10:10 XMPP over TLS presented by Peter Saint-Andre

https://datatracker.ietf.org/doc/draft-saintandre-xmpp-tls/

10:10–10:20 Prohibiting RC4 presented by Orit Levin

https://datatracker.ietf.org/doc/draft-popov-tls-prohibiting-rc4/

10:20-10:50 E-mail over TLS presented by Keith Moore and Chris Newman

https://datatracker.ietf.org/doc/draft-newman-email-deep/

10:50-11:00 TLS certificates for email presented by Alexey Melnikov

https://datatracker.ietf.org/doc/draft-melnikov-email-tls-certs

11:00-11:10 Opportunistic TLS Summary from STRINT presented by chairs

11:10-11:20 Opportunistic TLS terminology draft presented by Joe Hildebrand

https://datatracker.ietf.org/doc/draft-hoffman-uta-opportunistic-tls/

11:20-11:30 Open Mic/Discussion

STRINT

- Set of terms
  - “Opportunistic Keying” should be the term used
- Focus on Passive attack model
- Start with DH/ECDH (for PFS)
  - Fall back to plain text (collect information and send notification to the server?)
  - Escalate to authenticated (in parallel?)
- Invisible to users, e.g. they don’t know they have some encryption
- Threat model
  - Protecting from pervasive monitoring
  - Understand Middleboxes and how they effect OK at different layers
  - High-sensitivity sessions are out-of-scope! E.g. financial