TLS
Internet-Draft
Intended status: Standards Track
Expires: September 7, 2014

M. Thomson
Mozilla

March 6, 2014

Authenticated Content Promise Extension for (D)TLS
draft-thomson-tls-acp-00

Abstract

This document describes an extension to Transport Layer Security (TLS) and Datagram TLS (DTLS) that enables the negotiation of a promise to protect session content from modification and eavesdropping by third parties.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 7, 2014.

Table of Contents

1. Introduction

WebRTC [I-D.ietf-rtcweb-overview] creates a new understanding of the way that "user-generated content" is used on the world wide web. The established definition identifies content that is generated by users and used by sites; after all, the primary mode of interaction on the web is between users and sites.

WebRTC changes that by enabling users to communicate directly, with secure channels between established between user agents (or browsers). These channels might be established with the aid of a web site, but the content of the communication session can be made inaccessible to the site [I-D.ietf-rtcweb-security-arch]. With peer authentication, each user is able to be sure that:

- the content they are generating is only accessible to the authenticated peer; and

- the content they are receiving can be attributed solely to the authenticated peer.

On the originating end of a communications session, this guarantee is easy to provide. A web site is able to provide instructions for session setup that allow the browser to protect content from the site, and to restrict where content is delivered based on identity.

On the receiving side, this is more complicated. Since there is a desire to enable use cases where sites do have access to content that is received, there is a need for a signal of some form to distinguish the cases.

It is possible to use the WebRTC signaling channel for this purpose, but only with restrictions. The signaling channel is considered untrustworthy, so additional protection would be required to ensure

that any indicators could not be erased or re-attributed to other keying material. Furthermore, this would also require protection against replay. Prohibiting key reuse between confidential and non-confidential sessions would suffice for this purpose, though this is undesirable for other reasons.

1.1. Authenticated Content Promise

This document describes a Transport Layer Security (TLS) [RFC5246] extension, which, if negotiated, establishes a session as being confidential. Peers that negotiate this extension promise that:

- Any content that is written to or read from the connection MUST be protected from modification by entities other than the one that is authenticated (i.e., the user).

- Any content that is written to or read from the connection MUST NOT be recorded or forwarded to any entity other than the one that is authenticated.

In addition to establishing an authenticated channel for communications, this provides a key advantage over signaling-based methods for ensuring privacy. Key continuity is possible, which allows clients to operate without identity providers and still have a stable basis for establishing continuity of identity with peers.

1.2. Conventions and Terminology

At times, this document falls back on shorthands for establishing interoperability requirements on implementations: the capitalized words "MUST", "SHOULD" and "MAY". These terms are defined in [RFC2119].

2. Authenticated Content Promise

A new extension type ("authenticated_content_promise(TBD)") is defined. If this extension is negotiated, both client and server are bound by a promise to protect content.

```
enum {
    authenticated_content_promise(TBD), (65535)
} ExtensionType;
```

The "extension_data" field of this extension MUST be empty.

3. Security Considerations

Endpoints need to take care to avoid rendering of authenticated content alongside other content in a way that could cause user confusion equivalent to the effect of modifying content. For instance, unauthenticated audio could be played at higher volume levels than authenticated audio, potentially misleading users about what sounds can be attributed to each.

This looks a little like digital rights management (DRM), but it really doesn't promise to protect content to the degree required by DRM schemes. It relies solely on users and their trust each other (and their user agents, operating system and hardware). Nothing in this mechanism stops a compromised end system from modifying or eavesdropping on communications, from information being overhead or seen by people nearby, or from any action taken on the part of the authentiated entities, such as screen recording.

A little care is needed to avoid side channels, some of which are quite obvious. For example, even with echo cancellation, audio played over speakers can be picked up by nearby microphones; video playback might be observable in a mirror.

4. IANA Considerations

IANA has allocated a TLS extension code point of (TBD) for this extension.

5. Acknowledgements

Eric Rescorla helped identify the problem and formulate this mechanism.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

6.2. Informative References

[I-D.ietf-rtcweb-overview]
Alvestrand, H., "Overview: Real Time Protocols for Brower-based Applications", draft-ietf-rtcweb-overview-09 (work in progress), February 2014.

[I-D.ietf-rtcweb-security-arch]
Rescorla, E., "WebRTC Security Architecture", draft-ietf-rtcweb-security-arch-09 (work in progress), February 2014.

Author's Address

Martin Thomson
Mozilla
Suite 300
650 Castro Street
Mountain View, CA 94041
US

Email: martin.thomson@gmail.com