Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 6, 2014

P. Hoffman
VPN Consortium

February 2, 2014

Opportunistic Encryption Using TLS
draft-hoffman-uta-opportunistic-tls-00

Abstract

This document defines the term "opportunistic encryption using TLS" as it applies to application protocols that use TLS.

Status of This Memo

Copyright Notice

1. Introduction

The term "opportunistic encryption" has many informal definitions, and this panoply of definitions has made discussion of using opportunistic encryption in particular protocols more difficult. The term has acquired many different meanings in different contexts, so having a single definition that can be used by protocol specifications and application developers will benefit the Internet community.

Opportunistic encryption using TLS is considered a good way to prevent passive monitoring of communications that would otherwise be sent unencrypted. It is clear that such monitoring is fairly pervasive in many Internet environments, and it is also clear that many people would like prevent their communications from being watched by governments, companies, groups, and individuals whom they do not know. Opportunistic encryption using TLS causes the start of application communication to happen later than it normally would have due to the round trips and mathematical computations required to establish a TLS session. The creators of an application program must weigh these and other factors when deciding whether or not to use opportunistic encryption in their program. Similarly, protocol designers need to take these and other factors into account when deciding whether or not to require, suggest, or even allow opportunistic encryption using TLS in their protocol specifications.

The definition of opportunistic encryption using TLS in this document explicitly sets user interface requirements for applications. Although this is rarely done in other IETF standards, doing so is required here for security reasons.

Note that "opportunistic encryption using TLS" is different than "unauthenticated TLS". The latter describes a similar but distinct concept, and it applies to different scenarios. There is a wide industry agreement that unauthenticated TLS is almost always a bad practice. The two terms are often confused, and thus "unauthenticated TLS" is described only in an appendix of this document.

This document applies to all versions of TLS, including TLS 1.2 [RFC5246], TLS 1.1 [RFC4346], and TLS 1.0 [RFC2246]. It may or may not apply to future versions of TLS. The definition of "opportunistic encryption using TLS" in this document applies to any protocol that can be protected with TLS; this means that it mostly applies to layer 7 protocols, also known as "application layer protocols". This document only defines opportunistic encryption using TLS; it does not describe opportunistic encryption with other encrypting protocols such as IPsec.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119, BCP 14 [RFC2119].

2. Definition of ’Opportunistic Encryption Using TLS’

An application supports opportunistic encryption using TLS if the application attempts to perform TLS negotiation without the user who is running the application knowing whether or not TLS is in use. The application MUST NOT have any user-visible configuration that enables opportunistic encryption using TLS. Stated another way, it is impossible for a program to have a configuration option for opportunistic encryption: having such an option inherently is not for opportunistic encryption.

When an application that supports opportunistic encryption negotiates TLS, that application might or might not authenticate the TLS server. It is expected that the common case is that applications that supports opportunistic encryption will not authenticate the TLS servers they connect to. However, it is acceptable for an application that supports opportunistic encryption to only complete the TLS negotiation if the TLS server can be validated.

When an application that is doing opportunistic encryption successfully creates a TLS session, that application MUST NOT show the user any indication that TLS is in use.

An application that does opportunistic encryption using TLS finds the appropriate TLS server using one or more of many mechanisms, none of which are described here in detail. Some of those mechanisms include in-protocol upgrade to TLS, in-protocol pointers to TLS servers, DNS queries whose responses indicate the presence of appropriate TLS servers, and simply trying a TCP port on which TLS is expected.

3. IANA Considerations

None

4. Security Considerations

Opportunistic encryption using TLS prevents observation by passive attackers on the network. However, it doesn’t completely prevent the attacker from knowing anything about the contents of the encrypted information. For example, the attacker can know what protocol is being encrypted, the approximate size of the encrypted messages, and so on. The attacker can also learn about the cryptographic capabilities of the client and server by observing the TLS handshake.

The purpose for the requirement that the application not have any user-visible configuration that enables opportunistic encryption is that having user-visible configuration is likely to cause lower security for the Internet. A widely-used setting that says "use TLS even when it is not called for" would cause server operators to become more lax with their TLS deployments, such as not bothering to renew (or even get) widely-accepted certificates for their sites because they know that most applications could reach them with TLS anyway.

The purpose for the requirement that the application not show that TLS is in use if the TLS was established with opportunistic encryption is that such an indication is likely to cause lower security for the Internet, particularly in web browsers.

5. References

5.1. Normative References

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

5.2. Informative References

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

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

Appendix A. Unauthenticated TLS

The term "unauthenticated encryption", when used in the context of TLS, is fairly straight-forward. However, in discussions on many security and protocol mailing lists, it is often confused with "opportunistic encryption using TLS".

Unauthenticated encryption for TLS is the act of setting up a TLS session at the request of a user where the TLS client does not authenticate the TLS server.

When the TLS session is being set up at the request of the user, such as when the user enters a URL that should only be resolved with TLS, using unauthenticated TLS is rarely the expected or desired result. In such a situation, the application might allow unauthenticated TLS after giving the user some warning, or the application might even have a configuration setting that tells the application to allow unauthenticated TLS even when trying to set up an explicit TLS session.

Many security-conscious protocol developers are severely critical of applications that allow unauthenticated encryption with TLS, even if the application gives the user warnings when authentication failed. Similarly, many security-conscious protocol developers are severely critical of applications that allow unauthenticated encryption to be configured at all.

Note that "opportunistic encryption using TLS" may allow the TLS session to be set up without the client authenticating the server. This is a completely different scenario than "unauthenticated encryption" using TLS. The definition of opportunistic encryption with TLS precludes the TLS session being set up at the request of the user; the definition of unauthenticated encryption with TLS requires that the TLS session is being set up at the request of the user.

Author’s Address

Paul Hoffman
VPN Consortium

Email: paul.hoffman@vpnc.org