Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 9, 2013

N. Mavrogiannopoulos
KU Leuven - IBBT
November 5, 2012

Preventing cross-protocol attacks on the TLS protocol
draft-mavrogiannopoulos-tls-cross-protocol-02

Abstract

This memo proposes a fix in the TLS key exchange signature generation to prevent cross-protocol attacks.

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 May 9, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1. Introduction

The TLS protocol [RFC5246] suffers from an issue in the ServerKeyExchange message signature discovered by Wagner and Schneier in [WS-ATTACK]. They describe a cross-protocol attack on the SSL 3.0 [RFC6101] protocol, that re-uses a signed ServerKeyExchange packet in another session with a different key exchange algorithm. In effect the attack uses a server as an oracle to obtain signed ServerKeyExchange messages that are relayed to another, unrelated, session. The described attack turned to be impossible to implement in practice, but the underlying idea is applicable to all TLS protocol versions, and it provides a tool for new attacks on the protocol. The [CROSS-PROTOCOL] attack is a prominent example, which takes advantage of interactions between the Diffie-Hellman and Elliptic Curve Diffie-Hellman ciphersuites to perform a TLS server impersonation after obtaining 2^40 signed messages.

In this document we propose a fix for the TLS protocol which makes it immune to these attacks, but does not require a protocol version upgrade.

2. Terminology

This document uses the same notation and terminology used in the TLS Protocol specification [RFC5246].

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 [RFC2119].

3. The new ServerKeyExchange signature

The goal of this memo is to restrict the applicability of the server provided signed ServerKeyExchange to the current session. A simple fix may be to include the negotiated ciphersuite into the signature. However, the TLS protocol is complex and a key exchange method does not always imply a single format of the ServerKeyExchange signature. For example, the elliptic curves key exchange method may be used with an arbitrary elliptic curve [RFC4492] which requires different data in the ServerKeyExchange than when used with a named curve. Such key exchange suboptions are negotiated using TLS extensions and such extensions should be covered by the signature, to prevent any attack that takes advantage of the different signature format.

For that we propose that the signature of the ServerKeyExchange message to be modified to include in addition to explicit identifiers of the algorithms, all the previously exchanged messages. The proposed signature for a ServerKeyExchange message is shown below.

```
enum { server (0), client (1) } ConnectionEnd;

enum { dhe_dss (0), dhe_rsa (1),
       ec_diffie_hellman (2)
     } KeyExchangeAlgorithm;

struct {
    KeyExchangeAlgorithm kx_algorithm;
    select (KeyExchangeAlgorithm) {
      case dhe_dss:
      case dhe_rsa:
        ServerDHParams params;
      case ec_diffie_hellman:
        ServerECDHParams;
    }
} Parameters;

struct {
  Parameters params;
  digitally-signed struct {
    ConnectionEnd entity;
    Parameters params;
    opaque handshake_messages<0..2^24-1>;
  }
} ServerKeyExchange;
```

The new format includes explicit indicators of the entity (server), the key exchange algorithm used, the handshake messages exchanged, and the parameters of the key exchange. This modification will be negotiated by using a new TLS extension to allow backwards compatibility.

4. The extension

In order for a client to advertise its support for the new ServerKeyExchange format we add a new extension "new_server_key_exchange", with value TBD-BY-IANA, to the enumerated ExtensionType defined in [RFC5246]. The "extension_data" field of this extension is empty.

5. Server and client behavior

Clients, that wish to protect against cross-protocol attacks, SHOULD include the extension of type "new_server_key_exchange" in the (extended) client hello.

Servers that receive an extended client hello containing a "new_server_key_exchange" extension, MAY accept the request for the

new ServerKeyExchange format by including an extension of type "new_server_key_exchange" in the extended server hello.

Servers compliant to this document, that did not receive the extension MUST set the gmt_unix_time part of the Random value included in ServerHello to zero. Because in cross-protocol attacks the server's random value is redirected to the client, this is a way for the server to indicate support for the extension even in the presence of an adversary.

Clients compliant to this document, that advertised this extension but didn't receive a corresponding extension from the server, MUST check the gmt_unix_time part of the Random value included in ServerHello message for the value zero. If the gmt_unix_time is zero the client MUST abort the handshake with an "illegal_parameter" fatal alert.

Note that this extension is applies to all versions of the TLS protocol including TLS 1.2 [RFC5246] and SSL 3.0 [RFC6101].

6. Security considerations

This extension modifies the ServerKeyExchange message in order to prevent attacks to the protocol similar in nature with the Wagner and Schneier attack. In order for the protection to be applicable, both the client and the server must support this extension.

Compliant servers that did not receive the extension from the client are required to set the 4 bytes of the server's random value, that encodes the time, as zero. This provides a tool to indicate support for the extended format even in the presence of an adversary, but comes at the cost of reducing the total randomness from the server from 32 bytes to 28 bytes.

7. IANA Considerations

This document defines the TLS extension "new_server_key_exchange" (value TBD-BY-IANA) whose value should be assigned from the TLS ExtensionType Registry defined in [RFC5246].

8. References

8.1. 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.

8.2. Informative References

[WS-ATTACK] Wagner, D. and B. Schneier, "Analysis of the SSL 3.0 protocol", In Proceedings of the Second USENIX Workshop on Electronic Commerce, USENIX Press , November 1996.

[CROSS-PROTOCOL] Mavrogiannopoulos, N., Vercauteren, F., Velichkov, V., and B. Preneel, "A cross-protocol attack on the TLS protocol", In Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS 2012), ACM , October 2012.

[RFC6101] Freier, A., Karlton, P., and P. Kocher, "The Secure Sockets Layer (SSL) Protocol Version 3.0", RFC 6101, August 2011.

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006.

Author's Address

Nikos Mavrogiannopoulos
KU Leuven ESAT/SCD/COSIC - IBBT
Kasteelpark Arenberg 10, bus 2446
Leuven-Heverlee, B-3001
Belgium

EMail: nikos.mavrogiannopoulos@esat.kuleuven.be