Liaison from the ISOC to ISO/IEC JTC1/SC6 and its National Body members in relation to ISO-IECJTC1-SC6_N15618

Date: 2013-06-06

Source: Internet Society

Abstract

This document contains a liaison from Internet Society, the IESG, and the IAB to ISO/IEC JTC1/SC6 and its National Body members.

This liaison is based on:

- ISO/IEC JTC1/SC6 N15618, which is a document from the Chinese National Body
- ISO/IEC JTC1/SC6 N15596, which is a liaison statement from the Internet Society to JTC1/SC6 concerning TISec.

Liaison from the ISOC
to ISO/IEC JTC1/SC6 and its National Body members
in relation to ISO-IECJTC1-SC6_N15618

The Internet Society (ISOC) notes the ISO/IEC National Body of China contribution to the ISO/IEC JTC1/SC6/WG7 meeting with interest and would like to contribute to the discussion on this topic.

IP protocols, including IP security protocols, require a protocol number assignment from the Assigned Internet Protocol Numbers registry. That registry is more than 50% assigned. Long standing IETF practice is to be conservative in allocating these numbers.

In the 15 years since the publication of the IPsec standards (IKE, ESP, and AH), numerous proposals for extensions, algorithms, and methods for the integration of authorization protocols such as RADIUS and Diameter have been proposed. Some of them achieved IETF consensus and were subsequently published as Requests for Comments (RFCs); others were appropriately abandoned because a proliferation of non-standard IP protocols would introduce significant cost, instability, and vulnerabilities to Internet. IPsec enjoys worldwide security expert review, is broadly implemented in the industry, and is used to protect IP in a wide variety of configurations and network topologies.

When the IETF considered TISec in August 2012, it was concluded that TISec appears to be targeted at a set of requirements that could be solved with IPsec; IKEv2 with OCSP extensions and ESP would provide the same functionality as TAI and TUE, respectively.

The IETF publishes standards for communications that pass across networks that may be owned, operated and maintained by people from numerous jurisdictions with numerous requirements for security. Communication exchanges are made less reliable by the introduction of other servers that need to be reachable in order for the communication to succeed.

The IETF has a broad base of work on IPsec that includes over 100 RFCs, with a demonstrably successful process for adding cryptographic algorithms to cryptographically agile protocols, including IPsec. IPsec algorithms include industry algorithms, e.g., Blowfish and RC5, as well as national algorithms, e.g., AES and Camellia. The IETF welcomes contributions to define code points for Chinese algorithms.

Based on the above the Internet Society requests that ISO honor the Class A liaison agreement and not start work on TISec and instead encourage the authors of such proposals to engage in the IETF open standards process.

What follows is additional detail on the similarities of IPsec and TISec.

Protocols and Services

Terminology alignment:

- TISec is a combination of TAI and TUE.
- IPsec is a combination of IKEv2 and ESP or AH.

Both IPsec and TISec are IP-based security protocols that provide basic services such access control, confidentiality, integrity, and anti-replay.

Both IKEv2 and TAI work when the initiator and responder perform a Diffie-Hellman exchange and then authenticate each other with digital signatures; TISec uses the "AS" to vouch for the certificates; IKEv2 can return certificate status information as well as using either OCSP (Online Certificate Status Protocol) or CRLs (Certificate Revocation Lists) providing the same functionality. The use of CRLs does not require another server to be reachable in order for the communication to succeed.

Authentication Mechanisms/Applications

The IKEv2 certificate-based mutual authentication mechanism uses 4 messages, regardless of whether it's a remote access scenario.

```
                 4-Pass
        Client              Server
init -+-    ------------->
      |   Request
      |    <-------------
      +-              Response
auth -+     ------------>
      |    Request
      |     <------------
      +-              Response
```

IKEv2 also supports other authentication mechanisms beyond shared secrets and certificates such as EAP and ERX; EAP and ERX exchanges can occur in as little as 6 messages.

```
                          6-Pass
                Client               Server
         init -+-    ------------->
               |   Request
               |    <------------
               +-             Response
         eap  -+-    ------------->
         erx   |   Request
               |     <------------
               +-            Response
         auth -+     ------------>
               |    Request
               |     <------------
               +-             Response
```

In addition, IKEv2 supports a mechanism to allow an IKEv2 client to request configuration, including IP address assignment, from an IKEv2 server/gateway. This mechanism provides a way for a remote client to use an IP address from an “internal” or protected subnet and access that network through the IPsec gateway.

VPN Connections

IPsec can be configured to support the “road warrior” or the “subnet-to-subnet” connection models, either by being manually configured to connect to the IPsec gateway or through the use of DNS KX records. Regardless, endpoints announce the set of addresses “behind” them, and packets would be sent in tunnel mode where the inner IP header would contain the IP addresses of the actual endpoints.

```
-----------+                                          +-----------
 Protected V                                          V Protected
 Network                                                Network

    Host---+                                          +---End Point
           |                                          |
           +-IPsecGW--[zero or more routers]--IPsecGW-+
           |                                          |
    Host---+                                          +---End Point
```

```
-----------+
 Protected V
 Network

    Host---+
           |
           +-IPsecGW--[zero or more routers]--IPsec Endpoint
           |
    Host---+
```

Luckily, overlapping subnets on either side of IPsec gateways is no longer a problem in IPv6 networks. However, in IPv4 networks where there is a subnet overlap, the IPsec gateway can implement proxy ARP and fulfill their data relay needs.

TUA and ESP

ESP and TUE seem to be the same except for where TUE changes the order of the SN and SPI and the supported algorithms.

Both TUA and ESP support "tunnel" and "transport" mode.

Algorithms

To ensure interoperability, the IETF chooses mandatory to implement algorithms, but these algorithms are not mandatory to use. There is a history of standardizing code points for national algorithms in IETF protocols: GOST (from Russian Federal), Suite B (from USA), SEED and ARIA (from Republic of Korea), and CAMELLIA (from Japan). In fact, informal conversations about code points for SM2 and SM3 have occurred. SCB2, SM1, and SMS4 could follow the same process as the other national algorithms and receive code points.

IPsec supports a wide variety of elliptic curve domain parameter sets and additional code points can be added to support national regulation.

Implementation Options

IKEv2 is designed to permit minimal implementations that can interoperate with all compliant implementations. There are a series of optional features that can easily be ignored by a particular implementation that is designed for an environment where that feature is not needed.

IKEv2 supports more authentication mechanisms than TAI because IKEv2 supports shared secrets, certificates, and other (e.g., token card, biometric, and so on through EAP, ERX, IEEE 802.1X) while TAI only supports shared secrets and certificates.

IPsec like TISec supports multiple certificate encoding formats. Though not currently defined in IPsec support for GBW certificates could be added.