Security Extension for UNI and E-NNI 2.1

IA # OIF-SEP-03.2

October 8, 2012

Implementation Agreement created and approved
by the Optical Internetworking Forum
www.oiforum.com

The OIF is an international non-profit organization with over 90 member companies, including the world's leading carriers and vendors. Being an industry group uniting representatives of the data and optical worlds, OIF's purpose is to accelerate the deployment of interoperable, cost-effective and robust optical internetworks and their associated technologies. Optical internetworks are data networks composed of routers and data switches interconnected by optical networking elements.

With the goal of promoting worldwide compatibility of optical internetworking products, the OIF actively supports and extends the work of national and international standards bodies. Working relationships or formal liaisons have been established with IEEE 802.1, IEEE 802.3ba, IETF, IP-MPLS Forum, IPv6 Forum, ITU-T SG13, ITU-T SG15, MEF, ATIS-OPTXS, ATIS-TMOC, TMF and the XFP MSA Group.

For additional information contact:
The Optical Internetworking Forum, 48377 Fremont Blvd.,
Suite 117, Fremont, CA 94538
+1 510 492 4040
info@oiforum.com

www.oiforum.com

Security Extension for UNI and E-NNI 2.0

ABSTRACT: This Implementation Agreement defines a common Security Extension for securing the protocols used in all versions of the OIF's UNI and E-NNI. It is based on previously agreed upon security requirements for UNI 2.0 and E-NNI, which call for a complete, unified, and simplified approach to security. Guidelines for using this approach in the most straightforward manner are given, and informative material on operational security aspects is included. This version 2.1 obsoletes version 1.0 of the *Security Extension for UNI and NNI*, its Addendum, and versions OIF-SEP-03.0 and OIF-SEP-03.1 of this document.

TECHNICAL EDITOR

Richard Graveman, RFG Security
for Department of Defense
15 Park Avenue
Morristown, NJ 07960 USA
+1 973 984 8780
rfg@acm.org

WORKING GROUP CHAIRS

Rémi Theillaud, Marben Products

Evelyne Roch, Ciena Corporation

Doug Zuckerman, Telcordia Technologies

Table of Contents

List of Figures

None.

List of Tables

None.

Security Extension for UNI and E-NNI 2.0

1. Introduction

1.1 Overview

This document comprises a complete and updated set of optional-to-implement security methods for the OIF's UNI and E-NNI Implementation Agreements (IAs). It contains both normative information needed to provide a simple, complete, and interoperable set of security services and informative information intended to provide implementers and users with supplementary information on security. It specifies a profile of IPsec for securing the OIF's control plane protocols for signaling and routing.

Its goals are:

- To define a complete, high-quality, interoperable security system for all control plane traffic between two network elements using a single pair of IPsec Security Associations running the (when implemented) mandatory-to-implement IPsec and IKE transforms;
- To define additional security services and mechanisms that implementations can use for fine-grained control of security;
- To provide information on operational security issues such as access controls, infrastructure protection and hiding, route filtering, denial-of-service attacks, and IPsec redirection or restoration.

1.2 Relationship to other Standards Development Organizations (SDOs)

This IA uses RFCs written by the Internet Engineering Task Force (IETF) as normative references to almost all of the work described herein. It uses, in particular, the Security Area's work on IPsec, maintenance and extensions of IPsec, and Syslog. It uses the *MPLS and GMPLS Security Framework* from the Routing Area's MPLS Working Group. It also uses the Routing Area's work on OSPF and PCE security and operational security documents written in the Operations and Management Area.

Many of the cryptographic methods (e.g., DES, AES, SHA-1, SHA-2, HMAC, and various modes of operation) are documented and standardized by the U.S. National Institute of Standards and Technology (NIST).

1.3 Acknowledgements

Fred Gruman (Fujitsu), Monica Lazer (AT&T), Scott McNown (DoD), Lyndon Ong (Ciena), Jonathan Sadler (Tellabs), and Rémi Theillaud (Marben Products) provided helpful comments.

The editor also thanks the following people for their contributions to earlier versions of this IA:

- Sid Chaudhuri
- Don Choi
- Renée Esposito
- Sheila Frankel
- Jim Jones
- Monica Lazer
- Scott McNown
- John Naegle
- Dimitrios Pendarakis
- Walter Rothkegel
- Jonathan Sadler
- Tom Tarman
- Stephen Trowbridge
- Hannes Tschofenig
- Doug Wiemer

1.4 Outline of the Implementation Agreement

This IA is divided into normative sections (Sections 2 through 6), which define protocol methods for the Security Extension, and informative sections, which contain additional operational security information, implementation guidelines, configuration suggestions, and so forth. The following sections comprise the remainder of this IA:

- Section 2 specifies the general approach to control plane security
- Section 3 covers the cryptographic methods
- Section 4 contains specific details for securing signaling, routing, and discovery protocols
- Section 5 explains how logging and auditing can be used to enhance end-to-end security
- Section 6 presents different models of trust relationships and their uses in authentication and key agreement
- Section 7 provides information on operational security issues
- Section 8 covers work on IPsec APIs
- Section 9 summarizes this IA
- Section 10 contains references

The appendices contain a pointer to a security glossary, list of acronyms, control plane security requirements identified by the OIF, the rationale for the choice of IPsec, information for implementations based on outdated versions of IPsec and IKE, and areas where ongoing work may affect this IA.

2. Control Plane Security with IPsec and IKEv2 (Normative)

2.1 Keywords

Throughout this IA, when written in ALL CAPITALS, the key words “MUST”, “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in IETF RFC 2119 [Bra97a]. The key word “NOT RECOMMENDED” carries the same meaning as “SHOULD NOT.”

The key words “Normative” and “Informative” are used inside parentheses (or inside square brackets [when already inside parentheses]). The former indicates that the following section, sub-section, or paragraph contains information required,

recommended, or suggested for implementers of this IA. The latter indicates that the following section, sub-section, or paragraph contains hints or advice for implementers or users.

2.2 Applicability Statement

This IA applies to all versions of the OIF's UNI and E-NNI specified in [UNI1.0], [UNI1.0r2], [UNI1.0r2r], [UNI2.0], [UNI2.0-RSVP], [E-NNI1], [E-NNI2], [E-NNI-OSPF1] and [E-NNI-OSPF2]. It covers all control plane protocols used for signaling, routing, and discovery that run over IPv4 [Pos81] or IPv6 [DH98]. It can also be applied to protocols not running over IPv4 or IPv6 (e.g., IS-IS) by using encapsulation.

Since the publication of [SecExt] and [SecAdd], (1) the OIF has started new work on the UNI and E-NNI and released Implementation Agreements for UNI 1.0r2, UNI 2.0, E-NNI signaling, E-NNI routing, and logging and auditing; (2) the IETF has continued to revise and enhance IPsec, IKE, and the list of associated cryptographic transforms; and (3) suggestions to clarify certain aspects of [SecExt] have been received. This IA keeps the work started in [SecExt] up to date and aligned with current practice by addressing these items.

2.3 Internet Protocol Security (IPsec)

For an overview of the components of IPsec, see the IPsec Roadmap document [FK11]. IPsec [KS05] and ESP [Ken05a] and MUST be implemented.

IPv4 implementations that provide NAT traversal MUST follow [Hut05]. See also [AD03] (Informational) for a discussion of NAT traversal requirements.

AH [Ken05b] MAY be implemented, but use of ESP is preferred over AH in all cases.

Transport mode IPsec SAs are NOT RECOMMENDED except in cases specifically mentioned herein (e.g., for [RFC4891] tunnels).

Caution (Informative): If IPsec Tunnel Mode is used and the implementation treats these IPsec tunnels as virtual interfaces (see, for example [ELM10]), these virtual interfaces may be assigned DCN routing protocol costs that, if advertised by the DCN routing protocol, cause traffic between other systems to be routed inappropriately. For IPsec implementations that have this side effect, inappropriate DCN routing protocol costs due to such virtual interfaces should not be advertised across the DCN routing protocol. Note, as an additional alternative, that [KS05] allows IPsec Transport Mode to be used with certain restrictions.

2.4 Internet Key Exchange (IKE)

IKEv2 [KHNE10] MUST be implemented. For additional information about IKEv2, see [Kra03]. To support public key authentication (e.g., digital signatures), [Kor07] MUST be implemented. For implementations of IKEv2 that allow use of a legacy authentication system, [Tsc08] SHOULD be implemented. Implementations of IKEv2 SHOULD measure resource consumption and use the initial exchange with cookies whenever they determine that a denial of service attack may be occurring.

2.5 IPv6 Considerations

- This IA specifies use of ESP and IKE with either IPv4 or IPv6.
- The following options are not covered in this IA and SHOULD NOT be used with IPv6 traffic secured according to these methods: link-local and deprecated site-local addresses, NAT traversal, and Mobile IP.
- Note that IPv6 implementations of IKEv2 MUST support the larger minimum MTU of 1280 and SHOULD support an MTU of 3000 as specified in [KHE08].
- Note that IPv6 subnet renumbering may break existing IPsec SAs, which then need to be re-established. Unique local addresses (ULAs, [HH05]), which avoid this problem, MAY be used.
- When using ESP or IKEv2 with IPv6, ICMPv6 MUST be handled as specified in [KS05]. See also [DM07] for guidelines on filtering ICMPv6 traffic.
- Either IPv6 Autoconfiguration or DHCPv6 MAY be used for dynamic address assignment with IPv6. The security methods specified in this IA, however, are generally meant to be used with well-known, persistent addresses.
- IPv6 packets using IKE or ESP as specified herein must be allowed to traverse firewalls and may be transported through IPv4 transition tunnels. Note also that IPv6 packets protected with ESP Tunnel Mode MAY be encapsulated with an IPv4 outer header [GPST07].
- Draft [ELM10] describes using IKEv2 to configure IPsec over IPv6 as a full-featured virtual interface with multiple prefixes, link-local addresses, multicast listener discovery, etc. This type of generalization may be useful, for example, for simultaneously configuring protection for both routing and signaling traffic.
- Additional information on securing IPv6 and, in particular, transition mechanisms for IPv6 can be found in [DKS07] and [NIST10].

3. Cryptographic Algorithms and Transformations (Normative)

In this IA, AES replaces DES and Triple DES as the REQUIRED confidentiality algorithm for ESP and IKE, because it is more efficient, it is presumed to offer better security, and it can be used in new modes for integrity or for combined integrity and confidentiality. This change has additional benefits and consequences. First, if AES is also used as the ESP (and IKE) integrity algorithm, the total number of algorithms in and code size of implementations is reduced and potential problems with weak hash functions are avoided. Second, AES is defined with new, more efficient modes of operation (counter mode [Hou04] and combined confidentiality and integrity mode [Hou05], [VM05], [NIST07]). Third, it is recommended that the security of IKE key exchanges be increased to match the increased level of security that comes with using AES.

3.1 ESP Transforms

The REQUIRED-to-implement suites for IPsec ESP are defined in [LS11] and [BP11]. Suite-B-GCM-128 and Suite-B-GMAC-128 are REQUIRED.

The other two suites in these documents, Suite VPN-B in [Hof05], and all other ESP transforms, including user-defined algorithms, MAY be implemented. See also [Man07] for a correction on the handling of the NULL authentication option.

3.2 IKEv2 Transforms

For a current list of assigned values, see [IANA-IKE]. The REQUIRED-to-implement suites for IKEv2 are defined in [LS11] and [BP11]. Suite-B-GCM-128 and Suite-B-GMAC-128 are REQUIRED. Implementations SHOULD support pre-shared secrets as well as the certificate-based methods in [BP11]. To minimize IKEv2 message size, certificates should be pre-installed, but for other cases the IKEv2 Certificate Encodings 12 and 13 (hash and URL) MUST be implemented.

The other two suites in these documents, Suite VPN-B in [Hof05], and all other IKEv2 transforms, including user-defined algorithms, MAY be implemented. See, for example, [LK08] for eight new Diffie-Hellman groups, three traditional mod-*p* groups with subgroups of large prime order, and five elliptic curve groups over prime fields. Note that implementations including the elliptic curve groups 19-21 in [LK08] need to heed the corrections to [LK08] noted in [FS10].

Implementations that provide AES counter mode for ESP MUST implement it for IKEv2 according to the specification in [SMM10]. Implementations of combined mode algorithms for ESP SHOULD also be capable of using these to protect IKEv2 traffic as described in [BM08].

4. Securing the OIF Control Plane Protocols (Normative)

(Informative) The document describing IPsec for securing IP Storage [Abo04] was used as a guide to specifying the original version of this profile of IPsec. The approach in this IA is similar, but the methods have been updated since that document appeared.

4.1 Signaling Protocols

IPsec selectors for ESP Tunnel Mode SHOULD be set up to secure all IP traffic between each pair of network elements using RSVP-TE signaling.

IPsec selectors MAY, however, be configured to protect specific protocols. RSVP-TE is IPv4 Protocol 46 or IPv6 Next Header 46.

Consideration SHOULD also be given to setting up IPsec-secured tunnels to access infrastructure services upon which signaling depends and which are not secured by other means. Examples may include NTP, DNS, SNMP, and Syslog.

(Informative) The RSVP messages used in the OIF's signaling protocols do not use the IPv4 Router Alert or IPv6 Next Header 0, which would be incompatible with the use of the confidentiality service of ESP.

(Informative) The RSVP policy and integrity objects and the TCP integrity object (MD5 checksum), if used with these methods, provide no additional security.

4.2 Link State Routing Protocols

The IETF, in [BMY06], has enumerated the sources, actions, and consequences of security threats to routing protocols. The consequences of such attacks (see again [BMY06]) can include disclosure of network configuration data, deception, disruption, and losing control of network functionality. The resulting damage can include congestion, black-holing, looping, partitioning, churning, instability, overload, starvation, eavesdropping, or delay. Attacks against routing protocols can disrupt the establishment of peering relationships; interfere with protocol components such as election of a designated router; forge or modify routing information; eavesdrop on the content or traffic patterns of routing information; corrupt the internal state of routing databases; or replace an authorized router with an imposter. Although the routing protocols used in the E-NNI do not determine IP forwarding, the consequences of compromising them have similar effects on the use of optical resources in the data plane.

This IA defines cryptographic protection for the OSPFv2, OSPFv3, and IS-IS routing protocols as they may be used in the OIF's E-NNI. Cryptographic protection does not cover (1) system security for routers; (2) problems that result from faulty implementations; (3) physical, personnel, and environmental security issues; (4) protection based on packet inspection by firewalls or intrusion detection systems; (5) security for other infrastructure protocols such as DHCP, DNS, or IPv6 neighbor discovery; or (6) certain denial of service attacks that result, for example, from flooding routers.

Implementations of the OIF's Security Extension for UNI and E-NNI 2.0 SHOULD provide the same security services for the routing protocol advertisements between control domains as for the signaling protocol messages themselves. If routing controllers communicate along the same path for which IPsec SAs to secure signaling are specified in the Security Policy Database (SPD), the SPD SHOULD specify use of these same SAs for routing protocol messages, but see the cautionary note in Section 2.3, above.

(Informative) Securing link state routing protocol messages with the OIF's Security Extension for UNI and E-NNI 2.0 prevents modification, address spoofing, forgery, replay, and "cut-and-paste" attacks against these protocols. It also can provide confidentiality, hide the names of the endpoints, and disguise the actual amount of routing protocol traffic transmitted, which inhibit network mapping attacks. Link state routing protocols, however, rely on distributing accurate topology and configuration information across a network. To accomplish this, the switches trust each other to act properly. Therefore, a compromised or misconfigured switch can do a lot of hard-to-detect damage. Protocol security between adjacent switches cannot solve this problem.

(Informative) To provide end-to-end routing protocol security, digital signatures on the messages can be used. Such an approach has been proposed not only for routing protocols ([Per88], [Ste93], [MBW97]) but also for secure email, XML, syslog, and SIP.

Methods exist to provide adequate security with signatures only 20 to 25 bytes long [BLS01] and to combine multiple signatures into a single, aggregated signature [Bon03], which lessen potential objections due to extensive message overhead. Methods such as these may be proposed for future OIF Control Plane protocols.

(Informative) Lacking an efficient, standardized method for signing OSPF or IS-IS payloads, the OIF has provided a different approach (see Section 5, below). It has specified a flexible, dynamically configurable logging and auditing capability, which, among other uses, can be turned on to generate a trace of a Control Plane protocol whenever needed. This capability is based on the syslog protocol as specified by the IETF. Although the syslog UDP transport mechanism (unidirectional, unfragmented packets) is chosen to minimize overhead, logging may add to network congestion or overload conditions. Operators may choose to turn logging off in such situations, manually or automatically.

4.2.1 Implementations not Using the Security Extension

OSPFv2 implementations not using the OIF's Security Extension for UNI and E-NNI 2.0 SHOULD provide OSPFv2 with the option for cryptographic authentication specified in Sections D.3, D.4.3, and D.5.3 of RFC 2328 [Moy98]. Implementations SHOULD also provide the HMAC-SHA-1 method specified in [Bha09b]. IS-IS implementations not using the OIF's Security Extension for UNI and E-NNI 2.0 SHOULD incorporate the authentication mechanism specified in RFC 5310 [Bha09a].

(Informative) Note, however, that these mechanisms do not include automated key management. See [MBJW10] for a thorough discussion of the issues with these methods. The IETF's KARP Working Group is chartered to address algorithm agility and key management for routing protocol security, and implementers should track this work and incorporate improvements.

4.2.2 Securing OSPFv2 with the Security Extension

Implementations of [NNI-OSPF1] or [NNI-OSPF2] MUST allow for IPsec protection of OSPFv2 messages. Wherever practical, they SHOULD do this for unicast messages with the same IPsec SAs used for signaling. Otherwise, ESP selectors for OSPFv2 MUST specify IPv4 Protocol 89 or IPv6 Next Header 89.

To aid in the diagnosis of multiple-hop or end-to-end security problems, implementations SHOULD also implement [LogAud]. As an alternative to deploying logging at all E-NNI nodes in a control domain, implementations MAY log only at certain levels and MAY use digital signatures on LSAs (link state advertisements) within a level (i.e., they MAY implement [MBW97] in addition to the methods in this IA). Note, however, that summarization of routing information (LSAs) does not allow preservation of signatures.

4.2.3 Securing OSPFv3 with the Security Extension

OSPFv3 is defined in [Col08] and uses the security methods specified in [GM06][1]. It makes essential use of the IPv6 All OSPF Routers IPv6 multicast address and defines IPsec ESP as the security mechanism for OSPFv3. Implementations of ESP for OSPFv3 MUST follow the guidelines in [WGI08] for supporting IPsec ESP multicast traffic. If modes of operation requiring a unique initialization vector (IV) are implemented, the methods in [MW10] MUST be followed.

IKEv2 is a two-party protocol; it cannot establish keys for multicast. When using IPsec to secure OSPFv3 multicast traffic, RFC 4552 [GM06] specifies manual keying. This is an unsatisfactory solution, because it imposes administrative overhead, does not scale well, and limits the functionality of IPsec. More work is needed on automated group key management for OSPFv3.

4.2.4 Securing IS-IS with the Security Extension

IS-IS routing implementations MUST allow for IPsec protection of IS-IS messages. Because IS-IS runs directly over a link layer protocol, not over IP, GRE [Far00] MUST be used to encapsulate messages between the IS-IS peers protected with IPsec. The protocol stack IS-IS/GRE/ESP/IP/<Layer 2> MUST be used. The IPv4 Protocol and IPv6 Next Header are 50 for ESP. The ESP Next Header is 47 for GRE. The version and Reserved0 fields in the GRE header MUST be set to 0. Because ESP secures GRE and IS-IS, the methods in [Dom00], [LA08], or [Bha09a] SHOULD NOT be used. Wherever practical, implementations SHOULD protect IS-IS over GRE with the same IPsec SAs used to protect the signaling traffic between the same two points. To aid in the diagnosis of multiple-hop or end-to-end security problems, such implementations SHOULD also implement [LogAud].

(Informative) Note: No description of a signature option for IS-IS, which would correspond to [MBW97], exists. Such capability is for future study.

4.2.5 Additional Issues with Securing Routing

Management interfaces to routers implementing the OIF's E-NNI routing protocols, in particular implementations of MIBs for OSPFv2, OSPFv3, and IS-IS, SHOULD be secured with the methods specified in [SecMang].

(Informative) The most general security solutions for protocols like OSPF and IS-IS allow the link state protocol to work correctly as long as one uncorrupted path between any two points exists. There may be multiple failures, and the corrupted routers may in fact be cooperating to carry out an attack. Perlman (in [Per88] and [Per00]) has shown how to how achieve security in such cases, which are called "Byzantine failures." Addressing such threats, in whole or in part, is for future study.

[1] This standard recommends protecting OSPF messages with IPsec ESP, which also provides confidentiality, although it does not provide end-to-end security against the case of a misbehaving router. The most significant difference between [GM06] and this IA is that whereas [GM06] *allows* Tunnel Mode, this IA *recommends* it.

4.3 Discovery Protocols

Discovery protocols are not currently defined for the OIF UNI and E-NNI. Use of Link Management Protocol (LMP) defined in the OIF UNI 1.0 Release 1 was removed in subsequent versions of the UNI. The material in Section 4.3.1 is provided for information only. If work on discovery resumes, security requirements and specifications for securing discovery protocols ought to be reconsidered.

4.3.1 Use of the Security Extension with LMP

The Link Management Protocol (LMP, RFC 4204 [Lan05]) proposes using IPsec to secure LMP, which is, in principle, consistent with this IA. LMP uses UDP port number 701, but the LMP standard recommends securing all UDP traffic between the parties using LMP with the same IPsec SAs. However, the following notes apply in addition to the specification of IPsec in [Lan05]:

1. As specified above, the confidentiality service with ESP MUST be implemented and may be used as required by local policy.
2. The specification of IPsec in [Lan05] is updated with the newer transforms and protocols for IKEv2 and ESP, as specified above.
3. Use of IKEv2 with pre-shared keys is REQUIRED wherever manual keying is specified. ([Informative] The same applies to securing LMP with IKEv1.)

As for signaling and routing protocols, wherever practical, LMP MAY share SAs with other protocols protected by the methods in this IA. That is, when LMP messages are sent between systems using the Security Extension, the SPD SHOULD be configured so that all LMP messages are protected with the same IPsec SAs as other traffic secured with the Security Extension. Note that this applies only to unicast messages.

Management interfaces to systems implementing discovery protocols SHOULD be secured with the methods specified in [SecMang].

4.4 Path Computation Element Protocol (PCEP)

Security for OIF control plane routing protocols using PCEP [VR09] or PCE discovery (e.g., [Rou08]) and for the PCE servers may be critical. PCE is an attractive target to attack: a compromised or spoofed server or protocol message can result in a complete breach of the control plane. Confidentiality is also a concern.

PCEP runs over TCP port 4189. Securing all communications between a NE and PCE with the methods in this IA is RECOMMENDED. A yet to be defined solution based on TLS could provide an adequate alternative.

If PCE discovery is added to OSPFv2 as in [Rou08], then signing and verifying the advertisements as described in [MBW97] is an OPTIONAL enhancement in addition to hop-by-hop security.

5. End-to-End Security with Logging and Auditing (Normative)

Using IPsec as defined in this IA can ensure that control plane protocol messages cannot be spoofed, modified, or replayed by unauthorized parties, but it cannot guarantee that intermediate Network Elements (NEs) implement the protocol correctly. Incorrect behavior may result from implementation errors, misconfiguration, or a security breach. It is normal for signaling and routing protocols to modify messages, so incorrect behavior needs to be defined as violating the definition of the protocol (for example, in the case of a routing protocol that summarizes multiple advertisements, reporting an incorrect summarization).

The OIF's Logging and Auditing with Syslog version 1.1 IA [LogAud] defines the PROT@26041 Structured Data item, which allows specific control plane protocol messages to be logged on receipt or transmission.

If, for example, signaling or routing messages traverse multiple hops, it is possible with this mechanism to isolate incorrect behavior. Then, appropriate action can be taken with respect to the incorrectly behaving systems. The following example illustrates how this can be done.

Suppose that:

- a message conveying the intention *X* is sent from *A* to *E* with three intermediate hops, *B*, *C*, and *D*, in that order
- the message has IPsec integrity and data origin authentication applied on each of the four hops
- a message with a different, misrepresented intention *X′* arrives at E.

The first step is to turn on logging of such messages as they are received and transmitted. In this example, that means messages transmitted from A to B, B to C, C to D, and D to E. Then:

- if a systems fails to generate a requested log message, incorrect behavior at that system has been located
- if a system logs incoming message(s) with intention X and a corresponding outgoing message with a different intention X′, incorrect behavior at that system has been located
- if one system logs an outgoing message M and the next in line logs a different incoming message M′, then one of the two is logging something different from what it is doing or seeing, and incorrect behavior has been isolated to these two systems

Note 1: This example illustrates the need for tools to control log file generation, reduction, and on-line monitoring.

Note 2: The above process may, of course, be optimized in practice. In this example, for instance, one could start by logging messages at the endpoints and in the middle, at C: if C logs intention X, the problem occurs afterwards; if C logs intention X′, the problem has already occurred before, and so on.

Note 3: In practice, this process should take into account whether the problem is occurring across certain administrative domains, with certain types of equipment, with a new release of software, and so forth.

Note 4: Network administrators should ensure that their Syslog implementation can accommodate sufficiently long log messages to record the necessary control plane protocol information.

6. Identity and Keying in IKEv2

6.1 Required Methods (Normative)

Implementations of this security extension for the UNI and E-NNI MUST bind the endpoints of each SA to a list of sending and receiving SC PC IDs for signaling or RC PC IDs for routing. A single SA MAY be bound to both SC PC IDs and RC PC IDs. Implementations MUST verify that messages received on each SA are appropriate for the associated SC PC IDs or RC PC IDs.

Implementations MUST support certificate-based public keys and SHOULD support pre-shared keys. Certificates MUST be associated with lists of SC PC IDs or RC PC IDs allowed for each end of a SA established from these keys. Actual SAs MAY be bound to IDs derived from subsets of the allowable lists. Manual keying MUST be implemented as a testing and debugging tool but MUST NOT be used to secure unicast traffic in production systems.

Pre-shared secrets are simple and straightforward, but they do not scale well, over space or time. Therefore, public key authentication is REQUIRED. Because the IETF's PKIX documents ([CSFBHP08] etc.) contain many options, and the ISAKMP, IKE, and IKEv2 documents do not specify how to use these, interoperability has been hampered. A "PKI for IPsec" Profile is now defined (see [Kor07], *The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX*, RFC 4945), and guidelines for using this profile with the OIF's Security Extension are given here:

- Revocation lists SHOULD be checked but CRLs MUST NOT be sent in IKEv2 messages. The OCSP method in [MT07] MUST be implemented. (If standardized, the extension in [SH11] MUST also be implemented.) The out-of-band method in Section 3.2.3 of [Kor07] MAY be implemented, in which case certificates SHOULD contain CRL distribution points, and Delta CRLs SHOULD NOT be used.
- Network elements using this Security Extension may communicate with a small and stable set of other NEs, so (1) certificate retrieval via Hash and URL is REQUIRED and (2) certificate caching is RECOMMENDED.
- Except for self-signed certificates used as trust anchors, all certificates must be X.509 Version 3.
- Implementations supporting X.509 Version 3 certificates MUST allow an empty Subject field and SubjectAltName extension that specifies the SC PC IDs or RC

PC IDs that may be bound to this certificate. Implementations SHOULD support partial matching with substrings, wildcards, or regular expressions. This information MUST be used to bind sub-lists of SC PC IDs or RC PC IDs to a SA when the SA is created.

- (Informative) Service providers issuing certificates to users, either directly or through a third party, should consult RFC 4809 [BTL07], Requirements for an IPsec Certificate Management Profile, for a checklist of PKI lifecycle items to take into account.
- (Informative) Freely available tools to help generate certificates include OpenSSL [HowTo] [HP-UX] and Simple-VPN [SJB10].

6.2 Alternate Approaches (Informative)

If a lighter-weight approach to PKI is desired, several alternatives exist, e.g., self-signed or organizationally signed certificates such as the IETF's BTNS. In all cases, however, identity information at SA creation MUST be used to bind SAs to SC PC IDs or RC PC IDs as specified in Section 6.1.

Implementations may use Stand-Alone BTNS as described in [TBW08], Problem and Applicability Statement for Better than Nothing Security (BTNS), with unsigned or self-signed certificates. They may use either symmetric or (preferably) asymmetric BTNS. This mode of operation is better suited to use within a single carrier's domain or between carriers who have established some out-of-band mechanism to verify the configuration. It is not well-suited for authentication of users at the UNI. The extensions to the IPsec PAD and SPD described in [WR08] need to be implemented to use BTNS. This includes the ID type PUBLICKEY in the PAD and the BTNS_OK flag in the SPD. Somewhat better control can be maintained by avoiding wildcard PAD entries of type PUBLICKEY.

RFC 4430 [SKTV06] describes a method called KINK for using Kerberos with IKEv1 and points out a list of changes in IKEv2 that need to be considered to implement KINK for IKEv2. Therefore, use of KINK with IKEv2 is for future consideration.

7. Operational Security (Informative)

Basic background information on operational security practices for service providers is contained in [Kae07]. Additional information specific to MPLS and GMPLS networks is contained in [Fan10]. This material is not replicated here but assumed as a starting point.

7.1 Security for Cryptographic Processors

The quality of cryptographic implementations (which entails more than timing measurements!) varies considerably. This section points out areas commonly known to contain vulnerabilities and provides pointers to additional information.

Modern cryptographic processes have resisted direct attacks but tend to be vulnerable to so-called side channel attacks that extract secret information from timing, power consumption, acoustical or electromagnetic emanations, or the behavior of a system when faults are induced. Typing at a keyboard can be read by measuring the vibrations on a

nearby windowpane. CRT and LCD displays can be read from large distances. AES keys can be extracted by measuring cache hit and miss timings. Using cryptographic keys can leave a tell-tale pattern in the power output at a USB port. Some ciphers inadvertently reveal their secret keys if a calculation error occurs or is induced. Keys stored in DRAM remain partially readable for minutes after the power is shut off. Many more examples of this sort exist. The seriousness of these vulnerabilities varies from case to case.

Many of these vulnerabilities can only be exploited with physical access or proximity to the cryptographic equipment. In these cases, personnel and physical access control security is important. "Logical access control" can also play a role—the cache hit attack can only be carried out by a program running on the same chip.

Almost all cryptographic processes depend on some randomness, which is usually provided by a software-based pseudo-random number generator (perhaps with some hardware generated randomness as an assist). The randomness requirements for cryptographic processes are much stronger than those for other computing tasks (e.g., running simulations). Widely used and longstanding implementations of systems like SSL and Kerberos version 4 have fallen victim to attacks on their random number generators. See [ESC05] and [Gut98] for more information.

Software is flexible, subject to reverse engineering, and rarely free of errors. It can be updated intentionally or unintentionally. In some spectacular cases, it contains features totally unrelated to its advertised purpose. It follows an entire life cycle of design, implement, test, deploy, update, and discard. Users are adept at working around software bugs, but cryptographic software does not have this luxury—the attacker exploits the bugs and often publicizes them for others to exploit.

Finally, many systems incur additional vulnerabilities because they are used in incorrect configurations or with an improper choice of options. Three general references on these topics are [NIST09], [Gut04], and [Koç09]. Research results on side channel attacks and other cryptographic implementation issues are available from many sources, but see, in particular, the proceedings of the annual Cryptographic Hardware and Embedded Systems conference.

7.2 Perimeter Access Control and Ingress Filtering

Packet filters exist on routers, firewalls, security appliances, and end hosts. Every implementation of IPsec contains one (in each direction). Background information on packet filters is covered in [SH09]. Typically, they examine addresses, protocols, and port numbers. Packet filters should be configured to drop the following traffic:

- *Address enforcement*: Source addresses of packets need to be appropriate for the interface on which they arrive. Packets with internal source addresses should not be accepted from external links, and outgoing traffic should have an internal source address. Local addresses should not be routed beyond their defined scope.
- *Disallowed services*: Incoming or outgoing packets using services not permitted on the internal network (e.g., SMTP, HTTP, or NNTP) should be dropped.

- *Inappropriate transit traffic*: If multiple external parties have access to, say, an edge router providing some service, then packet filters should ensure that these users cannot interfere with each other, learn too much about each other, or establish unauthorized communications with each other. The router is providing services to the outside from the inside, not communications between outsiders, and such traffic should be dropped.
- *Service not allowed to or from a given direction or address*: Certain services, e.g., network management, may be restricted to certain internal or external source or destination addresses. Traffic for these services not matching the allowed addresses should be dropped. For the OIF's Control Plane, such rules should be applied to signaling, routing, and discovery protocols as well as management traffic.
- *Known attacks*: Packets matching known attacks due to their protocols or port numbers or attempting to probe a private network with address or port scans should be dropped. Stateful filtering of UDP should be used where appropriate (i.e., incoming packets are only allowed in response to prior outgoing requests).
- *Ill-formed packets*: Packets with excessive fragmentation, disallowed IPv4 options or IPv6 extension headers, abnormal lengths, and so forth should be dropped.
- *Security policy violations*: Certain protocols may be required to use security services (e.g., SSL, TLS, SSH, Kerberos, IPsec, or SNMPv3). Traffic that violates this policy should be dropped.

Filtering certain traffic involves tradeoffs. ICMP or ICMPv6 is a good example. On the one hand, these messages may contain information needed to keep the network running properly. On the other hand, they may be used improperly as probes or as parts of other attacks. These should be analyzed on a case-by-case basis rather than being subjected to a blanket policy.

Tunneling protocols and open relays potentially violate packet filtering rules and need to be given special attention. Tunnel endpoints (e.g., GRE or IPv6 over IPv4) behind a packet filter potentially deliver traffic that violates the packet filtering rules. Therefore, the tunnel endpoint must be configured so that it is physically or logically outside of the network protected by the packet filter. Open relays at the application layer (e.g., SMTP or HTTP) or at the network layer (e.g., IPv4 source routing or IPv6 Type 0 Routing Headers) potentially violate addressing rules and need to be treated similarly.

Questions often arise about access to production networks for remote monitoring, maintenance, or troubleshooting. Requests for access to production networks from development networks or by vendors need to be handled according to local policy, because these inherently involve tradeoffs between cost and convenience on one hand and security on the other hand.

Packet filters are usually configured from one of two basic approaches, sometimes called the "stance." The stance can be characterized by whether the last rule is "allow

everything not forbidden above," or "forbid everything not allowed above." The former may be appropriate for providing public Internet service, but the latter is more suitable for networks providing a business infrastructure.

Additional protection beyond what packet filters can provide may be obtained by using application level gateways or intrusion detection systems. For additional information, see [SH09].

7.3 Applying Local Policy to RSVP Message Contents

RSVP-TE is the signaling protocol commonly used for the UNI and E-NNI [UNI2.0-RSVP] [E-NNI2]. RSVP-TE messages consist of a header containing an eight-bit message Type and length followed by a list of type-length-value (TLV) objects. The objects are defined by a major value called Class Number and a minor value called C-Type. RSVP-TE is designed for extensibility. In particular, unrecognized messages with Class Numbers 192–255 (so-called 11bbbbbb Class Numbers) are supposed to be ignored but passed along unchanged [Bra97b]. Furthermore, the last four values in this range, 252–255, allow for vendor-defined extensions, which the OIF uses as well [PrivExt].

If a NE supports both a UNI-N and E-NNI, two separate E-NNIs, or an E-NNI and RSVP-TE-based I-NNI), and it moves signaling messages between these two reference points, then it may pass unrecognized 11bbbbbb objects across this interface on the premise that this might be appropriate for compatibility with future extensions. On the other hand, signaling protocols must be protected from abuse as much as possible. This is particularly important for inter-domain interfaces, i.e., UNI-N and E-NNI. Network operators may want to prevent (a) using the signaling channel for unauthorized user-to-user communications or (b) overloading the signaling channel and degrading service for others or burdening the control plane resources more than necessary. At the same time, vendors want to produce robust implementations that are immune to protocol changes affecting only other entities.

This situation suggests that UNI-N and E-NNI implementations provide a table-driven mechanism to allow network operators to specify how to treat 11bbbbbb objects in signaling messages. This is somewhat similar to packet filtering, but at a different layer, because it works inside a single message. At a minimum, implementations should allow filtering to specify:

- permit-deny Class Number
- permit-deny Class Number + C-Type

Semantics for resolving the precedence among filtering rules are familiar to designers and users of packet filters.

The filtering rules should also convey how policy violations are handled. Messages that violate the network operator's policy should be logged with a Severity higher (lower numbered) than Notice (5) [LogAud]. The simplest protocol response to such messages is to drop them silently. (Other approaches are for further study. In all cases, mitigating denial-of-service attacks should be considered.)

Implementations should also support additional RSVP-TE content filtering capabilities based on the RSVP-TE message Type, state of the connection, subobjects contained in the object, size of the object, frequency of messages containing this object, the identity of the user, and so forth.

Implementations should also provide general usage statistics for the signaling channel including but not limited to user identities (where applicable), message counts, message types, message sizes, total byte counts, and errors.

7.4 Network Element Access Control and Traffic Visibility

Using IPsec ESP at a NE means that a security device such as a perimeter packet filter, firewall, or intrusion detection system may not be able to examine the contents of the packet it otherwise would. This is somewhat analogous to the case of the tunnel endpoint covered in Section 7.2. This can be handled in any of three ways, depending on local policy:

1. Terminate IPsec at the security device and treat the internal network as trusted.
2. Replicate the functionality of the security device within the network element at or above the IPsec layer. Note that IPsec requires a minimal amount of packet filtering to enforce its security policy.
3. Configure the security device to trust the network element to communicate with certain external addresses using IKEv2 and ESP, and allow such traffic to pass.

Implementations SHOULD provide wrapped ESP as described in [GMB10] for installations needing IPsec's authentication and integrity, not needing confidentiality, but requiring this type of packet inspection at intermediate points. Such intermediate points should also implement [KM10].

Protocols accessing a network element but not using IPsec may be authenticated and secured with the methods specified in [SecMang] or with application-specific security methods (e.g., DNSSEC or syslog signatures).

7.5 Infrastructure Hiding

Service providers may wish to hide details about the configuration, capacity, or other aspects of their networks. Thus, they may wish to foil probes (traceroute, for example) into the hop counts, timing, or other telltale signatures of their networks. See [Gil07] for a discussion of hiding a service provider's infrastructure. Several basic rules can be applied:

1. Use a different networking infrastructure (say, IPv4 over MPLS or IPv6 tunnels) for all of the P routers and network elements between PE routers. This makes the internal network opaque at the external network layer and thereby prevents probes into the internal topology.
2. Separate control plane, data plane, and management plane functionality in hardware and software. This helps limit the potential damage from an attack on any one of these, and it may allow each plane to implement additional security measures separately.

3. Separate resources, such as processors and memory, allocated to different users or external applications to make external probes more difficult.
4. Separate forwarding and routing processes for different services for the same reason.

7.6 Route Filtering

Route filtering complements routing protocol security and packet filtering. Just as the source address of every packet has to make sense for the interface on which it arrives, any routes that are advertised have to correspond to addresses appropriate for the given interface, and any IP routing protocol messages indicating otherwise should be ignored by the routing protocol, logged, and investigated.

7.7 IPsec Redirection and Session Resumption (Normative)

Optimized restart capabilities may be important to carriers who operate servers connected to many clients with IPsec. Two ideas have emerged: redirection and session resumption. The goal is simply to reduce the overhead of reestablishing IKEv2 connections after a failure, either on a different system or on the same one, respectively.

The main issues are key management, denial of service, and obtaining a new server address.

Implementations MAY provide IPsec Redirect (i.e., Gateway Failover) as described in [DW09]. This document is oriented towards VPN or remote access servers using IKEv2, but the methods can be used with any applications of IKEv2.

Implementations MAY provide IPsec session resumption as defined in [ST10]. This is also designed with VPN or remote access servers using IKEv2-EAP in mind. The mechanism is patterned after TLS session resumption (defined in RFC 4507). The idea is to store IKEv2 state in an encrypted ticket or cookie in the client, and restart an IKEv2 SA efficiently when presented with a valid ticket. This may happen after a server reboots or has intermittent network outages that time out IKEv2 SAs.

7.8 Defending against Denial-of-Service Attacks

Denial of Service (DoS) attacks can target communications links, processing power, memory (e.g., internal table sizes), or even disk space. The first goal is to continue operations on legitimate tasks—shutting down means “attacker wins.” The second goal is to pinpoint and eliminate the source of the attack.

Security mechanisms themselves need to follow the rule, “first, do no harm.” For IPsec ESP or AH, this means being able to verify and discard inauthentic traffic at line speed, so that these protocols actually protect against high-layer attacks such as TCP SYN flooding rather than acting as an enabler for a DoS attack. For IKEv2, this means being able to use the cookie mechanism to ensure that a two-way communications channel exists before committing state allocation or expensive processing resources.

Protocols should be designed so that:

- Resources must be allocated by the initiator first

- The responder can delay establishing state until two-way communications exist
- Attacks cannot be amplified by or reflected off of third parties

Network operators should consider the following measures to minimize the effects of DoS attacks:

- Keep up to date with known attacks, mitigation methods, and security patches
- Establish a working relationship with the appropriate computer emergency response and law enforcement organizations
- Deploy intrusion detection or intrusion prevention systems able to detect and repel known attacks
- Protect all critical systems; for example, an internal network may be protected but rendered useless by an attack on an external DNS server (see Section 7.9)
- Provide excess capacity and diversity (vendors, locations, software, etc.)

7.9 Domain Name System (DNS) Security

The Domain Name System (DNS) is vulnerable to the usual protocol spoofing attacks as well as direct attacks against the contents or consistency of the database itself. Many of these attacks result in denial of service, but potentially more serious compromises are also possible. DNS servers lying outside of the normal security perimeter may be particularly vulnerable.

Generally, the design of DNS presumes that all information is public, and no confidentiality services are provided for DNS transactions. Organizations wishing to hide internal DNS names may do so with well-known techniques that split the namespace into a global portion and an internal portion only accessible inside a secured perimeter.

In addition to applying normal host and network security measures to DNS servers and ensuring that up-to-date DNS software is correctly and securely installed, two protocol security standards exist. The first, called TSIG, is defined in RFCs 2845 [Vix00]. Cryptographic methods for TSIG are listed in RFC 4635 [Eas06]. If IPsec is not used, TSIG should be used to secure zone transfers. Note that the HMAC-MD5 mechanism, though marked mandatory, must no longer be used. RFC 3007 [Wel00] describes two methods for securing dynamic updates.

Securing the DNS database itself for queries and responses is a more complicated process called DNSSEC and described in [Are05a], [Are05b], and [Are05c]. The DNS implements a hierarchical, distributed database. The integrity of the entire hierarchy or parts of it is ensured with digital signatures contained in SIG records. The keys to verify these signatures are in KEY records, which are also signed and can be verified, in turn, by starting at a “trust anchor” and descending through the hierarchy. Additional mechanisms are provided to tie the keys together across delegation points and to report securely that a record does not exist. All of this takes some effort to deploy the right software and sign the zones of interest, but, increasingly, progress is being made deploying DNSSEC.

For additional information on securing DNS including a more complete description of these methods and checklists for deploying them, see [CR10].

7.10 Dual-Stack and IPv6 Transition Operations

The worldwide exhaustion of IPv4 addresses is likely to compel service providers to support both IPv4 and IPv6. This is also likely to become the de facto method of operation for a long time. Security policy has to be applied equally to both IPv4 and IPv6, and it is critical that neither one can compromise the security of the other, for example, through tunneling protocols.

IPv6 addressing, header processing, ICMPv6, and new capabilities such as routing headers, mobility, and autoconfiguration all have consequences for security. Some of the distinguishing features of IPv6, besides the 128-bit addresses, are that:

- Interfaces normally have multiple IPv6 address, and these often change over time
- Multicast is an essential part of the protocol, and layer 3 broadcast has been eliminated
- IPsec is a required capability built directly into the extension headers
- End-to-end addressing without NAT is the normal mode of operation
- The huge address space makes sequential or random address scanning of a prefix for vulnerable hosts impractical and also makes new security constructions like cryptographically generated addresses possible

A bewildering array of protocols for tunneling IPv6 over IPv4, or vice versa, as transition or coexistence mechanisms, exists. For production networks needing such a capability, the safest approach is to use configured tunnels as described in RFC 4213 [NG05].

Delving too far into the details of IPv6 security is out of scope here, but several helpful documents exist. The following make a good starting point, and the references within them can be followed further:

- RFC 4942 on IPv6 Transition/Coexistence Security [EKS07]
- RFC 4864 on Local Network Protection for IPv6 [VdV07]
- RFC 4890 on Filtering ICMPv6 [DM07]
- RFC 4891 on IPv6 in IPv4 Tunneling with IPsec [GPST07]
- NIST SP 800-119 on Guidelines for the Secure Deployment of IPv6 [NIST10]

Users should also note that many security products have not caught up with IPv6 yet. Some that do advertise IPv6 features are immature or incomplete, and others offer IPv6 capabilities at significantly degraded performance.

8. IPsec APIs (Informative)

APIs are needed for fine-grained, application-level control of IPsec. Work on this topic has been partially completed and is divided between the API itself and the concept of channel binding. An expired API draft [Ric08] describes the communications between the IPsec layer and the application in terms of two data structures called P Tokens (for "protection") and I Tokens (for "identity").

Channel binding (see [Wil09]), also called connection latching, associates a packet flow seen by an upper layer protocol with an IPsec SA. The parameters bound by this mechanism include type of protection, quality of protection, IPsec mode, and peer's identity.

An open question is how application security policy and system security policy can be aligned so that they do not get in each other's way.

9. Summary

This document comprises a complete and updated set of optional-to-implement security methods for the OIF's UNI and E-NNI. It contains both information needed to provide a simple, complete, and interoperable set of security services and supplementary guidance on security for implementers and users.

10. References

10.1 Normative References

The following documents contain provisions of this Implementation Agreement by reference. At the time of publication, the versions listed were valid. Many references are subject to revision, and users of this Implementation Agreement are encouraged to investigate the possibility of applying the most recent versions of the references below.

[Bha09a] Bhatia, M., et al., "IS-IS Generic Cryptographic Authentication," IETF RFC 5310, February 2009.

[Bha09b] Bhatia, M., et al., "OSPF HMAC-SHA Cryptographic Authentication," IETF RFC 5709, October 2009.

[BM08] Black, D., and D. McGrew, "Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol," IETF RFC 5282, August 2008.

[BP11] Burgin, K., and M. Peck, "Suite B Profile for Internet Protocol Security (IPsec)," IETF RFC 6380, October 2011.

[Bra97a] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," IETF RFC 2119, March 1997.

[Col08] Colton, R., et al., "OSPF for IPv6," IETF RFC 5340, July 2008.

[DH98] Deering, S., and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," IETF RFC 2460, December 1998.

[DW09] Devarapalli, V., and K. Weniger, "Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)," IETF RFC 5685, November 2009.

[Far00] Farinacci, D., et al., "Generic Routing Encapsulation (GRE)," IETF RFC 2784, March 2000.

[GM06] Gupta, M., and N. Melam, "Authentication/Confidentiality for OSPFv3," IETF RFC 4552, June 2006.

[GMB10] Grewal, K., G. Montenegro, and R. Bhatia, "Wrapped Encapsulating Security Payload (ESP) for Traffic Visibility," IETF RFC 5840, April 2010.

[CSFBHP08] Cooper, D., S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," IETF RFC 5280, May 2008.

[FS10] Fu, D., and J. Solinas, "ECP Groups for IKE and IKEv2," IETF RFC 5903, June 2010.

[HH05] Hinden, R., and B. Haberman, "Unique Local IPv6 Unicast Addresses," IETF RFC 4193, October 2005.

[Hof05] Hoffman, P., "Cryptographic Suites for IPsec," IETF RFC 4308, December 2005.

[Hut05] Huttunen, A., et al., "UDP Encapsulation of IPsec ESP Packets," IETF RFC 3948, January 2005.

[IANA-IKE] http://www.iana.org/assignments/ikev2-parameters

[KBC97] Krawczyk, H., M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," IETF RFC 2104, February 1997.

[Ken05a] Kent, S., "IP Encapsulating Security Payload (ESP)," IETF RFC 4303, December 2005.

[Ken05b] Kent, S., "IP Authentication Header," IETF RFC 4302, December 2005.

[KHNE10] Kaufman, C., P. Hoffman, Y. Nir, and P. Eronen, "Internet Key Exchange Protocol (IKEv2)," IETF RFC 5996, September 2010.

[KK03] Kivenen, T., and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE)," IETF RFC 3526, May 2003.

[Kor07] Korver, B., "The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX," IETF RFC 4945, August 2007.

[KS05] Kent, S., and K. Seo, "Security Architecture for the Internet Protocol," IETF RFC 4301, December 2005.

[Lan05] J. Lang, Ed., "Link Management Protocol (LMP)," IETF RFC 4204, October 2005.

[LK08] Lepinski, M., and S. Kent, “Additional Diffie-Hellman Groups for Use with IETF Standards,” IETF RFC 5114, January 2008.

[LogAud] Optical Internetworking Forum Implementation Agreement, “OIF Control Plane Logging and Auditing with Syslog version 1.1,” OIF OIF-SLG-01.3, October 2012.

[LS11] Law, L., and J. Solinas, “Suite B Cryptographic Suites for IPsec,” IETF RFC 6379, October 2011.

[MG98] Madson, C., and R. Glenn, “The Use of HMAC-SHA-1-96 within ESP and AH,” IETF RFC 2404, November 1998.

[Man07] Manral, V., “Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH),” IETF RFC 4835, April 2007.

[MBW97] Murphy, S., M. Badger, and B. Wellington, “OSPF with Digital Signatures,” RFC 2154, June 1997. (Experimental)

[Moy98] Moy, J., “OSPF Version 2,” IETF RFC 2328, April 1998.

[MT07] Myers, M., and H. Tschofenig, “Online Certificate Status Protocol (OCSP) Extensions to IKEv2,” IETF RFC 4806, February 2007.

[MW10] McGrew, D., and B. Weis, “Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic,” IETF RFC 6054, November 2010.

[Pos81] Postel, J., “Internet Protocol,” IETF RFC 791, September 1981.

[SecMang] Optical Internetworking Forum Implementation Agreement, “Security for Management Interfaces to Network Elements,” OIF-SMI-03.1, October 2012.

[SH11] Santesson, S., and P. Hallam-Baker, “Online Certificate Status Protocol Algorithm Agility,” IETF RFC 6277, June 2011.

[SMM10] Shen, S., Y. Mao, and N.S.S. Murthy, “Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol,” IETF RFC 5930, July 2010.

[ST10] Sheffer, Y., and H. Tschofenig, “Internet Key Exchange Protocol version 2 (IKEv2) Session Resumption,” IETF RFC 5723, January 2010.

[Tsc08] Tschofenig, H., et al., “The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method,” IETF RFC 5106, February 2008. (Experimental)

[VM05] Viega, J., and D. McGrew, “The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP),” IETF RFC 4106, June 2005.

[WGI08] Weis, B., G. Gross, and D. Ignjatic, “Multicast Extensions to the Security Architecture for the Internet Protocol,” IETF RFC 5374, November 2008.

10.2 Informative References

[Abo04] Aboba, B., et al., "Securing Block Storage Protocols over IP," IETF RFC 3723, April 2004.

[AD03] Aboba, B., and W. Dixon, "IPsec-NAT Compatibility Requirements," IETF RFC 3715, March 2004. (Informational)

[Are05a] Arends, R., et al. "DNS Security Introduction and Requirements," IETF RFC 4033, March 2005.

[Are05a] Arends, R., et al. "Resource Records for the DNS Security Extensions," IETF RFC 4034, March 2005.

[Are05a] Arends, R., et al. "Protocol Modifications for the DNS Security Extensions," IETF RFC 4035, March 2005.

[BLS01] Boneh, D., B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," *Advances in Cryptology—Asiacrypt 2001*, LNCS Vol. 2248, Springer-Verlag, 2001.

[BMY06] Barbir, A., S. Murphy, and Y. Yang, "Generic Threats to Routing Protocols," IETF RFC 4593, October 2006.

[Bon03] Boneh, D., et al., "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," *Advances in Cryptology—Eurocrypt 2003*, Springer-Verlag, 2003.

[Bra97b] Braden, R., et al., "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification, IETF RFC 2205, September 1997.

[BTL07] Bonatti, C., S. Turner, and G. Lebovitz, "Requirements for an IPsec Certificate Management Profile," IETF RFC 4809, February 2007.

[CR10] Chandramouli, R., and S. Rose, *Secure Domain Name System (DNS) Deployment Guide*, NIST Special Publication SP800-81r1, April 2010.

[DKS07] Davies, E., S. Krishnan, and P. Savola, "IPv6 Transition/Coexistence Security Considerations," IETF RFC 4942, September 2007.

[DM07] Davies, E., and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls," IETF RFC 4890, May 2007.

[Dom00] Dommety, G., "Key and Sequence Number Extensions to GRE," IETF RFC 2890, September 2000.

[E-NNI1] Optical Internetworking Forum Implementation Agreement, "Intra-Carrier E-NNI Signaling Specification," OIF-E-NNI-Sig-01.0, February 27, 2004.

[E-NNI2] Optical Internetworking Forum Implementation Agreement, "OIF E-NNI Signaling Specification," OIF-E-NNI-Sig-02.0, April 16, 2009.

[E-NNI-OSPF1] Optical Internetworking Forum Implementation Agreement, "External Network-Network Interface (E-NNI) OSPF-based Routing - 1.0 (Intra-Carrier) Implementation Agreement," OIF-ENNI-OSPF-01.0, January 2007.

[E-NNI-OSPF2] OIF Implementation Agreement, "External Network-Network Interface (E-NNI) OSPFv2-based Routing – 2.0 (Intra-Carrier) Implementation Agreement," July 2011.

[ELM10] Eronen, P., J. Laganier, and C. Madson, "IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)," IETF RFC 5739, February 2010.

[Eas06] Eastlake, D., 3rd, "HMAC SHA (Hashed Message Authentication Code, Secure Hash Algorithm) TSIG Algorithm Identifiers," IETF RFC 4635, August 2006.

[ESC05] Eastlake, D., 3rd, J. Schiller, and S. Crocker, "Randomness Requirements for Security," IETF RFC 4086, June 2005.

[Fan10] Fang, L., ed., "Security Framework for MPLS and GMPLS Networks," IETF RFC 5920, July 2010.

[FK11] Frankel, S., and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap," IETF RFC 6071, February 2011.

[Gil07] Gill, J., et al. "Service Provider Infrastructure Security," IETF work in progress draft-ietf-opsec-infrastructure-security-01 (expired), April 2007. Available from http://tools.ietf.org/ html/draft-ietf-opsec-infrastructure-security-01.

[GM06] Gupta, M., and N. Melam, "Authentication/Confidentiality for OSPFv3," IETF RFC 4552, June 2006.

[GPST07] Graveman, R., M. Parthasarathy, P. Savola, and H. Tschofenig, "Using IPsec to Secure IPv6-in-IPv4 Tunnels," IETF RFC 4891, May 2007.

[Gut98] Gutmann, P., "Software Generation of Practically Strong Random Numbers," *Seventh USENIX Security Symposium Proceedings*, The USENIX Association, 1998, pp. 243–257.

[Gut04] Gutmann, P., *Cryptographic Security Architecture: Design and Verification*, Springer-Verlag, 2004.

[HBR04] Huang, G., S. Beaulieu, and D. Rochefort, "A Traffic-Based Method of Detecting Dead IKE Peers," IETF RFC 3706, February 2004.

[HowTo] "Generating X.509 Certificates," http://www.ipsec-howto.org/x595.html.

[Hou04] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)," IETF RFC 3686, January 2004.

[Hou05] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)," IETF RFC 4309, December 2005.

[HP-UX] "Using OpenSSL Certificates with HP-UX IPSec A.02.01," http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c02035746/c02035746.pdf.

[Kae07] Kaeo, M., "Current Operational Security Practices in Internet Service Provider Environments," IETF RFC 4778, January 2007.

[KM10] Kivinen, T., and D. McDonald, "Heuristics for Detecting ESP-NULL Packets," IETF RFC 5879, May 2010.

[Koç09] Koç, Ç., ed., *Cryptographic Engineering*, Springer, 2009.

[Kra03] Krawczyk, H., "SIGMA: The SIGn-and-MAc approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols," *Advances in Cryptology—Crypto 2003*, Springer-Verlag LNCS Vol. 2729, pp. 400–425. See also http://www.ee.technion.ac.il/~hugo/sigma.html.

[LA08] Li, T., and R. Atkinson, "IS-IS Cryptographic Authentication," IETF RFC 5304, October 2008.

[MBJW10] Manral, V., M. Bhatia, J. Jaeggli, and R. White, "Issues with Existing Cryptographic Protection Methods for Routing Protocols," IETF RFC 6039, October 2010.

[NG05] Nordmark, E., and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers," IETF RFC 4213, October 2005.

[NIST07] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," NIST Special Publication 800-38D, November, 2007.

[NIST09] FIPS PUB 140-3, DRAFT Security Requirements for Cryptographic Modules, NIST Federal Information Processing Standard, Revised Draft, December 2009, available from http:// csrc.nist.gov/publications/PubsDrafts.html#FIPS-140--3.

[NIST10] Frankel, S., R. Graveman, J. Pearce, and M. Rooks, "Guidelines for the Secure Deployment of IPv6," NIST Special Publication 800-119, December 2010, available from http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf.

[Per88] Perlman, R., Network Layer Protocols with Byzantine Robustness, Ph.D. Thesis, Department of Electrical Engineering and Computer Science, MIT, August 1988, available from http://publications.csail.mit.edu/lcs/pubs/pdf/MIT-LCS-TR-429.pdf.

[Per00] Perlman, R., *Interconnections, Second Edition*, Addison-Wesley, Reading, MA, 2000.

[PrivExt] OIF Implementation Agreement, "OIF Application of Vendor Private Extensions in RSVP," RSVP-PVT-EXT-01.0, October 2011.

[Ric08] Richardson, M., "An Abstract Interface between Applications and IPsec," IETF work in progress draft-ietf-btns-abstract-api-02, November 2008. (expired)

[Rou08] Le Roux, J.L., et al., "OSPF Protocol Extensions for Path Computation Element (PCE) Discovery," IETF RFC 5088, January 2008.

[SecAdd] Optical Internetworking Forum Implementation Agreement, "Addendum to the Security Extension for UNI and NNI," OIF-SEP-02.1, March 31, 2006.

[SecExt] Optical Internetworking Forum Implementation Agreement, "Security Extension for UNI and NNI," OIF-SEP-01.1, May 8, 2003.

[SH09] Scarfone, K., and P. Hoffman, Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41, Revision 1, September 2009.

[Shi07] Shirey, R., "Internet Security Glossary, Version 2," IETF RFC 4949, August 2007.

[SJB10] Srivatsan, S., M. Johnson, and S. Bellovin, "Simple-VPN: Simple IPsec Configuration," http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c0.

[SKTV06] Sakane, S., K. Kamada, M. Thomas, and J. Vilhuber, "Kerberized Internet Negotiation of Keys (KINK)," IETF RFC 4430, March 2006.

[Ste93] Steenstrup, M., "Inter-Domain Policy Routing Protocol Specification: Version 1," IETF RFC 1479, July 1993.

[TBW08] Touch, J., D. Black, and Y. Wang, "Problem and Applicability Statement for Better Than Nothing Security (BTNS)," IETF RFC 5387, November 2008.

[TG05] Tschofenig, H., and R. Graveman, "RSVP Security Properties," IETF RFC 4230, December 2005.

[UNI1.0] Optical Internetworking Forum Implementation Agreement, "User Network Interface (UNI) 1.0 Signaling Specification," OIF-UNI-01.1, October 1, 2001.

[UNI1.0r2] OIF Implementation Agreement, "OIF-UNI-01.0-R2-Common - User Network Interface (UNI) 1.0 Signaling Specification, Release 2: Common Part," OIF-UNI-01.0-R2-Common, February 27, 2004.

[UNI1.0r2r] OIF Implementation Agreement, "OIF-UNI-01.0-R2-RSVP - RSVP Extensions for User Network Interface (UNI) 1.0 Signaling, Release 2," OIF-UNI-01.0-R2-RSVP, February 27, 2004.

[UNI2.0] OIF Implementation Agreement, "User Network Interface (UNI) 2.0 Signaling Specification Common Part," OIF-UNI-02.0-Common, February 2008.

[UNI2.0-RSVP] OIF Implementation Agreement, "User Network Interface (UNI) 2.0 Signaling Specification OIF-UNI-02.0-RSVP - RSVP Extensions for User Network Interface (UNI) 2.0 Signaling," OIF-UNI-02.0-RSVP, February 2008.

[VdV07] Van de Velde, G., T. Hain, R. Droms, B. Carpenter, and E. Klein, "Local Network Protection for IPv6," IETF RFC 4864, May 2007.

[Vix00] Vixie, P., et al., "Secret Key Transaction Authentication for DNS (TSIG)," IETF RFC 2845, May 2000.

[VR09] Vasseur, J.P., and J.L. Le Roux, "Path Computation Element (PCE) Communication Protocol (PCEP)," IETF RFC 5440, March 2009.

[Wel00] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update," IETF RFC 3007, November 2000.

[Wil09] Williams, N., "IPsec Channels: Connection Latching," IETF RFC 5660, October 2009.

[WR08] Williams, N., and M. Richardson, "Better-Than-Nothing-Security: An Unauthenticated Mode of IPsec," IETF RFC 5386, November 2008.

Appendix A: Glossary

A thorough glossary of Internet and TCP/IP security terminology can be found in [Shi07].

Appendix B: List of Acronyms

AES	Advanced Encryption Standard
AH	Authentication Header
API	Application Programming Interface
BTNS	Better than Nothing Security
CBC	Cipher Block Chaining (Mode)
CCM	Counter with CBC-MAC (Mode)
CRL	Certificate Revocation List
DCN	Data Communications Network
DES	Data Encryption Standard
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name System
DNSSEC	Domain Name System Security
DoS	Denial of Service
E-NNI	Exterior Network Node Interface
ESP	Encapsulating Security Payload
GMPLS	Generalized Multiprotocol Label Switching
GRE	Generic Routing Encapsulation
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
IA	Implementation Agreement
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
IP	Internet Protocol version 4 or Internet Protocol version 6
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPsec	IP Security
IS-IS	Intermediate System—Intermediate System
ISAKMP	Internet Security Association and Key Management Protocol

KINK	Kerberized Internet Negotiation of Keys
LMP	Link Management Protocol
LSA	Link State Advertisement
MAC	Message Authentication Code
MD5	Message Digest 5
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NE	Network Element
NNI	Network Node Interface
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
OCSP	On-Line Certificate Status Protocol
OSPF	Open Shortest Path First
OSPFv2	Open Shortest Path First version 2
OSPFv3	Open Shortest Path First version 3
P	Provider
PAD	Peer Authorization Database
PCE	Path Computation Element
PCEP	Path Computation Element Protocol
PE	Provider Edge
PS	Proposed Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RC PC ID	Routing Controller Protocol Controller Identifier
RFC	Request for Comments
RSA	Rivest, Shamir, and Adleman
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol Traffic Engineering Extension
RFC	Request for Comments
SA	Security Association
SC PC ID	Signaling Controller Protocol Controller Identifier
SHA	Secure Hash Algorithm
SIP	Session Initialization Protocol
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SPD	Security Policy Database

SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport layer Security
TSIG	Transaction Signatures
UDP	User Datagram Protocol
ULA	Unique Local Address
UNI	User-Network Interface
UNI-C	UNI Client
USB	Universal Serial Bus
VPN	Virtual Private Network
WG	Working Group
XML	Extensible Markup Language

Appendix C: Security Requirements for UNI 2.0 and E-NNI

Security mechanisms are required to protect the signaling, routing, and discovery protocols used for optical connections, because these connections carry high volumes of data and consume significant network resources. Security mechanisms safeguard transport networks against attacks that compromise their control plane, seek unauthorized use of their resources, or attempt to gain unauthorized information about their configuration and usage.

Communication protocols usually require two main security mechanisms: *integrity* and *confidentiality*. Integrity mechanisms ensure *data origin authentication* and *message integrity* of UNI or E-NNI messages so that unauthorized operations can be detected and discarded. For example, the UNI message integrity service can prevent a malicious UNI-C agent from causing denial of service at a service provider by sending an excessive number of forged connection creation requests. Integrity mechanisms detect and reject attempts to forge messages and to reorder, duplicate, truncate, or otherwise tamper with the proper sequence of messages. These mechanisms can also provide *replay protection* and *non-repudiation.* Replay protection is used to detect any reinsertion of previously sent messages into the communications channel, which can be used to gain unauthorized access. Replay protection is normally achieved by adding sequence numbers to the messages or by relying on another protocol (e.g., TCP) to guarantee the proper sequencing of the message stream above the integrity service. Non-repudiation provides evidence that prohibits a sender from denying sending a message, thus holding the sender accountable. This may be desirable for accounting and billing purposes.

Message integrity and confidentiality are normally achieved using symmetric cryptographic algorithms. These algorithms require pairwise shared secret keys and do not provide non-repudiation. To facilitate the use integrity and confidentiality services, public-key or *asymmetric* cryptographic algorithms are typically used, initially, to provide *two-way peer entity authentication* and *key agreement.* Asymmetric algorithms also provide *digital signatures,* which can be used to implement a non-repudiation service. The use of asymmetric algorithms may be supported by a public-key infrastructure (PKI) or some other, community-defined, key assignment scheme. Asymmetric algorithms are typically more computationally intensive than symmetric algorithms. *It is expected that from the point of view of the UNI 2.0 and E-NNI requirements, the most important security feature could be message integrity.* Confidentiality of messages is also likely to be desirable, especially in cases where message attributes include information private to the communicating parties (either the customer or network operator). Examples of such attributes include details about the users, such as account numbers, contract identification numbers, etc.

The potential use of non-co-located equipment increases security requirements. In this scenario, it is assumed that the network elements are connected via devices such as layer 2 switches and IP routers. Because these devices can belong to different network operators and may be outside the control of the service provider, control communication between them is subject to increased security threats, such as IP address spoofing, eavesdropping, denial of service attacks, and unauthorized intrusion attempts. To counter these threats, appropriate security services need to be deployed to protect the control channels.

Just as any other functionality, security consumes resources, and it must be designed from a point of view that keeps the costs and benefits properly aligned. Therefore, security should be:

- *Optional to implement and to use.* Some users may decide that they can implement adequate protection by other means (e.g., perimeter access controls and firewalls), so that protocol security is unnecessary. Vendors who choose to serve these users may offer a product without these security services.
- *Interoperable.* The purpose of having a standard set of security services in UNI and E-NNI is to ensure that protocol security interoperates between vendors' products within and between carriers' networks. Thus, the security services defined should have as few methods, formats, optional features, and algorithms as possible. The same methods should work with different Layer 2 protocols and with IPv4 or IPv6.
- *Synergistic with other functionality.* Security for control protocols (including signaling, routing, and discovery) is less costly and less error prone to implement and deploy if the same solution is used for bearer traffic, management, or user services like VPNs.
- *High assurance.* Solutions should be preferred if they are already well standardized, extensively analyzed, and widely used.

- *Readily available in reference implementations.* This encourages the development of complete, interoperable implementations.
- *High quality.* The algorithms and protocols should be chosen based on the level of security required. They should have no known defects or serious weaknesses, and the security should be designed to operate within a broad model of both active and passive attacks.
- *Efficient.* Standard state-of-the-art microprocessors should be able to perform many instances of the authentication and key negotiation protocol and tens of megabits of traffic protection per second of processing time. Dedicated hardware modules should be able to increase these numbers by two orders of magnitude.

In summary, to satisfy the above requirements, security for UNI and E-NNI control protocols must support confidentiality, data origin authentication, data integrity, and replay detection on a per-message basis. Two-way authentication of the parties must be integrated with an automated key management system.

Appendix D: Evaluation of Alternative Approaches

This section describes four approaches to securing control plane protocols and explains why the fourth, network layer security, best satisfies the OIF's control plane security requirements. One way in which these approaches can be differentiated is by the protocol layer at which each operates. In practice, the choice depends on the requirements and the availability of different solutions.

Multiple Application Layer Solutions

When security is specified protocol by protocol, it usually works differently and often incompatibly in each case. The sets of available security services and algorithms are likely to be incomplete, non-uniform, and non-extensible. This approach makes it difficult to tie security usage to a security policy that enforces what security is required where. When there are more than a couple of protocols, it quickly becomes expensive and error prone. Finally, security for each new protocol has to be considered *a priori*. Therefore, it is recommended that this approach not be followed.

Single Application Layer Solution

Instead of specifying security solutions protocol by protocol, a single security solution could be specified at the application layer. One standard system for implementing a full set of security services at the application layer is Kerberos (together with several extensions and the GSS-API). Kerberos provides entity authentication, integrity, and confidentiality services together with key management, so a reasonably complete system of security services is available. As is also the case for protocol by protocol security, a major drawback to using application layer security is that it has to be implemented within the application code. For Kerberos, in particular, the trusted third party authentication, key management protocols, and traffic protection methods are somewhat restricted and inflexible.

Adopting application-layer security would be a better approach than defining protocol-by-protocol security solutions, but it would also be hard to get it implemented in legacy code. Therefore, another solution that is easier to implement and deploy is preferable.

Session Layer Security

Security solutions above the Transport Layer can be implemented easily, yet are limited in their coverage for securing application layers. Two high-quality systems that can be implemented at the Session Layer exist, both of which provide (1) a full set of security services between the TCP layer and the application and (2) public-key-based authentication and key management. One is the Secure Shell (SSH) and the other is the Secure Sockets Layer or Transport Layer Security (SSL-TLS) system commonly used to secure Web sessions.

One major advantage to these systems is that they can be inserted between the application and the operating system with minimal difficulty. On the other hand, one drawback to these systems is that SSH and SSL-TLS only secure TCP, not UDP, ICMP, or other protocols such as RSVP or OSPF. Also, the common ways in which SSL-TLS and SSH are used (client server, with strong authentication requirements on one of the parties) differs from the peer-to-peer model of the optical control plane.

Network Layer Security

A major advantage of defining security at the network (IPv4 or IPv6) layer is coverage. Security at the network layer can also hide details like higher layer protocol headers and packet sizes. Another advantage of network layer security is that it can be deployed at outboard security processors or intermediate systems like routers or firewalls. All of the protocols mentioned in UNI and E-NNI run over an IPv4 or IPv6 network layer. In addition, many important supporting protocols do as well (DNS, NTP, SNMP, etc.). IP Security (IPsec) has all the necessary security functionality as well as coverage for these. IPsec has also been designed to address, to the extent possible, additional security issues like denial of service protection, forward secrecy, and anonymity.

These properties make IPsec the potentially best choice of security solution for UNI and E-NNI, but two additional points need to be considered:

1. IPsec has been regarded as overly complicated. This issue needs to be addressed on multiple fronts. First, the key management protocol in IPsec, IKE, has been the source of much of the complexity. It has been redesigned with this specific problem in mind, and this Implementation Agreement uses the new version. Second, the original IPsec documentation needed to be improved, and the IETF has addressed this as well. Specific profiles and recommendations are specified in this Security Extension for the OIF's UNI and E-NNI to simplify the number of choices involved in using IPsec.
2. To specify and enforce a security policy, it is necessary to have a way for the system operator or higher layer protocols to communicate with the IPsec processing layer. One popular method of communicating between IKE and the IPsec layer is PF_KEY described in [RFC2367], but this does not provide a complete solution for general

applications. Therefore, new work in this direction is described here as potentially useful when it is completed.

Appendix E: Using the Security Extension with RFC 2401 and IKEv1

The previous version of this document [SecExt] and its Addendum [SecAdd] describe how to protect the OIF control plane with IPsec as defined in RFC 2401 and IKEv1. The IETF has deprecated these methods and replaced them with IPsec as defined in RFC 4301 and IKEv2. Nevertheless, the older versions of IPsec and IKE are still in use. Therefore, this section points out updates to these methods that have appeared since the publication of [SecAdd].

- For dead peer detection, implementations can use the messages defined in [HBR04].
- Kerberized Internet Negotiation of Keys (KINK) is described in RFC 4430 as an alternative to IKEv1.
- A correction to the AES-XCBC-PRF-128 Algorithm for IKE is documented in RFC4434.
- RFCs 4493 and 4494 document the AES-CMAC alternative to AES-XCBC, which appeared in NIST SP 800-38b. Using AES CMAC as the IKE pseudo-random function (AES-CMAC-PRF-128) is covered in RFC 4615. The GMAC alternative is documented in RFC 4543.
- Using IPsec to protect OSPFv3 is covered in RFC 4552. The Informational Generic Threats to Routing Protocols RFC is number 4593.
- SHA-1 and HMAC-SHA-1 are documented in RFC 4634 (FIPS 180-2). The SHA-2 algorithms are covered in RFC 4868.
- RFC 4754 covers IKE Authentication using ECDSA. RFC 4753 contains an initial set of elliptic curve groups. An entire set of elliptic curve methods is described in RFC 6379 [LS11]. Note that groups 19, 20, and 21 should be implemented as specified in RFC 5903 [FS10], not as specified in RFC 5114 [LK08].
- An entire updated set of ESP and AH algorithms is presented in RFC 4835. In particular, it references the AES-GCM mode described in RFC 4106.
- Two Informational documents on the strength of cryptographic methods are RFC 4772 on why not to use single DES and RFC 4894 on the status of hash functions that have been attacked since the publication of [SecAdd].
- The information on generating certificates in [HowTo], [HP-UX], and [SJB10] applies to IKEv1 as well as IKEv2.

RFC 5840 describes a method for identifying ESP traffic that is authenticated but not encrypted.

Appendix F: Open Issues / Current Work Items

NIST is going to issue a new version of FIPS 140.

An automated group key management protocol for multicast IPsec is needed.

The crypto community is working on new hash functions, and NIST has begun a competition to design and select a "SHA-3."

The IETF never satisfactorily completed work on IKE and IPsec APIs.

Appendix G: OIF Members When the Document Was Approved

Acacia Communications
ADVA Optical Networking
Agilent Technologies
Alcatel-Lucent
Altera
AMCC
Amphenol Corp.
Anritsu
Applied Communication Sciences
AT&T
Avago Technologies Inc.
Broadcom
Brocade
Centellax, Inc.
China Telecom
Ciena Corporation
Cisco Systems
ClariPhy Communications
Cogo Optronics
Comcast
Cortina Systems
CyOptics
Dell, Inc.
Department of Defense
Deutsche Telekom
Emcore
Ericsson
ETRI
EXFO
FCI USA LLC
Fiberhome Technologies Group
Finisar Corporation
France Telecom Group/Orange
Fujitsu
Fundacao.CPqD
Furukawa Electric Japan
GigOptix Inc.
Hewlett Packard
Hitachi
Hittite Microwave Corp
Huawei Technologies
IBM Corporation
Infinera
Inphi
IPtronics
JDSU
Juniper Networks
Kandou
KDDI R&D Laboratories
Kotura, Inc.
LeCroy
LSI Corporation
Luxtera
M/A-COM Technology Solutions, Inc.
Marben Products
Metaswitch
Mindspeed
Mitsubishi Electric Corporation
Molex
MoSys, Inc.
NEC
NeoPhotonics
Nokia Siemens Networks
NTT Corporation
Oclaro
Optoplex
PETRA
Picometrix

PMC Sierra
Reflex Photonics
SHF Communication Technologies
Sumitomo Osaka Cement
Tektronix
TeraXion
TriQuint Semiconductor
Verizon
Xilinx
Yamaichi Electronics Ltd.

QLogic Corporation
Semtech
Sumitomo Electric Industries
TE Connectivity
Tellabs
Time Warner Cable
u2t Photonics AG
Vitesse Semiconductor
Xtera Communications