Use of IPsec by Manned Space Missions

Michael J. Pajevski
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive, Pasadena, CA 91109
818-393-6232
michael.j.pajevski@jpl.nasa.gov

Abstract—NASA's Constellation Program is developing its next generation manned space systems for missions to the International Space Station (ISS) and the Moon. The Program is embarking on a path towards standards based Internet Protocol (IP) networking for space systems communication. The IP based communications will be paired with industry standard security mechanisms such as Internet Protocol Security (IPsec) to ensure the integrity of information exchanges and prevent unauthorized release of sensitive information in-transit. IPsec has been tested in simulations on the ground and on at least one Earth orbiting satellite, but the technology is still unproven in manned space mission situations and significant obstacles remain.

Some of the challenges to using IPsec for manned space communications are bandwidth limitations lack of certified implementations for manned space systems, and various key and policy management issues. The benefits of IPsec are many: a standard that is sharable among International partners, does not impede networking, and can secure a wide variety of information exchanges without integrating security into each application. The potential benefits warrant the investment needed to overcome the challenges facing the use of IPsec for manned space missions.

Maturation of key and policy management standards and the development of certified (e.g., per NIST FIPS 140-2) manned space rated implementations are needed to make IPsec a better fit for space. Technical issues with IPsec and its associated management mechanisms that affect terrestrial use of the protocol must also be resolved in order to increase the feasibility of using IPsec for manned space system communications. This paper describes some of the issues affecting the use of IPsec for manned space systems and suggests approaches to overcome those issues.

TABLE OF CONTENTS

1. INTRODUCTION 1
2. THE CASE FOR IPSEC IN SPACE 2
3. PROBLEMS WITH USING IPSEC IN SPACE 3
4. STANDARDS DEVELOPMENT RECOMMENDATIONS 4
5. TECHNOLOGY MATURATION RECOMMENDATIONS 6
6. CONCLUSIONS 7
REFERENCES 7
BIOGRAPHY 7

1———————————

[1] 978-1-4244-2622-5/09/$25.00 ©2009 IEEE.
[2] IEEEAC paper #1564, Version 6, Updated 2008:11:04

1. INTRODUCTION

NASA and the DoD are developing space systems that will use Internet Protocol (IP) networking to connect information systems across the globe and in space. Leveraging IP and other common Internet standards takes advantage of commercial technology to provide much greater information exchange capability and flexibility, but with significant security related challenges. NASA's Constellation Program is pushing the envelope on the use of IP in space and started addressing the security challenges early on. This paper describes one aspect of the Constellation Program's approach to securing information exchanges between its various ground-based and space flight systems – i.e., the adoption of Internet Protocol Security (IPsec).

IPsec is a network layer security protocol that protects IP packets with cryptographic integrity and confidentiality processing and replay detection. This paper assumes the reader is knowledgeable of the IPsec protocol. For more information on IPsec, refer to RFC 4301[1], RFC 4302[2], and RFC 4303 [3].

The selection of IPsec by the Constellation Program was, in part, based on the Program's goal to leverage commercial standards and technologies to reduce cost, ease system integration, and facilitate partnering with educational, scientific, commercial, and international organizations. IPsec was also chosen because it fits the net-centric nature of the command, control, communications, and information (C3I) architecture of the Program. These and other reasons for choosing IPsec are described in Section 2 of this paper.

The two biggest technical challenges involved with using IPsec for space communications are the lack of IPsec device management standards suitable for space systems and the low maturity of IPsec technology in the space environment. Special aspects of space communications – such as bandwidth constraints, communication gaps, higher bit error rates and higher transmission latencies (than in terrestrial networks) – impose design constraints that affect standards development/adoption and technology maturation efforts. Special operating cases for space systems – such as ensuring critical event coverage and the ability to use one-way links (in whatever direction available) when the reverse direction has failed – must be considered as part of any standards

development/adoption and technology maturation efforts associated with space communications. Technical challenges associated with using IPsec for space communications are described in Section 3 of this paper.

Section 4 of this paper presents recommendations for the development of standards more suitable for space communications. Such standards are needed to better define system interfaces and to promote product development that supports space mission needs.

Section 5 of this paper presents recommendations for maturing IPsec technology in order to ensure its suitability for space missions.

2. THE CASE FOR IPSEC IN SPACE

IPsec provides secure communications for various businesses, institutions, militaries, and government agencies around the world. When IP is used to move data, IPsec is a prime candidate for protecting the data while it is in-transit. This section describes why IPsec is a good fit for protecting space mission IP traffic.

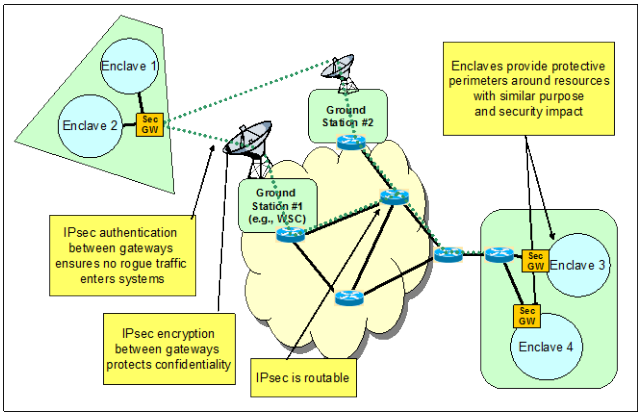
The selection of IPsec by the Constellation Program was, in part, based on the Program's goal to leverage industry standards and commercial technologies. Defining system interfaces in terms of widely adopted industry standards eases system integration – particularly when the standards are well defined and leave little up to vendor specific details.

Using open standards, such as the IETF RFCs that define IPsec, facilitates partnering with educational, scientific, commercial, and international organizations that might not have access to classified or proprietary communications security technologies. Communications security technologies such as the DoD's High Assurance IP Encryptor (HAIPE) were also considered, but IPsec prevailed because it provides a strong enough solution that is available to a wide variety of potential partners. HAIPE is a "Type 1" solution that is suitable for classified information and is available to a very limited set of partners.

Using commercial technologies based on open standards helps to reduce development cost because procuring commercially available products is typically much less expensive than producing new technologies. IPsec provides a standardized approach that is widely available in commercial offerings and provides ample protection for the transmission of unclassified information.

IPsec is a network layer solution that does not impair layer 3 routing (or layer 2 switching), and thus IPsec can provide end-to-end security across a communications path even when the path involves multiple hops. Because IPsec can provide end-to-end security without impacting routing, an IPsec solution supports common, terrestrial style networking and does not impose the need for a tunneling protocol such as Space Link Extensions (SLE) in order to carry spacecraft data over an IP network between control centers and ground stations. That said, IPsec is not presented here as a perfect solution and it does affect intelligent routing that relies on information in higher layer (e.g., transport, application) content within packets.

The following figure depicts IPsec tunnels extending from security gateways (Sec GW) in control center enclaves (lower right corner) through a ground network cloud and ground stations (i.e., antenna) to a security gateway on a spacecraft (upper left). The IPsec security gateways protect traffic between them and protect their enclaves from rogue traffic (if only authenticated traffic is allowed through).



IPsec adds bit overhead and is only for communication paths that provide enough bandwidth to tolerate the bit overhead. Bit overhead is incurred when the protected packet (including the original header – when in IPsec "tunnel mode") is wrapped, a new clear outer IP header for routing between the IPsec endpoints is added, padding is added as necessary for cryptographic processing and IPsec packet formatting, and to add IPsec processing related information (e.g., sequence number). The "integrity check value (ICV)" appended by IPsec (or any other protocol) for cryptographic integrity checking adds 96 to 256 bits (or more, depending on the integrity algorithm).

IPsec is a good fit for communications that involve long transmission latencies. One reason that the Constellation Program selected IPsec was that it could be used for low Earth orbit (LEO) missions, lunar missions, and even missions to Mars. IPsec supports long transmission latencies for several reasons. IPsec does not depend on (tight) inter-system clock synchronization or small time intervals between sending and receiving packets (but specific implementations might impose such constraints).

While it is true that IPsec relies on the coordination of keys and other parameters, this is true for any solution that enables long term operation – and the protocol for coordinating keys and other parameters between IPsec endpoints is separate from the IPsec protocols (i.e.,

Authentication Header {AH} and Encapsulating Security Payload {ESP}) that protect network traffic. IPsec can operate for a relatively long time between key updates – depending on data rates, cryptographic algorithms, the IPsec services used (e.g., if anti-replay is used), and the security needs of the system (e.g., the criticality of the data). That said, one of the fundamental challenges associated with using IPsec for manned space missions is finding a suitable IPsec management solution. The following section describes some problems related to using IPsec for space missions, starting with IPsec management issues.

3. PROBLEMS WITH USING IPSEC IN SPACE

Overview

IPsec is perhaps the best match for protecting IP based space communications, but it is not a perfect fit. This paper describes the following kinds of problems related to the use of IPsec for space communications:

(1) IPsec Management Issues

(2) Technology Maturity

(3) Delays, Gaps, Errors, and Bandwidth Constraints

(4) Implementation-Specific Details

The problems noted above are described in the subsections below. Recommendations are presented in Sections 4 and 5.

IPsec Management Issues

Manned space systems are tightly managed (i.e., little is left to chance), and the thought of an IPsec security association (SA) expiring and an Internet Key Exchange (IKE) negotiation starting automatically is a concern. However, this is exactly how IPsec operates on terrestrial networks – and this is how commercial products work. Either NASA's manned space mission culture will need to adapt to the way IPsec is used terrestrially or new approaches for managing IPsec SAs (and other IPsec device configuration data) must be developed if IPsec is going to fit into the manned space system paradigm of tightly scripted control.

The current state of standards for IPsec device management makes it difficult to effectively specify security-related interoperability requirements for space systems – particularly manned space systems. Existing standards are not a good fit for space communications and do not provide a complete solution. Progress has stalled on two Internet drafts for an IPsec device management approach that uses Simple Network Management Protocol (SNMP) Management Information Base (MIB) modules. Standards development for some approaches that could be very useful for space systems has yet to be pursued.

Existing IPsec device management standards fall short in terms of their suitability for space communications because the existing standards assume that IPsec peers must negotiate all of the SA parameters needed to establish IPsec protection that meets the security policies of the sender and the receiver. The exchange of parameters during SA negotiation consumes bandwidth (albeit rather infrequently), even though many of the parameters could be pre-arranged and/or re-used. A peer-to-peer negotiation based approach does not allow a control center to set up SAs for IPsec protection between two other systems (e.g., between a crew/cargo transportation vehicle and a space station).

The most commonly used existing standard for IPsec SA/key management is the Internet Key Exchange (IKE) (see RFC 4306[4]). For unicast traffic, IKE is a peer-to-peer negotiation protocol that involves exchanges of all the parameters needed to create new SAs in each peer device. For multicast traffic, the Group Domain of Interpretation (GDOI) for IPsec provides a client-server based approach that supports centralized management of SAs. Using multicast addressing for all space communications would facilitate SA management using existing standards and technologies that are a reasonable fit for space communications – but it is not desirable to limit IP-based space communications to only multicast addressing.

Another existing standard that falls short for space communications is the NETCONF protocol. NETCONF is an XML based approach that could be very useful, but the existing standards only define the general mechanism and its use over a few specific transport protocols. Schemas for IPsec device management are not defined. Also, the reliance on transport layer mechanisms to provide authentication, integrity, and confidentiality may be an issue for providing fine-grained access control (but this point is completely dependent on application design).

An SNMP based approach for managing IPsec configuration data looks promising, but only one of the three Internet drafts has been promoted to RFC status (as a Proposed Standard). The other two parts of the solution are still Internet drafts. See Section 4 of this paper for references to the RFC and Internet drafts, and for more description of this approach.

Technology Maturity

The high availability/reliability required for space systems (especially manned space systems) constrain system developers to the use of proven technologies. It is not enough for a technology to be proven in terrestrial uses. The technology must be proven in the environment in which the technology will be used. For security related technologies used in space communications, the "environment" includes aspects that all space communications technologies must address (e.g., transmission delays, bit errors, heating/cooling considerations, and radiation exposure) and the security-

related aspects of the environment (e.g., the kinds of attacks that the system is likely to be exposed to).

Although the DoD and NASA are planning space systems that utilize IP and IPsec, there is a lack of existing systems using these technologies. NASA's Glenn Research Center (GRC) operates an Earth orbiting satellite that uses IP and IPsec, but the satellite is a test bed that does not implement all of the IPsec related technologies that need to be proven suitable for space systems.

Recommendations for maturing IPsec technologies are presented in Section 5 of this paper.

Delays, Gaps, Errors, and Bandwidth Constraints

The IPsec standards and implementations used for space communications must be suitable for communications environments in which significant propagation delays, gaps in communication coverage, and bit errors occur. These characteristics of space communications are not a big issue for IPsec and are typically dealt with by framing, networking, transport, and/or application layer functions. These characteristics might impact IKE exchanges, but only by causing IKE to restart negotiations if delays or losses cause an exchange to fail.

If a complete communications gap or the loss of a link in one direction occurs when an SA expires, IKE will not be able to negotiate new SAs. In the case of a complete loss of communications, no data is flowing anyway. If only one direction of communications is lost, then IPsec implementations used for space systems should be able to continue sending or receiving traffic without the need for two-way communications to update IPsec SAs.

The bit overhead of IPsec is often cited by manned space system engineers, developers, and operators as why IPsec is not a good fit for space communications. IPsec is only viable for systems with enough bandwidth to handle the overhead. For most cases, the systems operated under the Constellation Programs have the necessary bandwidth.

Recommendations associated with handling delays, gaps, errors, and bandwidth constraints are not provided on their own in this paper – but they are covered as part of the recommendations for standards development in Section 4.

Implementation-Specific Details

The IPsec Architecture (RFC 4301) leaves some details up to the implementer. Some of these details can have security implications. An example is shown below. This draft of this paper points out that implementation specific details of IPsec can be problematic, but specific recommendations for such issues are not presented.

Excerpt from [RFC 4301], beginning of the last paragraph in Section 4.4.2:

```
Implementation Guidance: This document
does not specify how an SPD-S entry
refers to the corresponding SAD entry,
as this is an implementation-specific
detail.  However, some implementations
(based on experience from RFC 2401) are
known to have problems in this regard.
```

4. STANDARDS DEVELOPMENT RECOMMENDATIONS

Overview

One of the biggest challenges associated with using IPsec for space communications is finding a suitable approach for managing of IPsec security policies and SAs. The solutions offered by COTS vendors are often not well suited for space communications due to the reliance on IKE and/or the solutions are vendor specific.

IPsec related standards development is needed to provide security policy and security association management that is suitable for space systems, minimizes complexity (by providing interface commonality), fosters technology development among multiple vendors, and allows different system owners to select different products (as long as the products adhere to an adopted set of standards). Some small changes may be needed in the core IPsec standard (i.e., RFC 4301) to ensure that features important to the space environment are part of the standard rather than optional, vendor-specific features. Recommendations for such standards development are presented below.

The highest priority for standards development to support the use of IPsec in space should be the standardization of a suitable "automated SA/key management" protocol for IPsec (along with some optional/minor updates to the core IPsec architecture). The second highest priority should be the standardization of a security policy management protocol. Today's IKE based approaches (for unicast and for multicast traffic) only address the first priority. A set of emerging IETF standards based on SNMP covers both priorities. The NETCONF protocol provides another approach that could cover both priorities. Other concepts are also worth pursuing – such as the use of preset SA parameters and key derivation techniques to allow coordinated updating of SAs among IPsec peers with greatly reduced (in size and in frequency of occurrence) SA/key management data exchanges. These approaches are significantly different from each other, and selecting an approach depends on each system's network/security device administration approach and other system specific factors. All require some level of standards development and adoption in order to become viable approaches.

Internet Key Exchange (IKE) Standards

The most commonly used automated SA/key management protocol used by IPsec devices today is the Internet Key Exchange (IKE). There are different IKE standards for unicast traffic than for multicast traffic – and the two approaches are fundamentally different. For unicast traffic, IKE (see RFC 4306) provides a negotiation protocol between two IPsec peers. For multicast traffic, the "group domain of interpretation (GDOI)" for IKE provides a centralized management protocol based on a client-server model. Space systems would benefit from the ability to use peer-to-peer negotiation under some circumstances and centralized management for most situations – including cases involving unicast traffic. The development of a standard for centralized management of IPsec keys/SAs would be beneficial to space system development because space systems are often tightly managed and little is left to chance for on-the-fly negotiation (especially for establishing secure communications).

An alternate solution would be to use multicast IP for space communications and use the group domain of interpretation (GDOI) for IPsec to manage SAs. The ability to define multicast address groups and route traffic accordingly would support the use of multiple control centers and other multi-system coordination. Also, the IPsec SA/key management approach provided by the IKE GDOI fits the "tightly managed" paradigm followed for space systems.

The recommendation made here is to develop a centralized management approach for unicast traffic IPsec SAs. Such an approach should be relatively similar to the GDOI approach, but defined as a separate standard that suits unicast traffic. The details of such an approach are beyond the scope of this paper. Interested parties must make investments to fund the development of an appropriate specification if an IKE based approach to centralized management of unicast SAs is to ever become available.

SNMP Based IPsec Management Standards

An emerging approach that uses SNMP to manage IPsec security policies and security associations is documented in an IETF standard (RFC 4807) and two IETF Internet drafts (see bullets at end of next paragraph). Advancing the two IETF drafts to the Proposed Standard state would foster interoperable product development and provide a means for system owners to effectively/efficiently specify interoperability requirements.

RFC 4807, *IPsec Security Policy Database Configuration MIB*, [5] defines an SNMP MIB module for configuring the security policy database (SPD) of a device implementing the IPsec protocol. This standard, along with the following two Internet drafts, define a standard approach to IPsec security policy and security management that fits into a very common system administration approach (i.e., the use of SNMP):

(1) "IPsec Security Policy IPsec Action MIB", Wesley Hardaker, 10-Nov-06, <draft-ietf-ipsp-ipsecaction-mib-02.txt> [6]

(2) "IPsec Security Policy IKE Action MIB", Wesley Hardaker, 10-Nov-06, <draft-ietf-ipsp-ikeaction-mib-02.txt>[7]

The IPsec Security Policy IPsec Action MIB draft document defines a MIB module for configuration of an IPsec action within the IPsec security policy database (SPD). This module works within the framework of the IPsec Security Policy Database Configuration MIB (IPSEC-SPD-MIB) [RFC4807]. It can be referenced as an action by the IPSEC-SPD-MIB and is used to configure IPsec SA's that are created for network traffic between devices. Finalization and adoption of this draft would provide space systems with the ability to manage IPsec device configuration parameters (including the crypto keys) using an SNMP based approach that is commercially available and useful for managing a variety of network and security devices.

The IPsec Security Policy IKE Action MIB draft document defines a MIB module for configuration of an Internet Key Exchange (IKE) [RFC2409] action within the IPsec security policy database (SPD). This module works within the framework of the IPsec Security Policy Database Configuration MIB (IPSEC-SPD-MIB) [RFC4807]. It can be referenced as an action by the IPSEC-SPD-MIB and is used to configure IKE negotiations between network devices. Finalization and adoption of this draft would provide space systems with the ability to manage IPsec device configuration parameters (including the crypto keys) using an SNMP based approach that is commercially available and useful for managing a variety of network and security devices together with IKE for on-the-fly negotiation of SA parameters/keys.

The recommendation put forth in this paper is to purse the finalization and industry adoption of the two drafts (and adoption of RFC 4807). Additional investment is needed from interested parties in order to fund the completion and acceptance of the two Internet drafts. System owners will need to show interest in this approach to industry vendors in order to foster industry investment in product development.

XML Based IPsec Management Standards

Internet standards (i.e., IETF RFCs) exist for an XML based approach for managing network devices. The first RFC below defines the NETCONF Configuration Protocol, which provides device management operations on top of a Remote Procedure Call (RPC) layer. The NETCONF protocol rides above a transport protocol that must meet requirements specified in the NETCONF RFC. The second, third, and

forth RFCs listed below define how to use NETCONF over specific transport protocols. Currently defined RFCs for NETCONF are:

(1) RFC 4741; NETCONF Configuration Protocol; R. Enns, Ed.; December 2006; Proposed Standard. [8]

(2) RFC 4742; Using the NETCONF Configuration Protocol over Secure SHell (SSH); M. Wasserman, T. Goddard; December 2006; Proposed Standard. [9]

(3) RFC 4743; Using NETCONF over the Simple Object Access Protocol (SOAP); T. Goddard, Dec. 2006; Proposed Standard. [10]

(4) 4744; Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP); E. Lear, K. Crozier; December 2006; Proposed Standard. [11]

The RFCs above provide a framework for exchanging XML based network device configuration data between managed devices and management services. In order for a NETCONF based an approach to be useful for IPsec device management, schemas must be defined for managing IPsec devices (and, of course, compliant IPsec devices and IPsec management products are needed).

Defining standard schema for XML common schema should be defined in such a way that they can be used with NETCONF or with other XML based approaches for exchanging device configuration data.

Synchronized SA Derivation Standards

An approach considered for other security protocols (e.g., Secure Real Time Protocol – SRTP) is to derive traffic protection keys from shared master keys. This kind of approach could be very useful for space communications because it would enable synchronized updates of IPsec SAs with little or no communication overhead. Typical approaches such as time-based synchronization could allow spacecraft, control centers, and other systems to update SAs in unison for long periods of time without incurring additional communications overhead (or dealing with long delays) when transitioning SAs (i.e., to change keys and reset anti-replay sequence numbers).

No standards or drafts exist yet for using the approach described in the paragraph above for IPsec SA management. A new standard would need to be developed in order to define this approach. Owners of major space mission systems should consider investing in the development of such a standard because it will greatly serve space systems and it is not likely to develop otherwise (because it is not a major need for most terrestrial information systems).

5. TECHNOLOGY MATURATION RECOMMENDATIONS

Space systems are usually required to use technologies that are highly mature and reliable. This is particularly true for NASA's manned space missions, such as the Constellation Program's future missions to the International Space Station (ISS) and the Moon. The "technology readiness level (TRL)" requirements for the Constellation Program are a big part of ongoing discussion over the use of IPsec for space communications.

NASA and the DoD have already begun examining the readiness of IPsec technology for use in space. IPsec has already been shown to work properly in space communications with NASA GRC's "Cisco in Low Earth Orbit (CLEO)" satellite. CLEO provides a good test case for proving out IPsec technology, and space-rated IPsec technology maturation efforts should recognize and build upon NASA' successes with the CLEO satellite. Work has also been done under the DoD's Transformational Communications Satellite (TSAT) Program to test IPsec. The TSAT testing has occurred in labs on the ground, but sophisticated links simulation and other techniques have been used to conduct realistic test cases that mimic the communications characteristics that TSAT will experience. The TSAT testing of IPsec should also be recognized and built upon as part of proving out IPsec for space systems.

There is still much more work to do in order to raise the TRL of IPsec to the point where it is accepted for use in space systems – especially manned space missions.

It may be necessary to start proving out the maturity of core IPsec functionality first, and prove out additional functionality later as new technology becomes available. Some technologies, such as a centralized management mechanism for IPsec device management, may take some time to develop – but IPsec and IKE technologies are available today and the core aspects of using IPsec to protect space communications can be shown today.

Long before technology maturation efforts occur, the requirements that apply to the technology in question should be identified. Any standards development work that is needed to flesh out the requirements should also be done before embarking on the development and testing of new technology. Compiling the appropriate requirements set serves to develop the most appropriate implementations and provides the basis for developing verification requirements and specific test cases.

Once the requirements are ironed out, the first step in maturing IPsec technology for use in space systems should be the development of one or more implementations that provide the required IPsec functionality (including IPsec device management).

Once a viable implementation is available, rigorous testing of the technology should be performed. The testing may start on the ground, and can start relatively simply and progress to more complete tests that induce transmission delays, bit errors, communications gaps, and other characteristics of space communications. The devices must be subjected to stress testing (i.e., where the device is operated at or beyond its limits for extended durations) and environmental testing (e.g., for radiation, vacuum, cold, and heat). The implementations must also be subjected to a gamut of vulnerability testing in order to ensure the technology operates as expected even when exposed to cyber attack.

After proving out IPsec technologies on the ground, testing should be moved to space platforms. The ISS could provide a valuable platform for testing IPsec technologies in space. The ISS possesses a (non-critical) IP LAN with connectivity to the Mission Control Center (MCC) facility at NASA's Johnson Space Center (JSC) in Houston, Texas. IPsec technology testing aboard the ISS could prove the readiness of IPsec technology to Constellation Program management, systems engineers, and developers.

It is likely that technical issues will arise during IPsec technology testing under space mission conditions. The technology maturation process (and the surrounding requirements, standards development processes, product development/acquisition, and verification processes) must support the identification, tracking, corrective action, and verification needed to ensure a proper implementation of IPsec technologies to be used for space systems. If IPsec is to be accepted by system owners, developers, and operators – it is vital that Program/Project management recognize the need to prove the space worthiness of IPsec technologies and to pursue such efforts aggressively. Else, arguments against the use of IPsec due to its immaturity in the space environment may prevail and a potential fall-back to more traditional (for space systems) link layer security will hinder efforts towards more net-centricity in space systems.

6. CONCLUSIONS

IPsec is a good match for protecting the IP traffic exchanged for space missions, even manned space missions. However, some advancements in standards and implementations would be very beneficial to space systems.

One useful advancement to pursue is the standardization and development of an IPSec SA and policy management protocol that provides centralized management of distributed IPsec devices. Such work has begun on a couple of fronts (SNMP and XML based approaches), but that standards development work is not finished.

The IPsec technology needs to get recognized as mature before it can be used for space missions. Making sure that the proper implementations are available, and testing the implementations on the ground and then in space is needed to provide confidence in IPsec's suitability for space systems.

Acknowledgment: This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

REFERENCES

[1] RFC 4301, Internet Protocol Security (IPsec) Architecture, http://www.ietf.org/rfc/rfc4301.txt

[2] RFC 4302, Authentication Header (AH), http://www.ietf.org/rfc/rfc4302.txt

[3] RFC 4303, Encapsulating Security Payload (ESP), http://www.ietf.org/rfc/rfc4303.txt

[4] RFC 4306, Internet Key Exchange version 2 (IKEv2), http://www.ietf.org/rfc/rfc4306.txt

[5] RFC 4807, IPsec Security Policy Database Configuration MIB

[6] IPsec Security Policy IPsec Action MIB", Wesley Hardaker, 10-Nov-06, <draft-ietf-ipsp-ipsecaction-mib-02.txt>

[7] "IPsec Security Policy IKE Action MIB", Wesley Hardaker, 10-Nov-06, <draft-ietf-ipsp-ikeaction-mib-02.txt>http://en.wikipedia.org/wiki/Buisiness_Process_Execution_Language

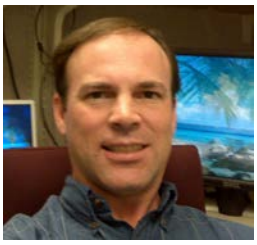
[8] (1) RFC 4741; NETCONF Configuration Protocol; R. Enns, Ed.; December 2006; Proposed Standard.

[9] RFC 4742; Using the NETCONF Configuration Protocol over Secure SHell (SSH); M. Wasserman, T. Goddard; December 2006; Proposed Standard.

[10] RFC 4743; Using NETCONF over the Simple Object Access Protocol (SOAP); T. Goddard, December 2006; Proposed Standard.

[11] RFC 4744; Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP); E. Lear, K. Crozier; December 2006; Proposed Standard.

BIOGRAPHY



Mike Pajevski has worked as a software engineer at the Jet Propulsion Laboratory for the past

7 years. He currently leads a systems security engineering team for NASA's Constellation Program. Mike has also supported JPL tasks for the Defense Information Systems Agency (DISA) on the security of the DoD's Global Information Grid (Grid).