NASA/TM—2016-219123

Security Policy for a Generic Space Exploration Communication Network Architecture

William D. Ivancic, Charles J. Sheehe, and Karl R. Vaden
Glenn Research Center, Cleveland, Ohio

November 2016

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI Program provides access to the NASA Technical Report Server—Registered (NTRS Reg) and NASA Technical Report Server—Public (NTRS) thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part of peer-reviewed formal professional papers, but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., "quick-release" reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov

- E-mail your question to help@sti.nasa.gov

- Fax your question to the NASA STI Information Desk at 757-864-6500

- Telephone the NASA STI Information Desk at 757-864-9658

- Write to:
  NASA STI Program
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/TM—2016-219123

Security Policy for a Generic Space Exploration Communication Network Architecture

William D. Ivancic, Charles J. Sheehe, and Karl R. Vaden
Glenn Research Center, Cleveland, Ohio

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

November 2016

Level of Review: This material has been technically reviewed by technical management.

Available from

NASA STI Program
Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
703-605-6000

This report is available in electronic form at http://www.sti.nasa.gov/ and http://ntrs.nasa.gov/

Contents

Security Policy for a Generic Space Exploration Communication Network Architecture

William D. Ivancic, Charles J. Sheehe, and Karl R. Vaden
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

Abstract

This document is one of three. It describes various security mechanisms and a security policy profile for a generic space-based communication architecture. Two other documents accompany this document—an Operations Concept (OpsCon) and a communication architecture document. The OpsCon should be read first followed by the security policy profile described by this document and then the architecture document.

The overall goal is to design a generic space exploration communication network architecture that is affordable, deployable, maintainable, securable, evolvable, reliable, and adaptable. The architecture should also require limited reconfiguration throughout system development and deployment. System deployment includes subsystem development in a factory setting, system integration in a laboratory setting, launch preparation, launch, and deployment and operation in space.

1.0 Goals

This document was produced as part of an effort to create a generic space exploration communication network architecture. The overall goal of this effort is to design a communication network for manned or unmanned space exportation that is (1) affordable, (2) deployable, (3) maintainable, (4) securable, (5) scalable, (6) evolvable, and (7) reliable (robust). Failure to meet items 3 through 7 will result in a system with significant hidden costs that only materialize after initial deployment.

A secondary goal is to design the network such that it requires limited reconfiguration throughout system development and deployment. System deployment includes subsystem development in a factory setting, system integration in a laboratory setting, launch preparation, launch, and deployment and operation in space—cradle-to-grave (end-of-mission).

2.0 Introduction

This document is one of three. Two other documents accompany this document—an Operations Concept (OpsCon) (Ref. 1) and a communication architecture document. The OpsCon should be read first followed by the security policy profile and then the architecture document.

The purpose of this particular document is to define what the security policy is and how it affects network architecture and design. Various existing and emerging network architectures, technologies, and security mechanisms are described. In addition, the following critical items that need to be considered are off-nominal operations, the effect that the environment has on the system, and how cryptographic systems work is presented.

Security is based on trust and risk management. Trust is built from the ground up and from the top down. Trust is the acceptance that the hardware is doing and what is expected of it, that software is doing what is expected of it, and that each entity in the system is doing what is expected of them. With trust comes some element of risk. Blind trust is dangerous. Thus, it is imperative that system developers and integrators test in a relevant environment to ensure that the system operates as expected (trust but verify).

3.0 Terminology

In order to ensure understanding, a common vocabulary must be established. The following sections define a common vocabulary relative to communication networking and data security.

3.1 Security Activities

The following are five security activities in an information system (Ref. 2):

Physical security deals with all the physical aspects in a system and its environment. Examples include access control to the equipment or physical redundancy. Physical security will not be addressed in this document.

Operational security is concerned with all the functional aspects of the system including maintenance, backups, and system configuration control. Operational security will not be addressed in this document.

Logical security includes security mechanisms such as types of cryptography, authentication procedures, and deployment of antivirus protection. This document will only address some aspects of cryptography and authentication related to protecting information.

Application security measures are taken throughout the code's life cycle to prevent gaps in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application (Ref. 3). Application security is briefly addressed in this document.

Telecommunication security is the set of security mechanisms directed and end-to-end security for the final user including resource utilization, communications protocols, and operating systems (OSs) and equipment. This document will address some areas of resource utilization and communication protocols.

3.2 Security Mechanisms

Access Control has a broad scope. Access control is the selective restriction of access to a physical place or resource. In this document we are concerned with access to information, networks or utilization of resources (e.g., access lists, ip-tables, Virtual Local Area Networks (VLANs)), and machine-to-machine access to systems (e.g., radio network access, etc.).

Authentication is the ability for a sender or a receiver to prove its identity to the entity it is communicating with.

Cryptography is utilized to accomplish this. This document will address authentication.

Confidentiality preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (Ref. 4). A loss of confidentiality is the unauthorized disclosure of information. Confidentiality is extremely important for sensitive data ranging from command and control to personal medical data (due to Health Insurance Portability and Accountability Act (HIPAA) (Ref. 5)). Cryptography is utilized to accomplish this. This document will address confidentiality.

Integrity is guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. Integrity is extremely important for data such as command-and-control messages, scientific data, and telemetry used for operational decision making. Cryptography is utilized to accomplish this. This document will address integrity.

Nonrepudiation ensures that communicating parties cannot deny the occurrence of a given event (typically the post or the reception of a message). For nonrepudiation with proof of origin, the recipient of data is provided with proof of the origin of data protecting against any attempt by the sender to falsely deny sending the data or its contents. Cryptography is utilized to accomplish this.

Availability is ensuring timely and reliable access to and use of information. Relative to security, availability has more to do with denial of service (DOS). Another area that affects availability is system

reliability. Relative to space exploration network architecture, we will assume data availability is a non-issue by design. Availability will not be addressed in this document.

4.0 Policy

Policy is everything. Policy (a.k.a. doctrine) will make or break a network design. Policies are the rules of engagement (how one is permitted to operate). Policy is often set by those who have little understanding of the full ramifications of their policies. Policy is often given as an overarching set of rules and an assumption that one size fits all. Blind policy can be very costly and overbearing and can become, in and of itself, a DOS.[1] Policy is extremely hard to change because it requires an understanding of why the policy is in place and what the ramifications are and places ultimate responsibility on the policy setter.[2] Security policy often blindly follows International Telegraph Union (ITU) (Ref. 6) or National Institute of Standards and Technology (NIST) (Ref. 7) recommendations without understanding the intent of those recommendations, which allow systems to be tailored. Thus, one will end up with the same security policy placed on an experimental testbed or a space-based network as those of an entire enterprise system—particularly within the U.S. Government.

The following are a few examples of policies related to a space-based communication network:

Space missions are generally government-funded. If you have a deep space mission that can utilize the relay satellite of another country, a country that may not have the same political ideals as your country, are you willing to utilize that asset and accept the risks that go along with that decision? Or, do you deploy your own relay system? In our fiscally restrictive world, do you have the resources to deploy your own system?

If you are using a Store, Carry and Forward (SCF) protocol, this will result in data at rest (DAR) at intermediate forwarding nodes. Are you willing to utilize the assets of another country that may not have the same political ideals as yours? Are you willing to use another country's ground stations when you have DAR that can be acted upon over a long period of time? Note, data in transit can be captured and copied and easily become DAR (Ref. 8).

There is no right or wrong answer in the two examples provided, but the answers drive the system design and the security design—both which should be as one.

5.0 Givens

The following are facts and observations that must be considered in order to develop sound security policies and architectures. They are presented in no particular order of importance. All must be considered.

[1]The following is a prime example of blind policy: In 2015, the U.S. Government implemented a policy that all Government laptop computers must have their hard disks encrypted. This is known as Data at Rest (DAR). This policy was put in place after a Government laptop with personnel information was lost or stolen. NASA often employs college students to work at their facilities for 10-week periods over the summer. It is useful to have the students issued laptop computers instead of desktop computers as they move from room to room depending on space availability. A request was made for laptops with the Linux operating system. The request was denied as the group in charge did not have a Linux laptop build with DAR, even though the current Linux open source build had DAR capability. However, the security group would allow the students to have a Linux desktop since the policy did not require desktop computers to have DAR enabled. Note, that at no time would the students have any critical information that needed protection and the hard disks are wiped clean at the end of the 10-week session.

[2]The U.S. military is often more willing to modify policy than other large organizations. To quote a general presenting at a meeting on space-based networking, "Doctrine will change to meet the needs of the warfighter." This may appear counter-intuitive at first until one comes to the realization that in the military, the policy makers have moved through the ranks and have experienced the ramifications of poor, inflexible doctrine.

1. “It is a well-known fact that no other section of the population avail themselves more readily and speedily of the latest triumphs of science than the criminal class.” —Inspector John Bonfield, Chicago Police 1888.
2. Too much security is no security as people find a workaround to avoid the security measures (Ref. 9).
3. “Security is hard. It is a negative deliverable. You don’t know when you have it, only when you have lost it!” —Latif Ladid (IPv6 Forum).
4. “Network Security itself does not provide any type of Return on Investment (ROI). It is about cost management. For example: You buy a Picasso straight from the artist and a safe to store it in. The safe adds no value to the painting. It only helps prevent loss of the painting (i.e., a cost to you).” —Yurie Rich, Command Information.
5. Architecture plays a major role in securing information systems. The placement of firewalls, proxies, and cryptographic elements all affect security and should be considered from day one of the design process.
6. The simpler the network architecture, the better the security because one is more likely able to identify security vulnerabilities and thereby protect against those vulnerabilities. Complexity makes systems more vulnerable and fragile.
7. Security breaks everything—or at least it appears to. Security is known as the ultimate DOS!
8. The application of the various security mechanisms and protocols is highly dependent on the environment in which they have to operate. Key factors include the available bandwidth, the end-to-end delay, and whether or not one has two-way communications.
9. We need sufficient data capacity in the link[3] to ensure security as cryptography adds overhead to data.
10. Private address space is just that, it is private and uncoordinated. Any attempt to coordinate private address space will likely result in failure—particularly when coordination is across disparate organizations, for example, the National Aeronautics and Space Administration (NASA) and European Space Agency (ESA).
11. “Everybody is talking about the Internet of things as the future of the Internet. Well, all of that is based on IPv6. There’s no way we can make IPv4 (IP version 4)...support the Internet of things in the future. It won’t work. We need to adopt IPv6. We need to make it happen.” —Jacques Latour, Canadian Internet Registration Authority (CIRA).
12. Securing information at the source provides much more flexibility than securing the information at lower layers and requires the least amount of trust.
13. Conversely, providing security at the physical layer or data link layer provides the least amount of flexibility, the greatest cost and requires the greatest amount of trust.
14. DAR has significantly different challenges than data in transit simply because time is not on your side. Note: data in transit can easily be turned into DAR.
15. Some data is only useful for a limited period of time. In such cases, time is on your side.
16. Ground-based systems can assume, for all practical purposes, infinite bandwidth or at least sufficient bandwidth to get the job done.
17. Space environments often feature limited bandwidth, extreme delays and highly asymmetric links.
18. During launch, communication links are extremely low-rate, for example, tens of kbps forward (uplink) to hundreds of kilobits per second on the return (downlink). This is due to the difficulty in pointing antennas on a vehicle moving at extremely high speeds with a constantly changing orientation. Note: launch vehicle data is much more important when things go wrong (e.g., tumbling).
19. It is possible to lock yourself out of your own system. Assume this will happen and always provide a mechanism to recover your system or be willing to accept the consequences (e.g., loss of system).

[3]Loosely correlates to radiofrequency (RF) bandwidth. However, noisy links, modulation, coding, et cetera, affect how much data can be transmitted over a given bandwidth.

20. Cognitive networking[4] requires situational awareness. One needs to expose many portions of a network to enable learning and intelligent decisionmaking. This is often in contrast with security, which attempts to hide situational awareness from all but the security mechanisms and operations.
21. Off-nominal contingency operations need serious consideration with regard to how those operations affect the security of the communications network and the physical systems. This is particularly difficult for space communications systems where the asset is only reachable via radio links. Furthermore, when a space-based system is in trouble, the communication links are often extremely low bandwidth and unreliable.
22. Security by obscurity is not security, particularly if the perceived security in nonexistent.[5]

6.0 Hardware

Machines do not trust, they perform activities and run software. "Trustworthy and secure, means that first and foremost, there must be a level of confidence in the feasibility and correctness-in-concept, philosophy, and design, regarding the ability of a system to function securely as intended." (Ref. 11).

The security principle of modularity services is to isolate functions into well-defined logical units so that they can be composed. Layering relates to the application layer, network layer, and security kernel/device layer. The modular units are put together at each layer and each layer is added together, which provides well-defined functionalities that can provide a valid model of trust (Ref. 12).

6.1 Virtualization

Virtualization provides the following functions that improve security via architecture: isolation and multitenancy;[6] segmentation; and service insertion and chaining. Virtual networks are isolated from other virtual networks and from the underlying physical network by default, ensuring users or processes access only the information and resources that are necessary for its legitimate purpose. Virtualization provides the ability to build policies that leverage service insertion, chaining, and steering to drive service execution in the logical services pipeline based on the result of other services. For example, one can map security policies to virtual machines (VMs) and seamlessly steer network traffic from designated workload VMs to advanced security appliances to enforce the proper policies.

Virtualization is performed using VMs whereby an entire OS is virtualized inside another physical machine and OS. Virtualization is also performed using containers (Ref. 13). Containers are often considered as something in the middle between a chroot[7] and a full-fledged VM. They create an environment as close as possible to a standard Linux installation but without the need for a separate kernel. Thus, containers require very little overhead.

Virtualization combined with software-defined networking (SDN) provides great flexibility in network design by allowing network administrators to manage network services through higher-level functional abstraction. This is done by separating control plane functions from the data forwarding plane.

6.2 Complex Electronics (CE)

The area of trust that must be incorporated into a space architecture is securing the device including the physical network element, the platform, and any CE. One must be able to trust that the device will be

[4]A cognitive network incorporates learning algorithms (Ref. 10).

[5]A high-level manager in NASA once stated that use of Consultative Committee for Space Data Systems (CCSDS) protocols over Internet Protocol (IP) was more secure because not as many people were familiar with CCSDS protocols. Yet, CCSDS protocols are published standards available for anyone to obtain and understand.

[6]Multitenancy is an architecture in which a single instance of a software application serves multiple customers.

[7]"Chroot" is an operation that changes the apparent root directory for the current running process and their children. A program that is run in such an environment cannot access files and commands outside that environmental directory tree.

available and function as expected. Complex devices must have their own individual security, functions, or policies that are independent, yet clear, simple, and sufficient for that device to ensure the device performs its intended purpose.

CEs will perform the bulk of sensor processing and provide the bulk of communications. Their functions vary from measuring a temperature to destroying an errant vehicle. Their complexity can vary from multicore processors to a simple wireless sensor node. CEs need varying levels of resource monitoring with built-in security services, dictated by the device's resources and trust needed and defined by its security policy.

7.0 Namespaces (Naming and Addressing)

Why have a section on namespace (naming and addressing) in a security policy document? Much of security and securing networks has to do with sound architecture. Proper use of naming and addressing is key to development of a simple, elegant architecture. In today's Internet, because of poor use of naming and addressing, it becomes very difficult to properly secure a network. This becomes more and more evident as devices become more mobile and the points of attachment to the network vary dynamically. Furthermore, many, if not most, of these mobile systems are multihomed systems. That is, information can be sent over a variety of links. It is also possible with today's technology to use those links simultaneously. Thus, traditional security methods fail miserably.

Much of our concepts presented here for naming and addressing come from three sources: "Patterns in Network Architectures" (Ref. 14), "A note on Inter-Network Naming, Addressing, and Routing" (Ref. 15), and "On the Naming and Binding of Network Destinations" (Ref. 16). In particular, Saltzer (Ref. 16) provides a summary of services, nodes, and attachment points that, if strictly followed, enables services (a.k.a. applications) to be distributed and/or move, multihoming of nodes, and mobility.

There are two basic forms for names: locators and identifiers. Locators (a.k.a. addresses) are points of attachment. It is highly desirable that addressing is hierarchical in order to aid in routing as agents need some clue about where to send information in order to get "closer to the destination" even if they do not know the best direct path. Identifiers are not necessarily hierarchical, and may or may not be human readable. Identifiers should be unique and are used to identify applications or services. Identifiers are bound to locators and discovered via some type of directory service. This binding may change over time, particularly for mobile systems or where an application may move.

In the Internet, there is one namespace, IP addresses, for routing. The World Wide Web contains Uniform Resource Locator (URL) for higher-level identifiers. The Domain Name System (DNS) directory provides a directory service for mapping computers, services, or any resource (e.g., email, Unique Resource Locator for Web services, etc.) connected to the Internet. The limitation of one namespace, and the global visibility of that namespace to applications, is a root cause of many complexities and fragilities within today's Internet architecture, including the inter-domain routing system, the DNS, IP neighbor discovery, and other aspects. This has led to a multitude of security issues related to not being able to verify ownership of particular identifiers or addresses and not being able to authenticate the bindings between particular identifiers and addresses. These issues have, to some extent, been patched over with Boarder Gateway Protocol Security (BGPSEC), Secure Inter-Domain Routing (SIDR) (Ref. 17), Domain Name System Security (DNSSEC) (Ref. 18), Secure Node Discovery (SeND) (Ref. 19), and other extensions, but these have shifted the security issues to issues of increased operational and infrastructure complexity. Both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) namespaces still have centralized (though hierarchical) allocation and management at the top by organizations such as Internet Assigned Numbers Authority (IANA), Internet Corporation for Assigned Names and Numbers (ICANN) and various regional Internet registries (RIRs). There are no real mechanisms available for creating new namespaces. Even with IPv6, the 128-bit fields have been fixed and follow formats with prefixes that IANA defines.

The traditional approach to networking in today's Internet is to build one big layer-3 network and then deploy firewalls and Virtual Private Networks (VPNs) throughout until one deems the network

secure. Unfortunately, the configuration becomes so baroque that it will almost certainly break eventually—if not already broken. One new approach is to use credentials to build pairwise relations with neighbors or end-to-end peers, and to verify hosts and data prior to committing resources. No firewalls, VPNs, et cetera, are required in order to implement the policies and security postures desired. Rather, the architecture is simply secure by design (Ref. 20).

8.0 Architecture

Architecture plays a major role in securing information systems. The placement of firewalls, proxies, and cryptographic elements all affect security. Security breaks everything, or at least sometimes it appears to. Security mechanisms often do not interact well with other protocols. For example, security mechanisms often try to hide situational awareness from everything but security mechanisms. Whereas, something like cognitive networking requires situational awareness.

8.1 Transmission Control Protocol/Internet Protocol (TCP/IP)

Today's terrestrial Internet based on IP technologies has known flaws. One is the difficulty in handling multihome mobile devices, or networks. The current Internet security architecture more often than not uses the point of attachment address to identify an entity. Thus, when a device has multiple points of attachment and is mobile, the points of attachment are constantly changing. For this case, security based on addressing fails miserably.

Following the Internet Architecture Board's (IAB's) Routing and Addressing Workshop in October 2006 (Ref. 21), the Internet Engineering Task Force (IETF) formed the Locator/Identifier Separation Protocol (LISP) working group to address known issues with the current Internet architecture (see section 7 of this document, namely, scalable routing and addressing architectures). In general, LISP was to address "locator/identifier separation." The current problems arise because the IP address combines two functions, routing locators (point of attachment) and identifiers (who you are) in one number namespace. Separating location from identity should allow for efficient aggregation of the routing locator space and providing persistent identifiers in the identifier space. The goal of LISP is to develop protocols that require no changes to either host protocol stacks or to the "core" of the Internet infrastructure, and offer traffic engineering, multihoming, mobility, and other benefits of an identification/location split and can be incrementally deployed (Ref. 22).

One evolving protocol and two future architectures that can utilize, replace, or enhance the current Internet are Host Identity Protocol (HIP) (Refs. 23 and 24), Recursive Inter-Networking Architecture (RINA) (Ref. 25), and Information-Centric Networking (ICN) (Ref. 26). Each of these has the potential to greatly improve and simplify architectures and security, particularly RINA. HIP and RINA are similar in that both attempt to solve the problem in TCP/IP architecture as a result of a poorly defined namespace. However, HIP attempts to leverage the TCP/IP architecture whereas RINA takes a clean slate approach.

8.2 Host Identity Protocol (HIP)

HIP was created, in part, to address the deficiencies of the current Internet as a result of the deficiencies in the namespace (i.e., DNS tied to point of attachment). In particular, in the current Internet, the transport layers are coupled to the IP addresses. Neither can evolve separately from the other. HIP attempts to solve this problem by separating the identity of a host from its location. HIP defines a new namespace between the network and transport layers of the TCP/IP architecture. HIP provides upper layers with mobility, multihoming, Network Address Translation (NAT) traversal, and security functionality. The location of the host is bound to IP addresses and is used for routing packets to the host over the current Internet. However, transport and application layers use host identity, which is associated to a private-public key pair. A host obtains the identity of a peer from the DNS or a Distributed Hash Table (DHT). If DNS or DHT infrastructure is not available, one can use opportunistic HIP for contacting

a peer without being able to authenticate the peer. Communications between entities will be protected, but both parties are taking a risk as they cannot validate the true identity of the peer, at least not using the feature provided within HIP. HIP is currently an experimental protocol within the IETF, but the HIP working group is presently chartered to produce standards track versions of the main HIP Request for Comments (RFCs) taking as a base the existing experimental RFCs. The working group will also specify certificate handling in HIP in a standards track RFC.

8.3 Recursive Inter-Networking Architecture (RINA)

"RINA is a new concept that is gaining momentum quickly with a multitude of newly funded research (Refs. 25, 27, and 28). RINA is a clean-slate Internet architecture that builds on a very basic premise, yet fresh perspective that networking is not a layered set of different functions but rather a single layer of distributed Interprocess Communication (IPC) that repeats over different scopes—i.e., same functions/mechanisms but policies are tuned to operate over different ranges of the performance space (e.g., capacity, delay, and loss)—Figure 1. Furthermore, how a Distributed IPC Facility (DIF) is managed, including addressing is hidden from the applications (Ref. 29) thereby enabling applications to be developed within a more secure architecture." —The Recursive InterNetwork Architecture (Ref. 30).

Some important features of RINA are

- Enabling of multihoming and mobility
- Reduction in overhead by reducing addressing
- Increased routing performance and reduce routing tables
- Enabling of scoped Quality-of-Service (QoS)
- Simplified security
- Enabling of shared infrastructure

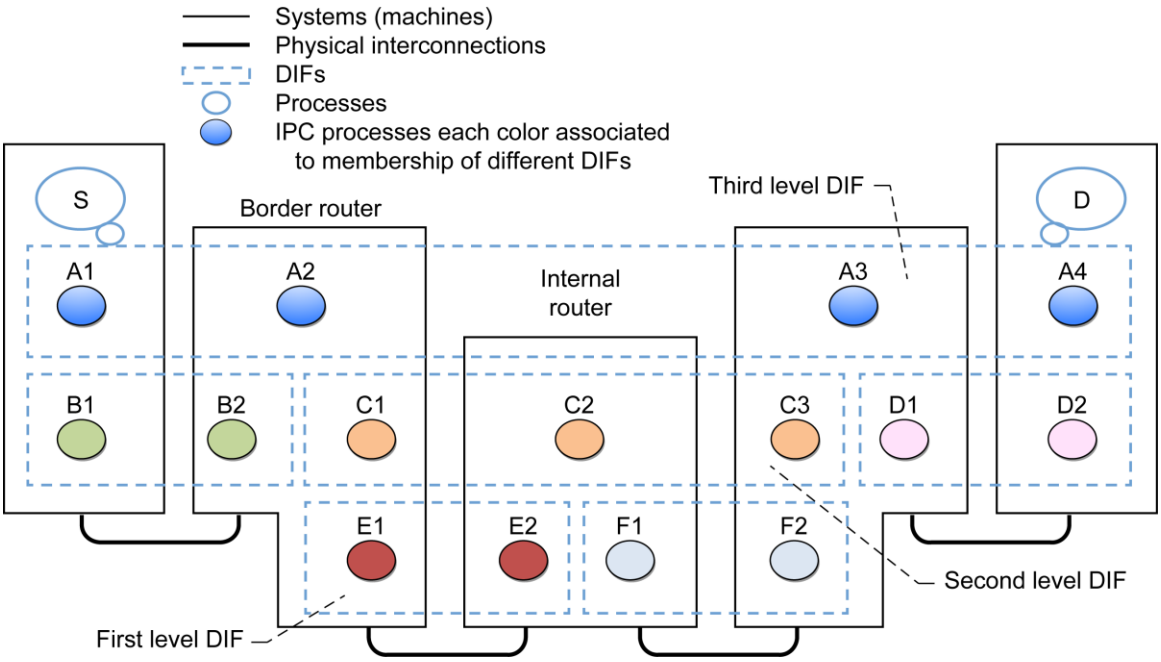

Figure 1.—Example of the Recursive Inter-Networking Architecture (RINA) architecture (Ref. 30). DIFs is Distributed Interprocess Communication (IPC) Facilities.

8.4 Information-Centric Networking (ICN)

"Information-Centric Networking (ICN) marks a fundamental shift in communications and networking. In contrast with the omnipresent and very successful host-centric paradigm, which is based on perpetual connectivity and the end-to-end principle, ICN changes the focal point of the network architecture from the end host to 'named information' (or content, or data). In this paradigm, connectivity may well be intermittent. End-host and in-network storage can be capitalized upon transparently, as bits in the network and on storage devices have exactly the same value. Mobility and multi-access are the norm, and anycast, multicast, and broadcast are natively supported." —RFC 7476 (Ref. 31).

Companies such as Google, Facebook, and Netflix are interested in ICN as these groups specialize in content delivery.

9.0 Environment

The application of the various security mechanisms and protocols is highly dependent on the environment in which they must operate. Key factors include the available bandwidth, the end-to-end delay, and whether or not one has two-way communications.

The available bandwidth may dictate what type of security protocols one wishes to use, particularly with regard to key negotiation such as Internet Key Exchange (IKE) or Internet Key Exchange Version 2 (IKEv2). Limited bandwidth may also render use of large keys or certain algorithms difficult, impractical or impossible.

Large end-to-end delays may break certain security measures. The basic problem is that many security schemes require some type of time-sensitive challenge/response technique. Often, time sensitivity is added to circumvent man-in-the-middle and replay attacks. In many cases implementations allow some adjustment of the time sensitivity. However when one gets into the realm of a few seconds of round trip times (RTTs), one may have reached the limitations of some protocol implementations. Protocols that have time-sensitive security mechanisms include IKE, IKEv2, and mobile-IP.

Most, if not all, key negotiation and time-sensitive security mechanisms require two-way communication in order for the receiving system to send a challenge to the communication initiator and for that communication initiator to send a response. Note, this does not necessarily mean that a specific link has to be bidirectional or symmetric, only that two-way communication must be possible end to end. Thus, if secure communication must be performed over a unidirectional link with no response, only those protocols that can operate in such an environment can be used. IP Security (IPsec) is one such protocol. However, pre-placed keys or cached keys and preconfigured security associations are necessary as negotiation of keys, algorithms, and security associations are not possible (see IPsec Section). In theory, Delay/Disruption/Disconnection Tolerant Networking (DTN) and its associated security mechanisms are supposed to work in this environment. However, there is currently no approved IETF standard for DTN or DTN security and no approved key management mechanism.

10.0 Off-Nominal Operations

Off-nominal contingency operations need serious consideration. Depending on the security mechanisms put in place, security is likely to be compromised in the name of recovery. The following are a few questions that must be considered:

- How does one perform hardware reset of a system (e.g., satellite and rover)? In many space-based systems, hardware reset signals can be set by ground command via a critical command decoder. The need to protect how such a reset is accomplished is critical.
    - This is particularly interesting for a system that is only reachable via SCF techniques (e.g., a rover on the dark side of the Moon) (Ref. 32). Sending such a command through a SCF network that may consist of multiple hops is nontrivial, particularly if one does not own and operate the entire network infrastructure.

- What happens if a system loses time synchronization and the system relies on a protocol that requires time synchronization such as DTN (Refs. 33 and 34)?

11.0 Cryptography and Key/Certificate Management

The main purpose of encryption is to hide information from anyone or anything that does not have a proper key. The intent is to make it so difficult to obtain the information that the effort becomes overbearing.

"One of the big revelations to come out of the National Security Agency (NSA) documents leaked in 2013 by Edward Snowden didn't have to do with what the NSA was doing with our data. Instead, it had to do with what the NSA couldn't do: Namely, the agency couldn't break cryptography. ...The weakness in encryption isn't the algorithms and it isn't data in transit; it's everything else (e.g. bad implementations, the weak keys, any kind of back doors being inserted in the software, and how encryption keys are stored)." (Ref. 35). Henceforth referred to as the "Snowden Revelation."

Note, recently it was estimated that the Federal Bureau of Investigation (FBI) paid over $1.3 million to have someone obtain access to an iPhone used by terrorists. Yet, it is unclear whether the technique used actually broke the encryption or simply found a way to get past the locking mechanism. Reports seem to indicate that the later may be true, which further backs the Snowden Revelation. "First, it was the FBI to break into an encrypted iPhone without Apple's help. Around the same time, the Los Angeles Police Department (LAPD) was breaking into an iPhone on its own. In either case, the mysterious hacks used by law enforcement did not actually break Apple's encryption algorithms, but they allowed investigators to access data on devices that were locked." (Ref. 36).

The following section provides an overview of cryptographic techniques used in communication networking including symmetric and asymmetric cryptography and key management.

Symmetric encryption uses the identical key to both encrypt and decrypt data (a.k.a. shared key). A major advantage of using symmetric encryption is symmetric key algorithms trend to be computationally much faster than asymmetric algorithms. A disadvantage is that symmetric keys are not scalable. One needs to maintain a separate symmetric key for each entity one wishes to communicate with in order to maintain separate and confidential communication channels. In addition, it is difficult to know if a symmetric key has been compromised. The longer one uses a key, the more information an attacker has to compromise the key. Thus, it is highly desirable to change symmetric keys periodically such as after a certain amount of time has passed or a certain amount of data has been encrypted. The ability to change the symmetric key periodically in a controlled manner is part of key management. If one changes the key for each time two identical entities communicate, that is known as a session key.

Asymmetric encryption uses two related keys (public and private) for data encryption and decryption. The private key is never exposed. A message that is encrypted by using the public key can only be decrypted by applying the same algorithm and using the matching private key. The main advantage of asymmetric cryptography is that it scales. One only needs to know the public key of each entity one wishes to have secure communications with. The disadvantage of asymmetric cryptographic algorithms is that they are much more computationally intensive and thus slower than symmetric cryptography.

Asymmetric cryptography is often applied to solve the secure key distribution problem. One can encrypt a session key using the public key of the entity one wishes to communicate with. Only the entity with the private key can then decrypt the encrypted session key. In this manner, asymmetric cryptography is used to establish a symmetric session key. Thus one gets the best of both asymmetric and symmetric cryptography: scalability and speed.

Asymmetric keys are often allocated as part of a security certificate (a.k.a. public key certificate, digital certificate, or identity certificate). A security certificate proves ownership of a public key. Security certificates are the basis for identity-based security and Public Key Infrastructure (PKI). The PKI for the Internet is described in a series of X.509 RFCs as well as International Telegraph Union—Telecommunication Standardization Sector (ITU–T) documents. For example, RFC 5280 (Ref. 37) profiles the X.509 v3 certificate and X.509 v2 Certificate Revocation List (CRL) for use in the Internet.

Key revocation is an essential part of key management. When a key has been compromised or is no longer valid that key must be removed from the system. Such removal procedures are known as key revocation. How one determines a key is compromised is out of scope for this document. One common way a key may become invalid is if an individual or entity is no longer part of the security enclave such as when someone leaves the company. When this happens, there needs to be a mechanism in place to inform all others in that enclave that a particular key is no longer valid even if the date on the associated certificate indicates otherwise.

Key management is an extremely complex and difficult problem in any environment. Within the Internet, protocols have been established for key management. However, the assumption is that systems are fully connected—at least most of the time—and that there is sufficient data capacity in the links to enable real-time communications with key servers, certificate authorities, and revocation list servers. In aeronautics and space, this is often not the case with the exception of the ground-based portion of the network. Communication links often have very low data capacity or low-data-rate links. Systems are often disconnected and, for space-based networks, this may be for very long periods of time. Furthermore, the transmission propagation delays for deep space communications may make negotiation of session keys impractical. Thus, although many of the cryptographic algorithms and techniques used in the Internet can be applied to aeronautics and space-based communications, many of the protocols and procedures cannot. Key management and distribution in aeronautics and space is an area that requires much research and development.

12.0 Security Layers/Mechanisms

12.1 Physical

The physical layer in communications networks pertains to the wired, fiberoptic, or wireless channels. These channels are susceptible to eavesdropping. With regard to wireless systems, jamming is also possible. Numerous techniques can be deployed to help protect these channels. Bulk encryption is one mechanism. For wireless systems, some often used security mechanisms including spread spectrum techniques, frequency hopping, and information theoretic security.[8] Combining all of these techniques results in a multidimensional, multifaceted, cross-layer security solution. Except for many-to-many radio systems, physical link security does not scale. It only secures point-to-point traffic. In addition, if one wishes to send the bulk encrypted data to some decryption unit that is not at the other end of the radio, one needs specialized hardware to wrap the data into routable packets that can be transported over the Internet (Figure 2). This is an extremely expensive proposition because it requires specialized hardware at each ingress and egress point. This generally means one must own the ingress and egress points inhibiting the use of shared infrastructure.

One attractive characteristic of bulk encryption is that it is relatively easy to manage because there is nothing like Security Associations (SAs) or Security Policy Databases (SPDs), Security Association Databases (SADs), and Peer Association Databases (PADs) as in IPsec (Ref. 38). Bulk encryption is relatively foolproof because everything is encrypted. However, scalable deployment of security keys is extremely complex—particularly for over-the-air keying (Ref. 39).

[8]Information theoretic security combines signal processing, communications, and coding technique to exploit radiofrequency channel characteristics such as multipath.

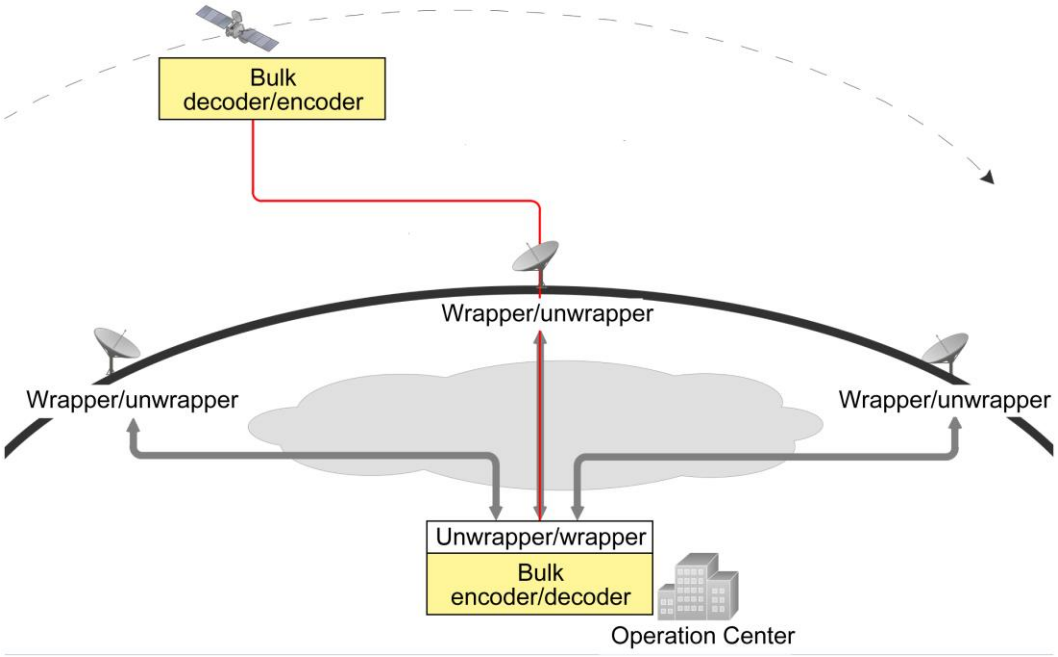

Figure 2.—Bulk Encryption Architecture.

12.2 Data Link

The data link can be over a wired or fiberoptic or wireless system. For wired systems, the traditional assumption has been that the system is trusted. There are exploits that occur in wired data links (Ref. 40), but for a closed space-based network, the assumption of a trusted wired network is reasonable. For wireless communications, security is usually performed in the data link layer. The security usually takes two forms, access control and encryption of the data channel. This is the case for commercial off-the-shelf (COTS) systems such as Wi-Fi (802.11 family) and WiMax (802.16 family). Access control may be performed using passwords, shared secrets, preconfigured Message Authentication Code (MAC) addresses or certificates.

CCSDS is currently, as of May 2015, developing a Space Data Link Security Protocol (SDLSP) (Ref. 41). This protocol will support the three Space Data Link Protocols: Telemetry (TM), Telecommand (TC), and Advanced Orbiting Systems (AOS). The SDLSP provides authentication, encryption, and authenticated encryption for the data in the Transfer Frame Data Field of a TM, TC, or AOS Transfer Frame. Note, the SDLSP does not address key management. It is also extremely bandwidth inefficient for securing IP traffic. Finally, as a data link protocol, it does not scale. It only secures traffic point to point.[9]

12.3 Network

Network-layer security is implemented by protecting the information payload to ensure confidentiality, authentication, and/or integrity. In many instances the original header is also obscured via a tunneling mechanism. In addition, mechanisms should exist that provide access controls at the egress and ingress of a system.

[9]In a properly architected communication network, lower-layer protocols should never (or very rarely) be tunneled over an upper-layer protocol.

In the Internet, network layer security is centered around IP addressing. One can use IPsec protocols to secure packets to ensure authentication, confidentiality, or both. IPsec-related protocols form the basis for IPsec. There are numerous (50 plus and growing) RFCs related to IPsec. RFC 4301 (Ref. 38) describes the security architecture for IP, which is designed to provide security services for traffic at the IP layer.[10] Other base IPsec RFCs describe encryption, cryptographic algorithms, and uses.

Network layer security can allow for great flexibility, but at the expense of complexity. IPsec is a prime example. One can control security at a network level down to a single source host to single destination host per protocol. Expect security in other network types (e.g., DTN and ICN) to implement similar granularity.

At the network layer, one may control access based on source or destination address or both using access lists such as those found in commercial routers or, in the case of Linux-based systems, iptables (Ref. 42). The iptables is a software mechanism to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Network layer security scales quite well in fixed networks.

One of the major flaws in today's Internet is that network security is closely associated with the point of attachment, the address. Thus, if an entity is mobile and multihomed (multiple points of attachment), security becomes difficult as the points of attachment keep changing. Thus, all of the SADs, SPDs, and PADs must be updated accordingly. IKEv2 Mobility and Multihoming Protocol (MOBIKE) (Ref. 43) is one protocol that attempts to address some of these issues.

12.4 Transport

Transport Layer Security (TLS) is designed to prevent eavesdropping, tampering, or message forgery for communication between hosts. TLS (Ref. 44) is the primary protocol used in the Internet today for communications security although Secure Socket Layer (SSL) (Ref. 45) may still be in use. SSL was developed by Netscape Corporation and for all practical matters has been replaced by TLS. The primary goal of TLS is to provide privacy and data integrity between two communicating applications. TLS is layered on top of some reliable transport protocol, generally Transmission Control Protocol (TCP), and provides security services to upper layer protocols such as Hypertext Transfer Protocol (HTTP) (Ref. 46). Use of TLS with HTTP (Ref. 47) is known as Hypertext Transfer Protocol Secure (HTTPS).

12.5 Application

One definition of Application security is a set of mechanisms to ensure the application is well written such that there are no vulnerabilities through flaws in the design, development, and maintenance of the application code. Another definition is methods of protecting applications from malicious attacks that may expose private information.

Some common applications are surfing the Web, remote login, file transfer, network management, Voice over Internet Protocol (VoIP), streaming media, Internet Relay Chat (IRC), and email. In reality none of these is secure per either definition above.

Various transport-layer security mechanisms are often used to limit access to an application. However, that does not mean the application is secure. Examples include

- Web applications use HTTP as the underlying protocol. HTTP can be secured to some degree with TLS.
- Secure remote login is generally performed using Secure Shell (SSH). SSH (Ref. 48) allows a user to establish a secure channel over an insecure network in a client-server architecture in a secure way. The SSH client has a local database that associates each host name (as typed by the user) with the

[10]If one wishes to understand what is required for any network security architecture, not just Internet Protocol, this is a good starting point.

corresponding public host key. Another method is to have the host name-to-key association is certified by a trusted Certificate Authority (CA).

- File transfers use File Transfer Protocol (FTP) which is unsecure. However file transfers can be secured using File Transfer Protocol Secure (FTPS), SSH File Transfer Protocol (SFTP) or Secure Copy (SCP). File Transfer Protocol Secure (FTPS) is provided by employing TLS protocol for channel encryption. SCP uses SSH 1.x which has been deprecated while SFTP uses SSH 2.x and is meant to replace SCP. For authentication FTPS uses X.509 certificates, while SFTP uses SSH keys.

Email and IRC (messaging) are protocols that were not designed with privacy or security in mind. The information can be secured using cryptographic techniques to either encrypt information and/or authenticate the sender of information to ensure information integrity. However, the information transmitted in the application is often the method used to gain initial access and exploit systems (e.g., viruses, malicious code, and phishing). Just because the information was encrypted does not mean that information is harmless.

Network management, in general, is a set of tools and protocols that allows one to control and configure network assets such as bridges, routers, servers, and workstations remotely as well as receive reports and triggers from those assets indicating the status and potential problems with systems. Simple Network Management Protocol (SNMP) is one of the main protocols used to perform these functions. SNMP has been refined over the years to include many security features to ensure only those SNMP controllers with proper credentials can manage assets. SNMPv3 includes three services: authentication, privacy, and access control. SNMPv3 introduced the concept of a principal, which is the entity on whose services are provided or processing takes place. The identity of the principal and the target agent together determine the security features that will be invoked, including authentication, privacy, and access control. The use of principals allows security policies to be tailored to the specific principal, agent, and information exchange and gives human security managers considerable flexibility in assigning network authorization to users (Ref. 49). SNMP is designed to operate in a fully connected network with relatively high bandwidth expectations. For space-based systems the basic ideas behind general network management applications would apply, but new techniques would need to be developed (Ref. 50).

12.5.1 Overlay Networks

A network overlay is simply one network residing on top of another. For example, Delay/ Disruption/Disconnection Tolerant Networking (DTN) is often consider an overlay network as it communicates over other heterogeneous networks via convergence layers (Figure 3). Thus DTN may operate over an IP network or Bluetooth (Bluetooth Special Interest Group) network. Likewise, it is possible to run an IP network over a DTN network such as was done in the Defense Advanced Research Projects Agency (DARPA) Wireless Network after Next (WNaN) radios (Ref. 51).

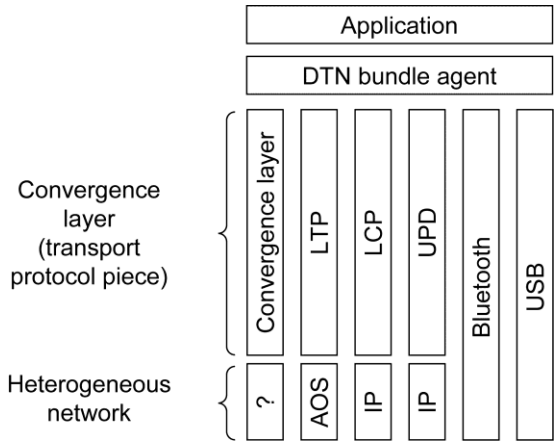

Figure 3.—Delay/Disruption/Disconnection Tolerant Networking (DTN) Bundle Protocol Architecture—RFC 5050 (Ref. 33).

ICN (Ref. 52) can also be considered a network overlay in some instances. ICN is an approach to evolve the Internet. Distributing and manipulating named information (e.g., pictures, videos, and cloud computing) is a major application in the Internet today. ICN enables data to become independent from location, application, storage, and means of transportation. Techniques such as in-network caching and replication are expected to greatly improve efficiency, better scalability with respect to information/bandwidth demand, and better robustness in challenging communication scenarios. Publish/Subscribe techniques are expected to dominate this network architecture. ICN has the potential to solve problems with mobility, multihoming, and simplifying security as emphasis is placed on protecting the data rather than the network.

13.0 Security Policy Profile

NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, and NASA Procedural Requirement (NPR) 2810.1, Security of Information Technology, provides more details on IT security requirements at NASA. However, these documents are directed at fixed terrestrial systems and must only be used as guiding principals rather than rigid documents. Policy must be tailored for the operational environment. Furthermore, these documents are somewhat dated in that they have no mention of ICN, DTN, RINA, or any other new networking concepts. The Internet and networking in general are changing. Systems are becoming mobile and multihomed (i.e., multiple connections off the system often to different links or even different service providers. New technologies such as SDN, ICN, and Multipath TCP (MP–TCP) are constantly being created. Much of these break traditional network security methodologies.

Proper security policy involves the development and application of sound risk management—yes, a sound security policy involves risk (Ref. 53). Self DOS is not sound security policy. Cover your butt (CYB)[11] is not a sound security policy. Security by obscurity is not a sound security policy. Sound security policy is only possible when one has a complete understanding of the network or networks involved in the overall communication architecture.

This security policy developed in the following subsections assumes a cooperating and collaborating multination network.

[11]Cover your butt (CYB) is an activity, usually in a work-related or bureaucratic context, done by an individual to protect himself or herself from possible subsequent criticism. CYB denotes a type of institutional risk-averse mentality that works against accountability and responsibility, which is harmful to the institution's overall effectiveness.

The system should work over shared infrastructure.

- One SHOULD NOT assume that we control all infrastructures.
- One SHOULD NOT assume that all entities providing infrastructure or communication services can be trusted.

The security policy MUST be at a level sufficient to (1) match the type of data is moving through the systems, (2) understand the degree that data (information) needs to be protected, and (3) identify where in the communication protocol stack that protection needs to occur (e.g., at the application, within the network, at the physical link or multiple places).

13.1 Recommended Policy

Complex Electronics (CE): CE need to be architected and designed for security policies. Software and hardware design must monitor operations and enforce assurance/security policies. The design should be kept as simple and small as possible. Access must be denied in the reset/default state. The protection scheme identifies conditions under which access is permitted. The security monitor failure state must be secure and within the defined normal operations of the system (fail safe).

Commercial off-the-shelf (COTS): Most commercial applications and Internet standard protocols will work perfectly spot fine in a space environment. For some communication links, the propagation delays can be quite long such as Earth to Mars or Earth to anything deep space beyond Mars. In this instance, a limited number of IP will work well. Another item that must be considered, which is not unique to space, is that systems are often disconnected from the network and do not have a clear, clean, large bandwidth connected path between source and destination. Anything on the ground or related to the ground infrastructure can most certainly use standard IPs and applications. Anything within a vehicle or near to the vehicle can most certainly use standard Internet Protocols (IPs) and applications to communicate within that domain. Thus we need sound security policies to enable use of COTS applications and Internet standard protocols while maintaining a secure network.

Studies have shown that “Open source (open source code) does not pose any significant barriers to security, but rather reinforces sound security practices by involving many people that expose bugs quickly, and offers side-effects that provide customers and the community with concrete examples of reusable, secure, and working code.” (Ref. 54). It is reasonable for one to expect similar with hardware and firmware (i.e., PLDs) as the greater the use and the variety of applications, the more likely vulnerabilities will be uncovered.

Encryption: Use encryption judiciously only where necessary. There is an expense for encryption and multiple layers of encryption add to the expense and complexity of the system. Encrypt all data that needs to be private or confidential at the source. If data is already encrypted at the source, bulk link-layer encryption does little to improve security, Bulk link-layer encryption does obscure what is happening on that direct data link, but for a very high price. Similar can be said for network-layer encryption. However, network-layer encryption does provide a mechanism for segregating networks while transversing the open Internet (i.e., red/black separation (Ref. 55)).

Data at rest (DAR): All data should be considered DAR simply because, for any large network that passes data over another’s network, one cannot truly ensure that data has not been copied and stored elsewhere.

Network segregation: Restrict access to only the networks of interest (i.e., segregate networks). This will simplify the security architecture and allow one to deploy proper security policies per network type.

Command and control: The following is required for all critical command and control networks such as those operating vehicle engines.

- Command-and-control networks MUST be segregated from general user network.
- Authenticate all command and control messages. Note encryption is a form of authentication. Authentication is not a form of encryption.

IPv4 vs. IPv6: All Internet Protocol (IP) systems should utilize IPv6 for a number of reasons:

- IPv4 is coming to end of life.
- There is a push for all new IPs to be IPv6 only (Ref. 56).
- IPv6 networks, if designed properly, should be greatly simplified as there should be no need for middle boxes such as NATs.
- IPv6 has scoped addressing (Ref. 57).

Shared infrastructure: Use of shared infrastructure is permitted. However, shared infrastructure should be treated as a "Black Network."[12] Data that needs to be protected should be encrypted to an appropriate level. Such encryption SHOULD be at the network layer or above, and SHOULD NOT be at the data link layer.

Use of shared infrastructure should be encouraged in order to reduce costs and increase flexibility and reliability.

Identity-based security: To remain architecturally sound and improve security, identity-based security (use of identifiers, secure namespaces, and certificates to validate identifiers) should be implemented (Ref. 20).

Auditing: One cannot place the same auditing requirements and implementations on space-based assets as would be done on ground-based assets.

Sign in: One cannot place the same sign in (a.k.a. log in) requirements and implementations on space-based assets as would be done on ground-based assets. For example, in manned space flight, you know the crew and hopefully trust them. Thus, local sign in may not be required. Safety over security.[13]

14.0 Summary

This document describes the various security mechanisms and a security policy profile for a generic space-based communication architecture. The overall goal is to design a generic space exploration communication network architecture that is affordable, deployable, maintainable, securable, evolvable, reliable, and adaptable.

Policies are the rules of engagement (how one is permitted to operate). Policy will make or break your network design. Policy should not be treated as one size fits all. Blind policy can be very costly and overbearing. Policy must be tailored for the operational environment. Documents such as NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, and NASA Procedural Requirement (NPR) 2810.1, Security of Information Technology, are directed at fixed terrestrial systems and must only be used as guiding principals rather than rigid documents when considering space and aeronautical environments.

[12]Encrypted and unencrypted networks are referred to as "red" and "black." The red network indicates the network is secure and the data is not encrypted (commonly referred to as the "plaintext" interface), and the black network is the side of the network that carries the post-encrypted data (commonly referred to as the "cipher-text" interface) (Ref. 55).

[13]The military High Mobility Multipurpose Wheeled Vehicles (HMMWVs) do not use keys. They have an on/off switch by the steering wheel, which makes it easier for the crew to get out of hot zones than if they have to find keys.

References

1. Ivancic, William K., et al.: Concept of Operations for a Generic Space Exploration Communication Network Architecture. NASA/TM—2015-218823, 2015.
2. Mahmoud, Ben; Larrieu, Nicolas; and Pirovano, Alain: An Aeronautical Data Link Security Overview. Presented at the 2009 IEEE/AIAA 28th Digital Avionics Systems Conference, Orlando, FL, 2009, pp. 4.A.4–1—4.A.4–14.
3. Application Security. 2015. http://en.wikipedia.org/wiki/Application security Accessed Sept. 8, 2016.
4. U.S. Code: Standards for Information Transactions and Data Elements. Public Law 42 u.s.c. 1320d-2, 2010. http://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap7-subchapXI-partC-sec1320d-2.pdf Accessed Sept. 8, 2016.
5. U.S. Congress: Health Insurance Portability and Accountability Act of 1996. 104th Congress Public Law 191, 1996.
6. International Telecommunication Union: Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800, 1991.
7. U.S. Department of Commerce: Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800–53, 2013.
8. Greenwald, Glenn; and MacAskill, Ewen: NSA Prism Program Taps in to User Data of Apple, Google and Others. The Guardian, vol. 7, no. 6, 2013, pp. 1–43.
9. Antonopoulos, Andreas M.: Can You Have Too Much Security? Network World, 2011. http://www.networkworld.com/article/2177700/ security/can-you-have-too-much-security-.html Accessed Sept. 8, 2016.
10. Ivancic, William D., et al.: Cognitive Networking With Regards to NASA's Space Communication and Navigation Program. NASA/TM—2013-216585, 2013. http://ntrs.nasa.gov
11. Boyens, Jon, et al.: Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Special Publication 800–161, 2015, p. 32.
12. Shin, Seugwon, et al.: FRESCO: Modular Composable Security Services for Software-Defined Networks. Presented at the 20th ISOC Network and Distributed System Security Symposium, San Diego, CA, 2013.
13. Linux Containers. LinuxContainers.org: Infrastructure for Container Projects. 2015. https://linuxcontainers.org/ Accessed Sept. 8, 2016.
14. Day, John D.: Patterns in Network Architecture: A Return to Fundamentals. Prentice Hall, Upper Saddle River, NJ, 2007.
15. Shoch, John F.: A Note on Inter-Network Naming, Addressing, and Routing. Internet Experiment Note #19, Notebook section 2.3.3.5, 1978.
16. Saltzer, J.: On the Naming and Binding of Network Destinations. Internet Engineering Task Force, RFC 1498, 1993. http://www.rfc-editor.org/rfc/rfc1498.txt Accessed Sept. 8, 2016.
17. Huston Geoff; and Bush, Randy: Securing BGP With BGPsec. Internet Society, vol. 14, no. 2, 2011.
18. DNS Security Extensions: ISMS and ISO 27001. http://www.dnssec.net/ Accessed Sept. 8, 2016.
19. Arkko, J., et al.: SEcure Neighbor Discovery (SEND). Internet Engineering Task Force RFC 3971, 2005. http://www.rfc-editor.org/rfc/rfc3971.txt Accessed Sept. 8, 2016.
20. Eddy, Wesley, et al.: Secure Naming and Addressing Operations for Store, Carry and Forward Networks. NASA/TM—2014-216665, 2014. http://ntrs.nasa.gov
21. Meyer, D.; Zhang, L.; and Fall, K.: Report From the IAB Workshop on Routing and Addressing. Network Working Group RFC 4984, 2007. http://www.rfc-editor.org/rfc/rfc4984.txt Accessed Sept. 8, 2016.
22. Farinacci, D., et al.: The Locator/ID Separation Protocol (LISP). Internet Engineering Task Force RFC 6830, 2013. http://www.rfc-editor.org/rfc/rfc6830.txt Accessed Sept. 8, 2016.
23. Moskowitz, R.; and Nikander, P.: Host Identity Protocol (HIP) Architecture. Network Working Group RFC 4423, 2006. http://www.rfc-editor.org/rfc/rfc4423.txt Accessed Sept. 8, 2016.

24. Gurtov, Andrei; Komu, Miika; and Moskowitz, Robert: Host Identity Protocol: Identifier/Locator Split for Host Mobility and Multihoming. Internet Protocol J., vol. 12, no. 1, 2009, pp. 27–32.
25. Pouzin Society: 2015. http://pouzinsociety.org/ Accessed Sept. 12, 2016.
26. Information-Centric Networking Research Group (ICNRG). 2015. http://trac.tools.ietf.org/group/irtf/trac/wiki/icnrg Accessed Sept. 12, 2016.
27. Tradeshow Management Services, Ltd.: Futurernet Expo Video. 2012. http://www.futurenetexpo.com/ Accessed Sept. 12, 2016.
28. IRATI: Investigating RINA as an Alternative to TCP/IP. 2012. http://irati.eu/ Accessed Sept. 12, 2016.
29. Day, J.; Matta, I.; and Mattar, K.: "Networking is IPC": A Guiding Principle to a Better Internet. Technical Report BUCS–TR–2008–019, 2008.
30. IRATI: The Recursive Internetwork Architecture. 2015. http://irati.eu/the-recursive-internetwork-architecture/ Accessed Sept. 12, 2016.
31. Pentikousis, K., et al.: Information-Centric Networking: Baseline Scenarios. Internet Research Task Force RFC 7476. 2015. http://www.rfc-editor.org/rfc/rfc7476.txt Accessed Sept. 12, 2016.
32. Macdonald, Malcolm; and Badescu, Viorel: The International Handbook of Space Technology. Springer-Verlag Berlin Heidelberg, New York, NY, 2014.
33. Scott, K.; and Burleigh, S.: Bundle Protocol Specification. Network Working Group RFC 5050, 2007. http://www.rfc-editor.org/rfc/rfc5050.txt Accessed Sept. 12, 2016.
34. Wood, Lloyd; Eddy, Wesley M.; and Holliday, Peter: A Bundle of Problems. IEEE Aerospace Conference, Big Sky, MT, 2009.
35. Laskowski, Nicole: Snowden: Data Encryption Is Good, But Not Good Enough. 2015. http://searchcio.techtarget.com/opinion/Snowden-Data-encryption-is-good-but-not-good-enough Accessed Sept. 12, 2016.
36. Smith, Chris: India Can Supposedly Bypass Iphone Encryption. 2016. http://bgr.com/2016/05/10/iphone-encryption-hack-india/ Accessed Sept. 12, 2016.
37. Cooper, D., et al.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Network Working Group RFC 5280, 2008. http://www.rfc-editor.org/rfc/rfc5280.txt Accessed Sept. 12, 2016.
38. Kent, S.; and Seo, K.: Security Architecture for the Internet Protocol Network Working Group RFC 4301, 2005. http://www.rfc-editor.org/rfc/rfc4301.txt Accessed Sept. 12, 2016.
39. National Security Agency: Field Generation and Over-the-Air Distribution of COMSEC Key in Support of Tactical Operations and Exercise. NAG–16F, 2001. https://info.publicintelligence.net/NSA-NAG-16F.pdf Accessed Sept. 12, 2016.
40. O'Connor, T.J.: Detecting and Responding to Data Link Layer Attacks. SANS Institute InfoSec Reading Room, 2010. http://www.sans.org/reading-room/whitepapers/detection/detecting-responding-data-link-layer-attacks-33513 Accessed Sept. 12, 2006.
41. The Consultative Committee for Space Data Systems: Space Link Data Link Security Protocol. Draft Recommended Standard CCSDS 355.0-R-2, 2012. http://public.ccsds.org/sites/cwe/rids/Lists/CCSDS%203550R3/Attachments/355x0r3.pdf Accessed Sept. 12, 2016.
42. Linux: Iptables. Section: iptables 1.4.20 (8), 2015. http://ipset.netfilter.org/iptables.man.html Accessed Sept. 12, 2016.
43. Eronen, P., ed.: IKEv2 Mobility and Multihoming Protocol (MOBIKE). Network Working Group RFC 4555, 2006. http://www.rfc-editor.org/rfc/rfc4555.txt Accessed Sept. 12, 2016.
44. Dierks T.; and Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.2. Network Working Group RFC 5246, 2008. http://www.rfc-editor.org/rfc/rfc5246.txt Accessed Sept. 12, 2016.
45. Frier, A.; Karlton, P.; and Kocher, P.: The SSL 3.0 Protocol (1969). Netscape Communications Corp., vol. 18, 1996, p. 2780.
46. Fielding, R., et al.: Hypertext Transfer Protocol—HTTP/1.1. Network Working Group RFC 2616, 1999. http://www.rfc-editor.org/rfc/rfc2616.txt Accessed Sept. 12, 2016.

47. Rescorla, E.: HTTP Over TLS. Network Working Group RFC 2818, 2000. http://www.rfc-editor.org/rfc/ rfc2818.txt Accessed Sept. 12, 2016.
48. Ylonen, T.; and Lonvick, C.: The Secure Shell (SSH) Protocol Architecture. Network Working Group RFC 4251, 2006. http://www.rfc-editor.org/rfc/rfc4251.txt
49. Stallings, William: Security Comes to SNMP: The new SNMPv3 Proposed Internet Standards. Internet Protocol J., vol. 1, no. 3, 1998.
50. Pierce-Mayer, Jeremy; and Peinado, Osvaldo: DTN Network Management. AIAA 2016–2367, 2016. http://arc.aiaa.org/doi/pdf/10.2514/6.2016-2367 Accessed Sept. 12, 2016.
51. Redi, Jason; and Ramanathan, Ram: The DARPA WNaN Network Architecture. Presented at the 2011 Military Communications Conference, IEEE, Baltimore, MD, 2011, pp. 2258–2263.
52. Information-Centric Networking Research Group (ICNRG). 2012. https://irtf.org/icnrg
53. Kassner, M.: Former NSA and CIA Director Recommends Managing Consequences Instead of Vulnerabilities. TechRepublic, 2016. http://www.techrepublic.com/article/former-nsa-and-cia-director-recommends-managing-consequences-instead-of-vulnerabilities/?ftag=TREa988f1c&bhid=21777107375198934460470472496894 Accessed Sept. 12, 2016.
54. Clarke, Russell; Dorwin, David; and Nash, Rob: Is Open Source Software More Secure? Project Report, University of Washington, Seattle, WA, 1999. https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/oss(10).pdf Accessed Sept. 12, 2016.
55. Cisco Systems, Inc.: Cisco Federal—DOD Architecture Solution. 2005. http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/Department_of_Defense.pdf Accessed Sept. 12, 2016.
56. Howard, L.: IPv4 Declared Historic. Network Working Group Internet-Draft, 2016. https://tools.ietf.org/html/draft-howard-sunset4-v4historic-00 Accessed Sept. 15, 2016.
57. Deering, S., et al.: IPv6 Scoped Address Architecture. Network Working Group RFC 4007, 2005. http://www.rfc-editor.org/rfc/rfc4007.txt Accessed Sept. 15, 2016.

Appendix A.—Acronym List

AOS	Advanced Orbiting Systems
BGPSEC	Boarder Gateway Protocol Security
CA	Certificate Authority
CCSDS	Consultative Committee for Space Data Systems
CE	Complex Electronics
COTS	Commercial Off-the-Shelf
CRL	Certificate Revocation List
CYB	Cover Your Butt
DAR	Data at Rest
DARPA	Defense Advanced Research Projects Agency
DHT	Distributed Hash Table
DIF	Distributed IPC Facility
DNS	Domain Name System
DNSSEC	DNS Security
DOS	Denial of Service
DTN	Delay/Disruption/Disconnection Tolerant Networking
ESA	European Space Agency
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
HIP	Host Identity Protocol
HIPAA	Health Insurance Portability and Accountability Act
HMMWV	High Mobility Multipurpose Wheeled Vehicle
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICN	Information-Centric Networking
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange Version 2
IP	Internet Protocol
IPC	Interprocess Communication

IPsec	IP Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IRC	Internet Relay Chat
ITU	International Telegraph Union
ITU–T	International Telegraph Union—Telecommunication Standardization Sector
LAPD	Los Angeles Police Department
LISP	Locator/Identifier Separation Protocol
MAC	Message Authentication Code
MOBIKE	IKEv2 Mobility and Multihoming Protocol
MP–TCP	Multipath TCP
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
NSA	National Security Agency
OS	Operating System
OpsCon	Operations Concept
PAD	Peer Association Database
PKI	Public Key Infrastructure
QoS	Quality-of-Service
RINA	Recursive Inter-Networking Architecture
RIR	Regional Internet Registry
RFC	Request for Comment
ROI	Return on Investment
RTT	Round Trip Time
SA	Security Association
SAD	Security Association Database
SCF	Store, Carry and Forward
SCP	Secure Copy
SDLSP	Space Data Link Security Protocol
SDN	Software-Defined Networking
SeND	Secure Node Discovery
SFTP	SSH File Transfer Protocol

SIDR	Secure Inter-Domain Routing
SNMP	Simple Network Management Protocol
SPD	Security Policy Database
SSH	Secure Shell
SSL	Secure Socket Layer
TC	Telecommand
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TM	Telemetry
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WNaN	Wireless Network after Next