Security Standards for the Global Information Grid

Gary Buda, Booz Allen & Hamilton, Linthicum, MD 21090
Don Choi, Defense Information Systems Agency, Reston, VA 20191-4357
Richard F. Graveman, Telcordia Technologies, Morristown, NJ 07960
Chris Kubic, Department of Defense, Ft. Meade, MD, 20755-6000

ABSTRACT

This paper presents an overview of requirements and issues related to improving the infrastructure security of the Global Information Grid (GIG). The context for "hardening" this infrastructure is to develop commercial standards that encourage products to support the GIG. Candidate infrastructure services for such hardening include signaling, routing, management, naming, and service location. The commercial standards of interest for GIG include certain relevant technologies at different stages of maturity, such as, Asynchronous Transfer Mode (ATM), Multi-Protocol Label Switching (MPLS), and optical networking. This paper also describes the Department of Defense (DoD) activities aimed toward defining security requirements and standards for hardening of switches and routers that implement these same networking technologies.

INTRODUCTION

The GIG [1] is a globally interconnected end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel.

As part of the GIG, the DoD operates many systems that transmit information over commercial network infrastructures between enclaves. The network infrastructure contains components, such as routers and switches, which direct the flow of information through the infrastructures. Today, commercial carriers provide over 95% of all the transmission service for all GIG communications. Additionally, many networks used by Government agencies within the GIG have outsourced their network management services. On the other hand, commercial carriers view network security as a business issue. They will not simply add security features without financial or market incentive. For them, a business case must be made, and this begins with customers' demand for these services.

The DoD is designing and deploying an enterprise-wide Information Assurance (IA) architectural overlay to the GIG [2] that is consistent with the overall GIG Architecture and implements a defense-in-depth strategy. The goal is to establish and maintain a consistent and acceptable overall IA posture across the GIG. IA services must be deployed for all GIG information systems both classified and unclassified. All systems are interconnected, so a security risk assumed by one entity becomes a risk shared by all those who are a part of the system.

The fundamental defense-in-depth strategy is that layers of IA solutions are needed to establish an adequate IA posture. Defense-in-depth is also predicated on a sound IA framework based on technical standards, performance benchmarks, and accepted best practices in conjunction with the IT industry.

This paper focuses on the network infrastructure portion of the GIG. While the GIG is composed of various network technologies, this paper focuses on ATM, MPLS, and optical networks, which are the critical networking technologies for the GIG in the near to mid-term. Many organizations are playing a role in defining these technologies, but this paper concentrates on (1) the ATM Forum (ATMF), (2) the Internet Engineering Task Force (IETF), and (3) the Optical Internetworking Forum (OIF).

REQUIREMENTS FOR DEFENDING THE NETWORK INFRASTRUCTURE

The networks within the GIG are constructed from a variety of switching and routing technologies and transport systems. Although the networking technologies and protocol layers that make up the different parts of these communication systems do not have simple and sharp boundaries, we will decompose the traffic on these networks into three basic types: user, control, and management communications.

User traffic is simply the information that users and their applications are transmitting over the network. Several DoD-approved products currently provide security services for user traffic.

Control traffic is any information transferred between network components that is necessary for establishing user connections. Control traffic includes signaling, naming, addressing, and routing information. Address and naming integrity and proper mapping between naming and addressing by the network infrastructure are essential for user traffic to be directed to the intended destination and

only the intended destination. Signaling must be protected to ensure user connections are established with the proper parties and service parameters. Routing information must be protected to ensure that user information will be forwarded properly and that the path user information takes is not manipulated. Protection of control traffic is also important to hide information about network configurations, numbers of users and types of services used, network capacity and response times, and traffic flow. If control information is unavailable to unauthorized parties, traffic analysis is hindered.

The third type of network traffic, management traffic, is any information used to configure network components, monitor the status and performance of the network, inform the network infrastructure about faults in the network, undertake corrective actions, and handle auditing, accounting, billing, and security information. Management traffic may be carried by a variety of protocols including Simple Network Management Protocol (SNMP), Telecommunications Network Management (TNM), Hypertext Transfer Protocol (HTTP), rlogin and telnet command line interfaces, or other proprietary management protocols. Protecting network management traffic is essential to ensure that network components are not monitored or modified by unauthorized entities. If the management of a network component is compromised, that component can often be configured to perform whatever function an attacker wishes. Simply being able to view configuration information on a network component may give an attacker knowledge of network capacity and topology, addressing schemes, or other potentially sensitive information.

Carrying sensitive DoD traffic may change the IA requirements for commercial network infrastructures. This applies specifically to the types of control and management information listed above, the sensitivity of which requires special protection. For example, routing tables contain topology information, which needs to be updated frequently. Because this information is transmitted over commercial networks, its authenticity, integrity, completeness, and confidentiality need to be assured.

DoD ACTIVITIES IN SECUIRTY STANDARDS

A. ASYNCHRONOUS TRANSFER MODE (ATM)

The ATM Forum was founded in 1991 to accelerate the development of interoperable specifications for and deployment of ATM. By 1995, the lack of ATM security was perceived as a drawback in the marketplace, and the Technical Committee formed the Security Working Group shortly thereafter. DoD has participated since the WG's beginnings in 1996. The first major task of the WG, completed in 1998, was to develop a security specification [3], [4], [5] for protecting *any* Virtual Channel. Although this appears at first sight to provide only user data protection, it can be applied, for example, to protect a Virtual Path Connection that carries user, control, and management traffic between enclaves. The primary security services provided are authentication, authorization, confidentiality, integrity, and replay detection. Key management, security service negotiation, and cryptographic resynchronization support these primary services. The development of this specification took into account the following additional requirements deemed important for the protection of the GIG:

- *Scalability.* The security services must support dynamic connectivity across large networks. Security must be robust with respect to changes in topology or coalitions.
- *Compatibility and minimal impact.* Security must function correctly and impose minimal performance penalties in networks where some users do not require security and some equipment is not capable of providing security.
- *Separability and nesting of security services.* Services like integrity and confidentiality should be designed so they can be selected and applied individually, in combination, or repeatedly, if necessary, at the endpoints or intermediate points in the network. It should be possible to implement security in an end system, switch, or adjunct security module.
- *Negotiation and private algorithms.* To provide these security services, a selection of algorithms, modes, key lengths, and other parameters should be allowed, and a secure method should be provided to select among these and additional, user-defined choices.
- *Support for PVCs and SVCs.* Security should function, as far as practical, in the same way for both permanent and switched VCs. For SVCs, a method should be provided for setting up security across different signaling protocols (e.g., UNI 4.0, PNNI, and AINI) without any additional round trip delays [6], [7], [8].

The version 1.1 enhancement [9] was completed in 2000. Its main objective was to make the specification easier to use. It added many clarifications and corrected some deficiencies. It removed incompletely specified features, brought the cryptographic algorithms up to date with common practice, removed many potential ambiguities, added SDL protocol descriptions and informative material, and is accompanied by a Protocol Implementation Conformance Statement (PICS) [10].

After the completion of the *ATM Security Specification version 1.1* [9], the two most important areas to cover were

(1) signaling and routing and (2) network management. For signaling (UNI, PNNI, and AINI) and routing (PNNI), the main security requirements were as described above: authentication, integrity, replay detection, confidentiality, and key management. (For additional background on securing link state routing protocols, see [11], [12], and [13].) The *ATM Security Specification* defined a key management protocol called SME (Security Message Exchange), but many vendors were implementing Internet Key Exchange (IKE) [14] as part of IPSec [15]. There was much overlap in functionality between SME and IKE, and as usual, key management was the hardest part of cryptographic security. Therefore, the ATMF's new specifications for control plane security [16] and PNNI routing security [17] allow the use of SME or IKE. But both of these protocols use a common record format called CPS that resembles IPSec's ESP to provide traffic protection. The CPS format is slightly different from ESP, because no IP header is present. Because of the need to avoid breaking existing ATM implementations, a new protocol identifier has been chosen to allow IKE, SME, or CPS traffic to flow in the same ATM VC used for signaling or PNNI routing. For PNNI routing security, several alternatives are provided to allow switches to discover which security mechanisms they have in common.

Securing the management of an ATM network element (NE) is not as simple as defining a new ATM security protocol. In most cases, such network management operations do not use ATM protocols at all, but rather, they rely on other protocols. Therefore, the ATMF Security WG is writing a set of guidelines [18] for securely managing an ATM NE. Often, what is provided is a Web-based management system, a command line interface, or SNMP. Therefore, the ATMF's guidelines will enumerate requirements for secure management and then show how various option such as SSL and TLS [19], [20], [21], Kerberos [22], the UNIX Secure Shell [23], and SNMPv3 [24] satisfy these requirements.

B. INTERNET PROTOCOL (IP)

The IETF and other entities have defined or implemented security for many TCP/IP protocols at different layers. Among these are the following:

- Above the application layer, message or file protection systems like GZIP, S/MIME, and PGP.
- Several full application layer security protocols: Kerberos, GSS-API, and SSH, as well as isolated security mechanisms in many other protocols, e.g., OTP, SNMPv1, RSVP, and RADIUS. Systems like SOCKS for firewall traversal.
- Infrastructure security, including SNMPv3 for secure network management; PKIX for X.509-based public key infrastructure; a public key based protocol for securing DNS; and cryptographic integrity checks for most of the popular routing protocols (e.g., BGP4, OSPF, and RIP).

  These have had mixed success to date. SNMPv3 has not been widely deployed; it lacks key management and is inflexible about choice of algorithms. PKIX and DNSSEC have been deployed slower than many hoped. The protocols for routing security lack confidentiality, key management, and flexible choice of algorithms. This is typified by [25]:

  None of the OSPF authentication types provide confidentiality. Nor do they protect against traffic analysis. Key management is also not addressed by this memo.
- For protecting HTTP traffic, one extremely popular session layer protocol, SSLv3 specified and developed by Netscape, together with its predecessor SSLv2, a variation named PCT by Microsoft, and the IETF's version TLS.
- IPSec at the network layer, which is a complete security system. It biggest drawback is that TCP/IP stacks are typically implemented in an operating system, so operating system support is needed for deployment. Also, methods for communicating security policy between the application and network layers still need to be completed.
- PPTP and various LAN or WAN security systems like IEEE 802.10. Most of these (1) lack proper security features, (2) suffer from inability to operate end to end, and (3) have not been widely deployed. Several wireless variations have been criticized for their security defects.

C. Multi-Protocol Label Switch (MPLS)

MPLS is a packet forwarding technique to improve throughput, Quality Of Service (QOS) support, and traffic engineering of IP router-based networks. Instead of routing each IP packet based on the IP header information, Label Switching Routers (LSR) in the core network use switching based on pre-assigned labels. This reduces the amount of packet handling, which improves network performance and permits explicit routing of specific types of traffic, e.g., a "Priority IP" service to a specific route to insure performance.

MPLS standards are being developed mainly by the IETF MPLS Working Group. The MPLS Working Group has produced a number of RFCs on MPLS including MPLS

architecture [26] and Label Distribution Protocol (LDP) specification [27].

MPLS supports both LDP and Resource ReSerVation Protocol (RSVP) [28] for Label Switching Path (LSP) setup and tear down. Both the LDP and RSVP specifications use MACs constructed with the MD5 algorithm for hop by hop authentication and integrity of the signaling messages. This is a sound construction, but it falls short of what is needed. First of all, some applications require confidentiality of signaling messages to protect records of customer activity, reduce their vulnerability to traffic analysis, or hide information about their network configuration. So authentication, message integrity, replay detection, and confidentiality should all be available, as security services from which the user can select. Secondly, a strong security system should provide two-way authentication coupled with a key management system. Key management is certainly harder than simple message protection, and automated key management is required for meaningful scalability. The argument has been put forward that key management is complex, but ignoring it does not make it go away. Key management is inherently hierarchical. Long-term keys protect shorter-term keys. Protocols provide "firewalls" like forward secrecy that limit the effect of a single key compromise. Thirdly, a variety of cryptographic algorithms and key lengths needs to be supported to cover different applications, jurisdictions, categories of information, and network configurations. These should include popular methods as well as a means to specify private algorithms. The protocol should accommodate these choices by supporting secure negotiation of services and mechanisms. Finally, attention should be given to auxiliary capabilities like enforcing security policy, reporting errors, and updating session keys.

D. Optical Networking

There is no industry consensus on the definition of Optical Networking. In a narrow definition it means pure end to end optical connections. A broad definition includes Optical-Electric-Optical connections (OEO). This paper uses the broad definition of Optical Networking.

Optical Networking standards are being worked by a number of standard organizations; OIF, IETF, International Telecommunication Union (ITU Telecommunication Study Group 15), and ANSI Technical Subcommittee T1X1. The initial implementations of Optical Networking are expected to be based on an OIF specification called UNI 1.0. This specification uses LDP and RSVP for optical connection establishment and tear down. For this reason, it specifies the same MD5 algorithm for authentication and integrity services for signaling messages. Like the MPLS, it does not support signaling confidentiality services.

INTEROPERABILITY ASSURRANCES AND FEATURES

In January 1996, the United States, United Kingdom, Germany, France, Canada, and the Netherlands released a jointly developed evaluation standard for a multi-national marketplace. This standard is known as the "Common Criteria for Information Technology Security Evaluation" (CCITSE), usually referred to as the "Common Criteria" (CC).

Under the CC, each level of trust rating from the Trusted Computer System Evaluation Criteria (TCSEC) can be specified as a Protection Profile (PP). A PP contains a set of security requirements either from the CCITSE or stated explicitly, which should include an Evaluation Assurance Level (EAL). The PP permits the implementation independent expression of security requirements for a set of Targets of Evaluation (TOEs) that will comply fully with a set of security objectives. A PP is intended to be reusable and to define TOE requirements that are known to be useful and effective in meeting the identified objectives, both for functions and assurance. A PP also contains the rationale for security objectives and security requirements.

A PP could be developed by user communities, product developers, or other parties interested in defining such a common set of requirements. A PP gives consumers a means of referring to a specific set of security needs and facilitates future evaluation against those needs. Protection profiles can be used by consumers to find requirements for security features that match their own risk assessment or by developers to select security requirements that they wish to include in their products.

The CC also contain criteria to be used by evaluators when forming judgments about the conformance of TOEs to their security requirements. The CC describe the set of general actions the evaluator is to carry out and the security functions on which to perform these actions.

A protection profile [29] has been written that specifies requirements for ATM switches, IP switches, IP routers, and optical switches. The PP focuses on the protection of control and management information in the router or switch. The PP specifically excludes protection of user data traversing the network infrastructure. Whereas the network management system is an integral part to the operation of switches and routers, it is not considered part of the TOE in this PP.

The PP was designed to cover three distinct target

environments that may be used by the DoD: (1) routers or switches owned and managed by the same organization, (2) equipment owned by an organization but managed by a network provider or commercial organization, and (3) services purchased from a provider.

CONCLUSIONS

The approach to securing the GIG requires several steps. First, security standards must be developed that will meet the DoD's security requirements. A standards-based approach is preferred so that multi-vendor solutions are possible that allow interoperability across the GIG. As new networking protocols are developed, security features must be included. The preferred approach is to have security inherent in new networking protocols. Security should be a concern of protocol designers from the start. Unfortunately, most existing network protocols have not been developed this way and require security enhancements.

Second, once security standards have been completed, the CC must be used to specify security functionality and assurance requirements for products in the form of a PP. Third, vendor products that meet the requirements expressed in the PP must then be evaluated to provide assurance that they do in fact meet the security objectives stated in the PP.

The security solution must be complete. The DoD's security requirements differ from those of commercial organizations. If commercial security is provided by a protocol, it is typically integrity. The DoD requires confidentiality, strong authentication, replay protection, authorization, and sound key management in addition to integrity. The DoD's involvement in protocol development, as has been achieved in the ATMF, is critical to the incorporation of the required security services.

IT and networking vendors must be convinced to incorporate security standards and features into their products. This is usually a case of proving a cost benefit to the vendors. In the past, DoD was a significant market share for IT vendors. Today, the DoD is no longer the IT industry's main customer. DoD has to devise new ways of convincing IT vendors of the need for incorporation of required security features.

REFERENCES

1. DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001, *Global Information Grid*, March 31, 2000.
2. DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 6-8510, *Department of Defense Global Information Grid Information Assurance*, June 16, 2000
3. *ATM Security Specification version 1.0*, ATM Forum Technical Committee, February 1999.
4. Peyravian, M., and T. Tarman, "Asynchronous Transfer Mode Security," *IEEE Network*, May/June 1997, pp. 34–40.
5. Byrd, G., N. Hillery, and J. Symon, "Practical Experiences with ATM Encryption," *Proceedings of the 2001 NDSS Symposium*, February 2001, pp. 23–32.
6. *UNI Signaling 4.0 Security Addendum*, ATM Forum Technical Committee, May 1999.
7. *PNNI Version 1.0 Security Signaling Addendum*, ATM Forum, May 1999.
8. *ATM Inter-Network Interface (AINI) Specification*, ATM Forum Technical Committee, July 1999.
9. *ATM Forum Security Specification version 1.1* , ATM Forum Technical Committee, work in progress, 2001.
10. *PICS Proforma for Security Specification Version 1.1* , ATM Forum Technical Committee, work in progress, 2001.
11. Perlman, R., *Network Layer Protocols with Byzantine Robustness*, Ph.D. Dissertation, MIT LCS TR-429, 1988.
12. *Proceedings of the 1997 NDSS Symposium*, The Internet Society, February 1997.
13. De Capitani di Vimercati, S., P. Lincoln, L. Ricciulli, and P. Samarati, "PGRIP: PNNI Global Routing Infrastructure Protection," *Proceedings of the 1999 NDSS Symposium*, February 1999, pp. 135–149.
14. Harkins, D., and D. Carrel, *The Internet Key Exchange (IKE)* , RFC 2409, Internet Engineering Task Force, November 1998.
15. Kent, S., and R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 2401, Internet Engineering Task Force, November 1998.
16. *Control Plane Security*, ATM Forum Technical Committee, work in progress, 2001.
17. *Addendum to PNNI v1.0—Secure Routing*, ATM Forum Technical Committee, work in progress, 2001.
18. *Methods for Securely Managing ATM Network Elements—Implementation Agreement*, ATM Forum Technical Committee, work in progress, 2001.
19. Rescorla, E., *SSL and TLS* , Addison-Wesley, 2001.
20. Freier, A.O., P. Carlton, and P.C. Kocher, *The SSL Protocol Version 3.0* , November 1996.
21. Dierks, T., and C. Allen, *The TLS Protocol*, RFC 2246, Internet Engineering Task Force, January 1999.
22. Kohl, J., and C. Neuman, *The Kerberos Network Authentication Service (V5)*, RFC 1510, Internet Engineering Task Force, September 1993.
23. Ylönen, T., *SSH Protocol Architecture*, work in progress, Internet Engineering Task Force, 2001.
24. Case, J., R. Mundy, D. Partain, and B. Stewart, *Introduction to Version 3 of the Internet-standard Network Management Framework* , RFC 2570, Internet Engineering Task Force, April 1999.
25. Moy, J., *OPSF Version 2*, RFC 2178, Internet Engineering Task Force, April 1998.
26. Rosen, E., A. Viswanathan, R. Callon, *Multiprotocol Label Switching Architecture*, RFC 3031, Internet Engineering Task Force, January 2001.
27. Andersson, L., P. Doolan, N. Feldman, A. Fredette, B. Thomas, *LDP Specification, RFC*: 3036, Internet Engineering Task Force, January 2001
28. R. Braden, R., L. Zhang, S. Berson, S. Herzog, S. Jamin, *Resource ReSerVation Protocol*, Internet Engineering Task Force, September 1997.
29. *Switch and Router Protection Profile*, February 22, 2000, work in progress.