Security, Internet Connectivity and Aircraft Data Networks

N. Thanthry

M.S. Ali

R. Pendse

Security, Internet Connectivity and Aircraft Data Networks

N. Thanthry, M.S. Ali & R. Pendse
Wichita State University

ABSTRACT

Internet connectivity which was in experimental stages only a few years ago is a reality today. Current implementations allow passengers to access Internet for pleasure and in some cases secure VPN access is provided to corporate networks. Several researchers are looking at the possibility of the existence of a total of three networks: passenger network (PN); crew network (CRN); and the control network (CON). Researchers envision an architecture where these three networks will co-exist in an airplane. The available Internet connectivity can be utilized for transporting flight critical information like cockpit flight data recorder (CFDR) data, digital flight data recorder (DFDR) data, cockpit voice recorder (CVR) data, and controller pilot data link communication. In addition, the internet connectivity could also be used for other safety mechanisms like video surveillance and remote control of the flight. Security is one of the major concerns that affect the successful deployment of Aircraft Data Networks (ADN) and other safety features. Several studies have been carried out to secure the network using firewalls and intrusion detection system but so far no study has focused on securing the communication channel (between the aircraft and the ground station) and its impact on the ADN. The scope of this research is to determine the viability and need of a security mechanism. The research will also focus on the performance of different security architectures and determine their usability in the framework of an ADN.

INTRODUCTION

Due to the recent technological advancements, deployment of Aircraft data networks (ADN) is on the rise. Many commercial airliners like Lufthansa, Scandinavian Airlines, China Airlines, and Singapore Airlines have already deployed ADN in their selected long haul flights. It is expected that, in the next 20 years, there will be 100,000 flights enabled with ADN flying across the world. With this volume of deployment, ADN security raises one of the major concerns for the authorities as well as airliners.

As pointed out by the authors of [1], aircraft data networks faces two kinds of security threats: internal and external. Internal security threats are originated from the passenger network where a malicious user can gain access to the control network and cause service impairments and/or attempt to take control of the flight. On the other hand, the external security threat is caused due to the security vulnerabilities of the satellite links.

Aircrafts equipped with ADN use satellite links to connect to the ground station. The advantages of satellite links lie in their ability to cover a large geographic area, distance insensitivity, and immunity to terrestrial hazards. Satellites are useful in providing broadband connectivity to remote locations which are harder to reach through terrestrial infrastructure. While satellite communication is advantageous, it has some peculiar characteristics like high delay-bandwidth product, low signal-to-noise ratio, long feedback loop, transmission error, variable Round Trip Time (RTT), and intermittent connectivity. These characteristics affect the communication, especially internet protocol (IP) based communication passing via the satellite network. A number of researchers have worked on improving the IP based communication performance over satellite networks. One of the solutions proposed in this area suggests using performance enhancing proxies (PEP) [3, 4] at strategic locations.

Apart from performance degradation, the satellite networks are also prone to security attacks. Due to their broadcast nature, satellite networks are prone to security threats like eavesdropping and flooding [5 - 7]. Usage of IPSec is one of the many solutions proposed to secure satellite communication. The versatility of IPSec lies in the fact that, unlike the other schemes which operate at the transport or application layer, IPSec operates at the Network layer thereby making it very easy to apply this security solution to different applications and with different transport layer protocols. Other

security mechanisms suggested for satellite communication include Transport Layer Security (SSL/TLS), Secure Shell (SSH), and Pretty Good Privacy (PGP), etc. However, the choice of security protocol depends upon the data type and the capacity of the encrypting device. In this paper, the authors analyze the ADN traffic pattern and look at various security options available for each data type. The main focus of the authors will be on the security mechanisms like IPSec and SSL/TLS.

The remainder of this paper is organized as follows: in the section that follows, the authors present a brief overview of IPSec and SSL/TLS security mechanisms. In the section entitled *Aircraft Data Network Traffic Pattern*, the authors present a discussion on the typical traffic pattern of ADN. In the section entitled *Security Mechanisms and ADN*, the authors discuss the advantages of each security mechanism with respect to ADN. In the *Simulated Results* section, the authors compare the performance of the two contending security mechanisms through simulation results. In the final section, the authors present their conclusions and suggest some future work.

OVERVIEW OF SECURITY MECHANISMS

Security is one of the major issues faced by most of the network administrators. Many schemes have been developed to address the security concerns of end users. It has been noticed that an enhancement in the security oftentimes adversely affects the application quality as perceived by the end users. Hence it is important for the end users/network administrators to choose the security mechanism that best suits their requirements.

In the case of an ADN, there are various types of traffic flow between the ground station and the aircraft. While some of this information may correspond to the flight control, others may be originated by the passengers. Typically, IPSec-based security mechanisms are used to protect sensitive information traversing the network. However, in the recent past, security mechanisms based on Secure Socket Layer (SSL) are also gaining importance due to their versatility.

Overview of IPSec

IPSec-based encryption is one of the means of providing security to confidential information. The versatility of IPSec lies in the fact that, unlike the other schemes which operate at the transport or application layer, IPSec operates at the Network layer. This makes it very easy to apply IPSec-based security mechanisms to different applications and different transport layer protocols.

IPSec offers authentication along with data encryption. IPSec achieves data security using three distinct components, each handling different aspects of security. Authentication header (AH) [9] is responsible for data authentication. Encapsulating security protocol (ESP) [8] is responsible for maintaining the data confidentiality. ESP defines the encryption mechanism, data format, etc. to ensure data confidentiality. Generally IPSec uses encryption algorithms such as data encryption standard (DES). Key exchange protocols are another important part of IPSec. Key exchange protocols such as internet key exchange (IKE) [10] ensure that the end points exchange the encryption and decryption keys securely.

IPSec operates in two different modes based on the security requirement. When operating in the transport mode, IPSec encrypts only the payload part of the IP packet. In tunnel mode, IPSec encrypts the entire IP packet and appends the encrypted IP packet with a new IP header specifying the address of the tunnel end point. The tunnel mode of IPSec offers maximum data security.

In order to provide enhanced security, IPSec induces some additional information (overhead) into the IP packet. IPSec overhead consists of IPSec header (24 to 57 bytes), authentication header (24 bytes in transport mode, 44 bytes in tunnel mode) and/or ESP header (30 - 37 bytes in transport mode and 50 - 57 bytes in Tunnel mode). In addition to the packet overhead, the IPSec encryption process also delays the entire packet delivery process and this delay depends upon the complexity of the encryption algorithm used by the IPSec process.

Overview of SSL/TLS

Compared to IPSec-based security mechanism, SSL/TLS is a newer security protocol (in terms of site-to-site access) developed initially by Netscape for web browsers. Unlike IPSec, SSL/TLS uses a layered approach. The record layer operates above the transport layer and provides encryption and authentication services. SSL/TLS uses symmetric key algorithms to protect user data. The keys to these algorithms are established by the handshake method which is handled by the handshake protocol. The handshake protocol uses public-key algorithms to create a master key between the SSL/TLS client and the server. The master key is used to generate cipher keys, initialization vectors, and message authentication code (MAC) keys. In addition to handshake protocol, there are other protocols like Change Cipher Spec (CCS) protocol, Alert protocol, and application data protocol which operate at the same level as handshake protocol. CCS protocol monitors the successful completion of handshake, whereas Alert protocol is responsible for notifying the protocol failures. The application data protocol is responsible for handling data to/from the higher layers.

Similar to IPSec, SSL/TLS accommodates a variety of encryption (DES, RC4), hashing (MD5, SHA), and key management (RSA, DH) algorithms. However, the standard specifies the usage of a specific combination of these security algorithms called cipher-suites in order to get a specific security effect.

Whenever a client wants to connect to a server, he/she first sends a hello message to the server. In response, the server sends a server hello message. This exchange of hello messages sets parameters like version, session ID, encryption method, and compression technique. Once this part is done, both client and server authenticate each other after which they exchange the session key. It has been observed that, with a Pentium Xeon

processor, this entire handshake process takes approximately 173 ms [17]. After the handshake process is complete, the client and server are ready to exchange application data. In addition to the handshake delay, typically SSL/TLS adds at least 23 bytes (depends upon the block cipher used and block size). However, there is no clear definition of the number of bytes added per packet in the case of SSL/TLS.

AIRCRAFT DATA NETWORK TRAFFIC PATTERN

As mentioned earlier, in addition to transporting passenger traffic, the available Internet connection could also be used to transmit certain flight parameters from the aircraft to the ground station. Currently, every aircraft stores approximately 15 minutes of cockpit voice information in the CVR. Every 15 minutes, this information is overwritten with the new data. As discussed in [16], with the recent technological advances, it is possible to store the flight information for the entire flight duration within the aircraft. In addition, using the Internet connection, this information could be transferred to the ground station in real-time, enabling the ground station crew to monitor the flight health and caution the flight crew in case of an emergency.

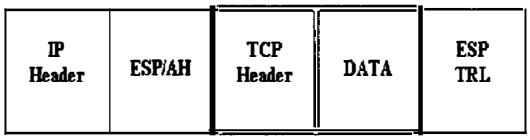

Fig. 1A. Encrypted IP datagram in transport mode

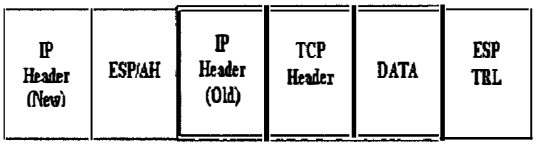

Fig. 1B. Encrypted IP datagram in tunnel mode

Fig. 1. Encrypted IP packet

In addition to the flight information stored in the black box, the available Internet connection could also be used to transmit video frames captured within the aircraft to the ground station in real-time in emergency situations. Passengers may use the available internet connection to browse through the internet for entertainment (streaming audio/video), or to connect to their corporate network. Depending upon the passenger volume, the amount of data generated from the passenger network varies. It has been noted that, DFDR stores approximately 122 Kbytes of data in 15 minutes, whereas digitization of cockpit voice communication requires approximately 136 kbps of bandwidth. If implemented, video traffic may require approximately 865 kbps of bandwidth. From the traffic profile, it can be observed that the data corresponding to DFDR and cockpit voice are sensitive information as compared to other traffic. Hence, they need to be protected against attack from external entities.

Previous research in this field has indicated that real-time transmission of these information segments from the aircraft to the ground station is not viable due to the high delay-bandwidth product of the satellite links. It was observed that almost all of the TCP-based data transmission applications suffered performance degradation due to the variable RTT and high delay of the satellite links. One of the possible solutions in this direction could be to use a streaming based data transmission between the aircraft and the ground station. In this scenario, the data collected from the CVR and DFDR are stored within the aircraft and at regular intervals, and downloaded to the ground station. In order to improve TCP performance, researchers have suggested using performance enhancement proxies (PEP) at strategic locations.

PEPs are generally located at the edge of the satellite networks. PEP agents act as proxy agents by sending proxy ACK messages for the data that passes through them. TCP PEP agents extract the TCP flow identification information and the sequence number from every TCP packet that passes through them. This data is used to form the proxy ACK message. Using PEP agents reduces the possibility of the source getting into slow start mode due to delayed acknowledgements.

In the next section, the authors discuss the effect of different security mechanisms on the performance of ADN traffic.

SECURITY MECHANISM AND ADN

In general, the perception is that the security mechanism deteriorates the application performance, which is partly true also. One of the main reasons for this is the complexity of the security mechanism itself. As the complexity of the security mechanism increases, the perceived security will also increase. On the other hand, with lower end systems, it affects the quality adversely.

In the case of ADN, the quality of aircraft traffic is affected by two factors: satellite link and security mechanism. The effect of the satellite links can be alleviated by using performance enhancement proxies (PEP). While PEP agents improve the TCP-based application performance, they do not work well in the presence of network layer encryption. When an end-to-end encryption mechanism like IPSec is used, the encryption scheme hides all the information including the transport layer header from the intermediate nodes. However, in order for PEP agents to work, they will need the transport layer information. This results in non-functioning of the PEP agents. Figure 1 shows the typical packet format of an encrypted IP datagram. As shown in the figure, the PEP agent could get just the IP header information but not the TCP header information.

The issue of IPSec and PEP coexistence was first identified by the authors of [15]. In their work, the authors explored many possible solutions to resolve the issue of security and performance enhancement working together. One of the possible solutions they proposed suggested that IPSec-based

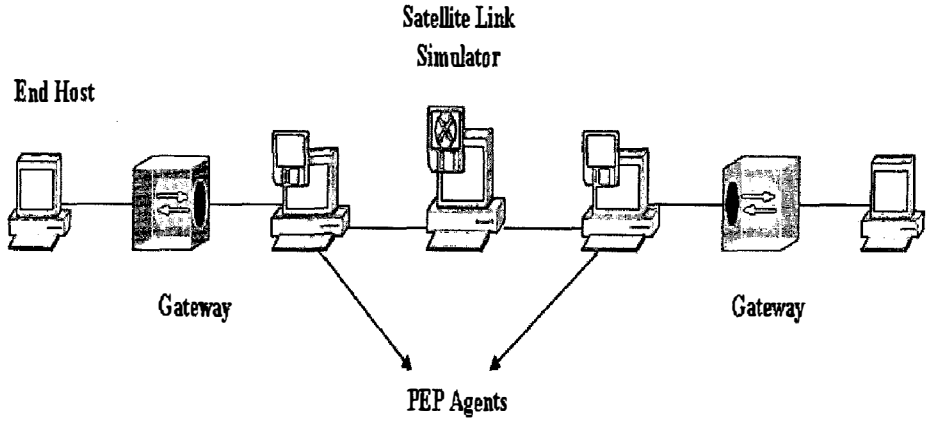

Fig. 2. Simulation test-bed

encryption should be used selectively. They suggested that the traffic streams that need performance enhancement should not be encrypted. The major drawback of this approach is that it compromises the security of user traffic for better performance. In another suggestion, the same authors suggested establishing multiple IPSec associations. In their proposed approach, the authors suggested that the PEP agents should be used as IPSec end points. The end systems need to establish security association with the PEP agents. PEP agents will have certain IPSec-based security association between themselves, and they will transport user data across the satellite network after applying encryption. This method requires a distributed PEP implementation, and it also requires the end systems to know the presence of PEP agents. The major drawback of this approach is its complexity. This approach involves multiple encryption/decryption processes which increase the delay and reduce the throughput.

Another approach suggested by these authors was to use other encryption techniques like SSL/TLS instead of IPSec. SSL/TLS-based encryption provides almost the same level of security as IPSec but operates at the transport layer instead of the network layer. As discussed earlier, SSL/TLS supports almost all encryption standards similar to IPSec. However, since it is encrypting at the transport layer level, it will leave the transport layer information unencrypted thereby opening up the network for attack. On the other hand, it does not hinder the operations of the PEP agents, thereby improving the quality of the data transfer applications. Hence from application performance perspective, SSL/TLS is a better option compared to IPSec.

In the next section, the authors present some simulation results to support their argument of choosing SSL/TLS-based security mechanism for ADN.

SIMULATION RESULTS

In order to verify the advantages of SSL/TLS-based security mechanism over IPSec, the authors built a small test-bed as shown in Figure 2. The authors used a satellite link simulator (by Spirent Communications) to emulate the satellite link characteristics in the network. In addition, the authors also used performance enhancement proxies availed from SCPS.org. All the systems used in the test-bed were of the same configuration (PIII, 800 MHz, 256 MB RAM). The authors compared the throughput performance (using netperf) of the network under various conditions i.e. in a normal scenario, with satellite link simulator active and in the presence of performance enhancement proxies. Table 1 presents the results obtained under different test conditions.

Table 1. Throughput measured using netperf (Mbps)

	Without PEP	With PEP
Normal Scenario	**6.7**	—
Normal Scenario with Satellite Link Impairments	**0.61**	**1.77**
IPSec-based Encryption	**0.5925**	**0**
SSL/TLS-based Encryption	**0.5975**	**1.76**

From the results, it can be observed that the throughput of the network was almost similar for both IPSec and SSL/TLS-based security mechanisms. However, in the presence of PEP, only SSL/TLS-based security mechanisms were able to deliver the data across the network while packets encrypted using IPSec were dropped at the PEP gateways. This

clearly indicates that SSL/TLS-based security mechanisms are better in the presence of satellite links and performance enhancement proxies.

CONCLUSIONS AND FUTURE WORK

In this research work, the authors focused on determining the security mechanism best suited for aircraft data networks. They compared the working of IPSec- and SSL/TLS-based security mechanisms. While IPSec provides better security, it fails to maintain the quality of service required by the TCP-based applications. On the other hand, SSL/TLS-based security mechanisms provide security almost equivalent to IPSec without affecting the quality to a larger extent. Hence, in the current conditions, the authors suggest using SSL/TLS-based security mechanisms for aircraft data networks.

One of the main drawbacks sited in the case of IPSec was its inability to provide transport layer information to the PEP agents. As a future work, the authors suggest making modifications to the existing IPSec key exchange protocol such that IPSec works along with PEP agents to improve the application performance in satellite link environments.

REFERENCES

[1] N. Thanthry and R. Pendse,
Aviation Data Networks - Security Issues and Network Architecture,
In the Proceedings of 38th International Carnahan Conference On Security Technology,
Albuquerque, New Mexico, October 2004.

[2] C. Partridge and T. Shepard,
TCP Performance over Satellite Links,
IEEE Network, Vol. 11, No. 5, pp. 44-49, September 1997.

[3] J. Border, M. Kojo, J. Griner and G. Montenegro,
Performance Enhancing Proxies,
Internet Draft, December 1999.

[4] J. Grinner,
TCP Performance Enhancing Proxy Terminology,
Internet Draft, November 1998. http://tcppep.lerc.nasa.gov.

[5] Y. Zhang, D. DeLucia, B. Ryu, and S. Dao,
Satellite Communications in the Global Internet: Issues,
Pitfalls, and Potentials,
In the Proceedings of INET'97, June 1997.

[6] M. Medawar,
Satellite Security: The Weakest Link?,
White Paper, GSEC Practical Assignment,
Version: 1.4b, SANS Institute, 2003.

[7] Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed,
Highlights of GAO-02-781, a report to the Ranking Minority Member, Permanent Subcommittee on Investigations, Committee on Governmental Affairs,
United States Senate, August 2002.

[8] S. Kent and R. Atkinson,
IP Encapsulating Security Payload (ESP),
RFC 2406, November 1998, www.faqs.org/rfcs/rfc2406.html.

[9] S. Kent and R. Atkinson,
Authentication Header,
RFC 2402, November 1998, www.faqs.org/rfcs/rfc2402.html.

[10] D. Harkins and D. Carrel,
The Internet Key Exchange (IKE),
RFC 2409, November 1998, www.faqs.org/rfcs/rfc2409.html.

[11] E. Rescorla,
SSL and TLS: Designing and Building Secure Systems,
Addison-Wesley, 2001.

[12] T.R. Henderson and R.H.Katz,
Transport protocols for Internet-compatible satellite networks,
IEEE Journal on Selected Areas of Communication,
Vol. 17, pp.326-344, February 1999.

[13] J. Border, M. Kojo, J. Griner, G. Montenegro, and Z. Shelby,
Performance enhancing proxies intended to mitigate link-related degradations,
RFC 3135, June 2001, www.ietf.org/rfc/rfc3135.txt.

[14] S. Kent and R. Atkinson,
Security architecture for the Internet protocol,
RFC 2401, November 1998,
http://www.faqs.org/rfcs/rfc2401.html.

[15] Y. Zhang,
A Multi-Layer IP Security Protocol for TCP Performance Enhancement in Wireless Networks,
IEEE Journal on Selected Areas in Communications,
22(4):767-776, May 2004.

[16] V. Ragothaman, N. Thanthry, R. Bhagavathula and R. Pendse,
IP Connectivity and DAP,
In the Proceedings of 23rd Digital Avionics System Conference, Salt Lake City, Utah, October 2004.

[17] V. Beltran, J. Guitart, D. Carrera, J. Torres, E. Ayguad and J. Labarta,
Performance Impact of Using SSL on Dynamic Web Applications,
In XV Jornadas de Paralelismo, pp. 471-476.
Almeria, Spain, (September 2004).