Security Issues in Airplane Data Networks

M.S. Ali, V. Ragothaman, R. Bhagavathula, and R. Pendse

Department of Electrical and Computer Engineering, College of Engineering

1. Introduction

The presence of network connectivity between the airplane and its ground stations presents numerous challenges in terms of security provisioning. Unlike terrestrial networks, the network connecting an airplane with its ground stations cannot sustain outages as this would result in not only considerable loss of revenue, but also result in loss of precious human lives. Therefore, the security provisioning within the IP network connecting the airplane with its ground stations needs to be carried out to ensure minimal, if any, network outages due to malicious network activity, both within and without an airplane. The authors summarize the security issues related to airplane data networks and propose an in-house network monitoring tool tuned towards airplane data networks that provides real-time warning of impending network threats to allow the network administrators to carry out appropriate responses to intrusions.

2. Security

The major component of an Aeronautical Telecommunication Network (ATN) is Mobile IP [1] which provides seamless access to network resources irrespective of the location of the communicating node. Mobile IP was introduced as an extension to IP; however, it does not inherently support any security mechanisms to ensure a secure means of communication between the mobile node and its corresponding home network. Recently, many additions have been made to Mobile IP to improve its security feature-set.

One of these features is IPSec which can be optionally employed between the HA and the FA to provide a secure means of communication [2]. However, tests carried out at the Advanced Networking Research Center (ANRC) at WSU show that IPSec operations become a performance bottleneck in the absence of appropriate hardware support. It was observed that with increasing number of packets to be processed by the IPSec processes, the CPU utilization increases up to 99% with packets getting dropped in the process due to inability of the router to handle the encryption/decryption of the incoming traffic beyond a specific limit. Furthermore, the contribution of the cryptography processes to the total CPU utilization statistics is also dependent upon data rates.

With the introduction of a network connection between the airplane and the ground stations, the airplane is assumed to cater to three distinct types of networks: Passenger Networks (PN) Crew Networks (CrN), and Control Networks (CoN). In order to facilitate an efficient monitoring of network activity within the PN, the CrN and the CoN, the authors recommend the application of Intrusion Detection Systems (IDSs) concepts to formulate an intelligent mechanism that would provide real-time warning of impending network threats to allow the network administrators to carry out appropriate responses to intrusions. The IDS sensors would be located within the individual networks (PN, CrN and CoN) for monitoring. In addition, another sensor would be located within the aircraft access network to ascertain if malicious traffic is introduced into the CrN and/or the CoN. Due to the lack of appropriate network traces that reflect typical airplane Internet access patterns, the researchers have employed standard terrestrial network traces to ascertain the behavior of “normal” traffic streams. The details of the considered IDS mechanism are presented next.

3. Anomaly Detection Engine

While conventional IDSs are based upon the availability of “signatures” to ascertain malicious traffic, there usually exists a time lag between the identification of a security breach, the development of a “signature” and the application of the signature to detect malicious activity. While this is permissible for a terrestrial network a networked airplane cannot afford to have the link connecting the ground station with the airplane to be compromised for even a minuscule amount of time. To this effect, the authors considered the usage of an anomaly detection based framework to supplement the existing signature based IDSs.

To introduce anomaly detection into the framework of an IDS, the authors employed snort with a pre-processor plug-in called Statistical Anomaly Detection Engine (SPADE) [3]. Every packet that SPADE monitors is assigned an anomaly score. The anomaly score that is assigned is based on the observed history of the network. The fewer times that a particular kind of packet has occurred in the past, the higher its anomaly score will be. Packets are classified by their joint occurrence of packet field values. For example, packets with specific destination IP addresses and specific source/destination ports would be assigned specific (and usually) different anomaly scores.

SPADE maintains a probability table that reflects the occurrences of different kinds of packets in history, with higher weight for more recent events. SPADE calculates a raw anomaly score directly from the probability of anomaly. For a packet X, the raw anomaly score is calculated using the formula,

$A(X) = -\log2(P(X))$

where, P(X) is the probability of an anomaly that is computed by SPADE by consulting the probability table. The higher the raw anomaly score, the greater is the perceived anomaly associated with that packet. SPADE also yields a relative anomaly score which lets the network administrator compare the relative anomaly associated with a packet with respect to the other packets within the time frame that SPADE has been active.

The anomaly detection engines will supplement the signature based IDSs that would be located in the same locations as the anomaly detection engines. The signature based IDSs would generate alerts based on signatures of known security breaches. The anomaly detection engine would alert the network administrator of any network anomaly within the CrN, the CoN and the PN. This would enable the network administrator to determine an impending network threat and take appropriate action.

A few scripts were created (in perl) to parse through the log-files created by SPADE, and to access the MySQL database where SPADE and snort write their respective alerts. SPADE has the ability to report malicious packets with a raw anomaly score that is above a specific threshold in an effort to reduce the number of false-positives. Every time SPADE detects a packet whose anomaly score exceeds the specified threshold value, it is recorded in the log-file and in the MySQL database. SPADE was configured to track the anomaly scores and dynamically adjust the more optimum threshold so as to reduce the number of false-positives visible in the alerts.

4. Conclusions

A survey of the various security issues related to the deployment of a networked airplane essentially points out to the similarities that exist between traditional terrestrial networks and in-flight-networks. However, careful consideration is warranted for provisioning the satellite links and the security of the networks within an airplane to ensure minimal disruptions in the network connectivity between the airplane and the ground stations. Security issues related to the airplanes are further exacerbated by the fact that disruption in network connectivity between the airplane and the ground stations could be a pre-cursor to a larger security concern and the number of such incidents needs to be minimized. The usage of IPSec is regarded to be more appropriate within the framework of a networked airplane. However, simulation results reveal the CPU intensiveness of the various encryption and decryption processes within IPSec leading to issues related to its scalability.

With the usage of an anomaly detection engine within the framework of a networked airplane is expected to yield a better defense against impending network attacks from within and outside the airplane. The anomaly detection engine considered for the current work is based on a statistical estimation of anomaly and is integrated into snort, a freely available IDS.

5. Acknowledgements

This work was supported in part by Cessna Aircraft Inc., the State of Kansas, the National Institute of Aviation Research (NIAR) and Cisco Systems. Many thanks are due to the engineers at these organizations for providing valuable insights into the interaction of aviation related components with networking elements.

6. References

[1] C.Perkins, “Mobile Networking Through Mobile IP”, IEEE Internet Computing, January 1998.

[2] John K. Zao and Matt Condell, “Use of IPSec in Mobile IP”, RFC 2119, November 1997.

[3] Statistical Packet Anomaly Detection Engine (SPADE). http://www.silicondefense.com/spice. No longer supported at this web-site. Integrated SNORT available from http://www.ossim.net