International Civil Aviation Organization

THE FIFTH MEETING OF AERONAUTICAL TELECOMMUNICATION NETWORK (ATN) IMPLEMENTATION CO-ORDINATION GROUP OF APANPIRG (ATNICG/5)

Kuala Lumpur, Malaysia, 31 May – 4 June 2010

Agenda Item 12: **Asia/Pacific Security:**
- **Review AMC Security**
- **Discuss Implementation Document: Security Checklist**

ASIA/PAC AERONAUTICAL TELECOMMUNICATION NETWORK SECURITY GUIDANCE DOCUMENT

(Prepared and presented by FAA/USA)

SUMMARY

This paper identifies some considerations which have been raised with regard to IPv6 security. This paper also provides the IPv6 security consideration and its advantages of IPv6 since IPsec is "built-in" rather than an "add-on" feature. There are other considerations which relate to the overall security infrastructure.

1. Introduction

IPv6 security is considered to be one of the advantages of IPv6 since IPsec is "built-in" rather than an "add-on" feature. Furthermore IPsec is mandatory for IPv6; it is optional for IPv4. However, having IPsec protocol built-in is not the only security consideration in deployment of IPv6. There are other considerations which relate to the overall security infrastructure. This paper identifies some considerations which have been raised with regard to IPv6 security.

2. NIST SP 500-267

In 2008, the U.S. Government published National Institure and Standards and Technology (NIST) Special Publication (SP) 500-267, "A Profile for IPv6 in the U.S. Government, Version 1.0.[NIST 500-267]" With regard to security this document notes the following:

> "The current state of IPv6 security and network protection technologies and operational knowledge lags behind that of IPv4 and the existing Internet. Additional efforts are required to "raise the bar" in these areas to ensure the safety of IPv6 deployments in operational Federal information technology systems."

In an attempt to address this issue NIST 500-267 contains a specification for IPv6-enabled Network Protection Devices (NPD). NPDs are Firewalls or Intrustion Detection/Protection devices that examine and selectively block or modify network traffic.

In addition to the NDP considerations, the following general security issues are associated with IPv6 [NIST IPv6 Guidance]:

1. Transition Complexity
2. New Protocols
    a. Lack of operational experience,
    b. Interactions
3. Address scanning no longer pratical
4. Address autoconfiguration vs. privacy addresses
5. IPsec complexity, interoperability, applicability, interaction with other protocols

3. ICANN SAC 021

In order to address the NDP issue in an authorative manner, the ICANN Security and Stability Adivsory Committee conducted a Survey of IPv6 Support in Commercial Firewalls [ICANN SAC 021]. The survey concluded that support for IPv6 transport and security services is available from commerical firewalls for all market segments, however, availability of advanced security features is lagging in the small, home office and small/medium business segments and strongest in the large enterprise, service provider segment. The survey could not definitively answer the question, “Can an organization that uses IPv6 transport enforce a security policy at a firewall that is commensurate to a policy currently supported when IPv4 transport is used?” The survey results do suggest that an organization that adopts IPv6 today may not be able to duplicagte IPv4 security feature and policy support.

4. RFC 4942

IPv6 Transition/Co-existence Security Considerations [RFC 4942] gives an overview of security issues associated with IPv6. The issues are grouped into three general categories: issues due to the IPv6 protocol itself; issues due to transition mechanisms; and issues due to IPv6 deployment.

5. Summary

Although IPv6 has built-in security features, lack of operational experience and on-going development of Network Protection Devices remains a security consideration in IPv6 implementation. However, as noted in this paper these are recognized issues that are being addressed by several organizations. Therefore while the issues may persist in the short term in the longer term it can be expected that these issues will be sufficiently addressed as experience and implementation of IPv6 grows.

6. Recommendation

It is recommended that these issues be monitored to ensure that they are addressed when Asia/Pac eventually transitions to IPv6.

7. References

[NIST 500-267] National Institure and Standards and Technology (NIST) Special Publication (SP) 500-267, “A Profile for IPv6 in the U.S. Government, Version 1.0.
http://www.antd.nist.gov/usgv6/usgv6-v1.pdf

[NIST IPv6 Guidance] NIST’s Guidance on IPv6
http://csrc.nist.gov/groups/SMA/ispab/documents/ minutes/2005-12/S_Frankel-Dec2006-ISPAB.pdf

[ICANN SAC 021] ICANN Security and Stability Adivsory Committee
Survey of IPv6 Support in Commercial Firewalls
http://www.icann.org/en/committees/security/ sac021.pdf

[RFC 4942] IPv6 Transition/Co-existence Security Considerations
http://tools.ietf.org/html/rfc4942

– – – – – – – – – – –