Federal Aviation Administration

AMHS Security

Task Status

ATS Message Handling System (AMHS) Implementation Workshop
Bangkok, Thailand

January, 27th – 28th 2010

Vic Patel

FAA/ATO-P Information Security Team

William J. Hughes FAA Technical Center
Atlantic City International Airport
Atlantic City, NJ 08405
USA

Asia/Pacific ICG Strategic Objective: Security

- **Task (1) Develop ATN System Security Policy**
  - ✓Asia/Pacific ATN System Security Policy Document
  - ✓ Adopted by ICAO Asia-Pacific as of October 2008
- **Task (2) Develop ATN System Security Checklist**
  - ✓Asia/Pacific ATN Develop Security Checklist
  - ✓ Adopted by ICAO Asia-Pacific as of September 2009
- **Task (3) Co-ordinate and monitor ACP working group and other regions**
  - No significant changes
- **Task (4) Develop ATN System Security Guidance**
  - Asia/Pacific ATN System Security Guidance
    - A security guidance document would provide background information and recommended practices primarily to support the Security Implementation
    - Addresses Technical controls and checklist in detail
    - Appendix for Regional Incident Response Plan and Contingency Plan

Security Policy

- The Asia/Pacific region has developed a ATN System Security Policy*

1. The policy requires that ATN systems be verified to have appropriate security controls.

2. The policy requires that ATN systems be formally approved for operation a Designated Approval Authority for each state/organization.

*Ref: document “518Integrity_Policy” on ICAO Asia/Pac Web site

Security Policy

- Security Policy Outline:
  - Purpose.
  - Applicability.
  - Authority.
  - Implementation and Enforcement.
  - System Integrity Requirements.
  - System Integrity Services
    - Confidentiality
    - Data Integrity
    - Authenticity.
    - Availability.
    - Accountability.
    - Interoperability.
  - System Integrity Policy Statements
    - Functional Policy Statements
  - Verification and Authorization

Security Checklist

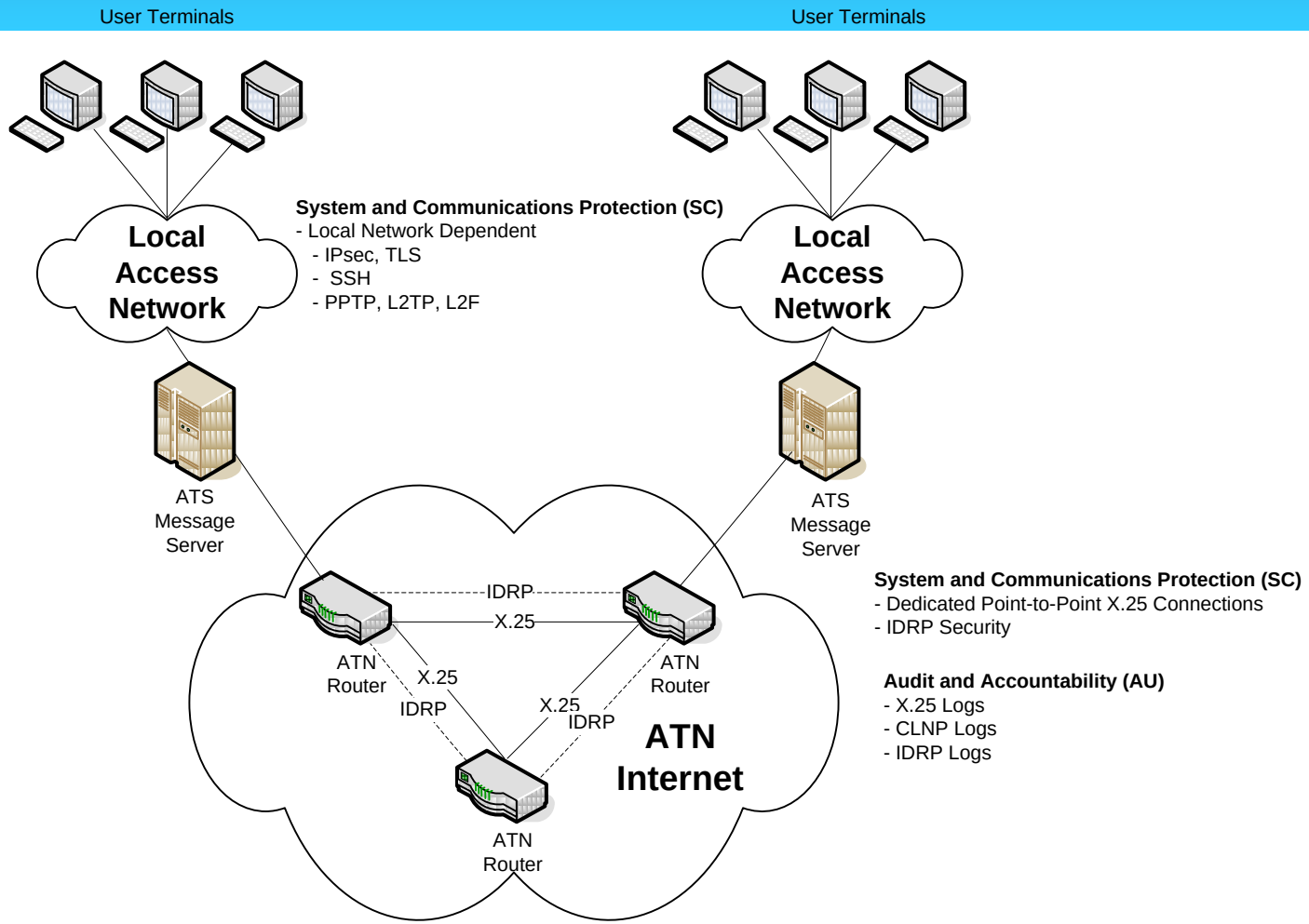
- A checklist serves to see that controls are in place
- It is generally the basis on which the Approving Authority grants approval
- There are comprehensive checklist that have been defined by the National Institute of Standards and Technology:
  - NIST SP 800-18, Security Self-Assessment Guide for Information Technology Systems, November 2001
  - NIST SP 800-53, Recommended Security Controls for Federal Information Systems, December 2006
- These documents are comprehensive and may be too complex for practical use

- The ISO standard for Security equivalent to NIST SP-800-53 is ISO 17799 "The Information Security Standard". 800-53 has a cross reference matrix to 17799 in Appendix G.

AMHS Technical Controls

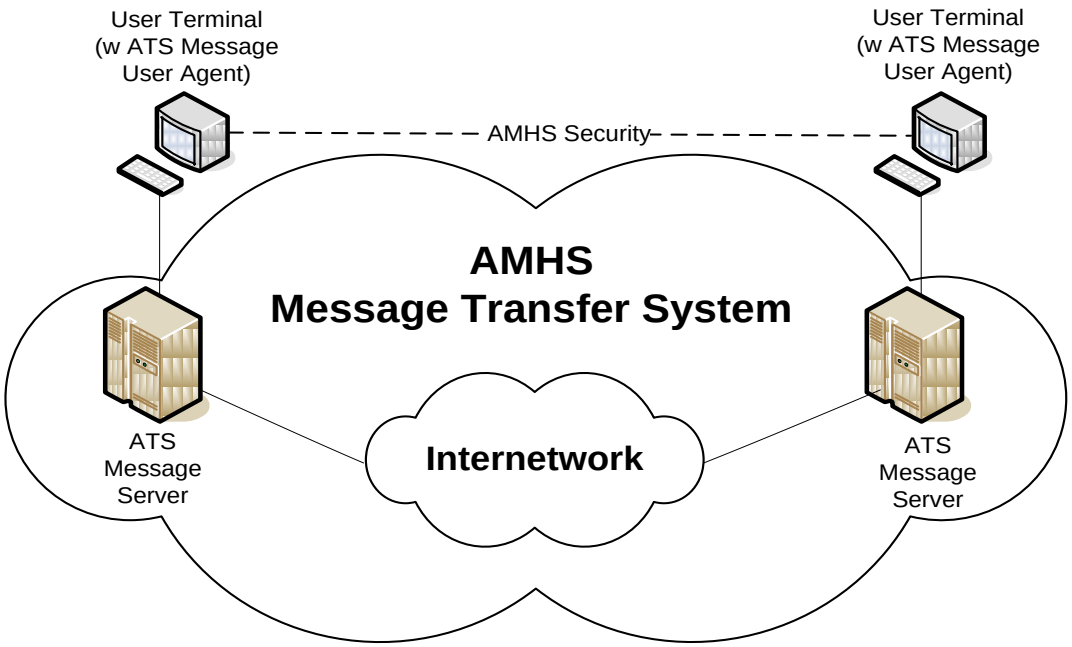
- Network Security Provisions
  - From User Terminal to Message Server or Between Message Servers (Routers)
- End-to-End Security Provisions
  - Defined in ICAO Doc 9705 Edition 3 using the ATN Digital Signature Scheme
    - May not be implemented if region does not move to ATN air-ground security provisions

AMHS Technical Controls



AMHS Technical Controls

System and Communications Protection (SC)
- AMHS Security applied from
  ATS Message User Agent to ATS Message User Agent



Network Security

Secure Communications from User Agents to MTA Server

- Technique depends on connectivity
  - Internet Protocol Security (IPsec)
  - Transport Layer Security (TLS) (formerly Secure Sockets Layer (SSL))
  - Layer 2 Protocols (Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F)
  - Secure Shell (SSH)

Network Security

Secure Communications between Routers which support MTA Servers

- Communications Security
  - IDRP Security
    - Initially pre-shared keys
    - Longer term - PKI
- Audit Logs
  - TCP, IP, BGP Logs

Security Implementation

What security controls when

- Technical controls may initially consist of securing router connections
  - Initially using pre-shared keys
  - Migrate to limited use of certificates
- As the AMHS evolves to enhanced services, including directory services, AMHS application security may be employed
  - Not expected for some time (if ever)
  - More likely next step to secure User Agent to MTA Server communications
- Firewalls and other security appliances should be introduced as needed.
- An incident response capability should be introduced along with the technical controls

Other Regional Security Documents

- System-wide Contingency Plan

  A system-wide contingency and disaster recovery plan would identify the coordination activities, processes, and procedures to be followed in the event that an AMHS system is unavailable.

Other Regional Security Documents

- NIST SP800-34, Contingency Planning Guide for Information Technology Systems, June 2002

  "IT contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. Contingency planning generally includes one or more of the approaches to restore disrupted IT services:

  - Restoring IT operations at an alternate location
  - Recovering IT operations using alternate equipment
  - Performing some or al of the affected business processes using non-IT (manual) means"

Other Regional Security Documents

- System-wide Incident Response Plan

  The incident response plan would specify common procedures for identifying, reporting, and responding to computing incidents.

Next Steps

- States should identify a Designated Approving Authority (DAA) in accordance with the approved Asia/Pacific Security Policy

- States are encouraged to develop their own or use the approved Asia/Pacific Security Checklist

- States may adopt the technical controls recommended in Asia/Pacific Security Guidance document

Questions