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

Draft Second Edition

June 2010

INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA AND PACIFIC OFFICE

ASIA/PAC
AERONAUTICAL TELECOMMUNICATION NETWORK
SECURITY GUIDANCE DOCUMENT

DRAFT

Second Edition

June 2010

TABLE OF CONTENTS

1. INTRODUCTION

This Security Guidance Document for the Asia/Pacific Region provides guidance on the implementation of security for states and organizations operating in the region.

1.1 Background

As noted in the Asia/Pacific System Security Policy [Asia/Pac SSP], the fundamental objectives for system security of the ATN are to:

1. Protect ATN data from unauthorized disclosure, modification, or deletion, and
2. Protect ATN resources from unauthorized use and denial of service.

These objectives are achieved through the application of a set of high-level security services. The Asia/Pacific Security Policy identifies the following services:

(1) Confidentiality. Ensures data is not disclosed to unauthorized entities.

(2) Data Integrity. Ensures data has not been altered or destroyed in an unauthorized manner.

(3) Authenticity. Ensures that the source of data or the identity of an entity is as claimed.

(4) Availability. Ensures resources, services, and data are accessible and usable on demand or in a timely, reliable manner by an authorized entity.

(5) Accountability. Enables activities to be traced to users and processes that may then be held responsible for those actions.

These security services are in turn realized by the implementation of a comprehensive set of management, operational, and technical controls. Controls may be organized into the following control classes:

Management controls are safeguards or countermeasures that focus on the management of risk and the management of system security.

Operational controls are safeguards or countermeasures for a system that are primarily implemented and executed by people.

Technical controls are safeguards or countermeasures for a system that are primarily implemented and executed by the system through mechanisms contained in the components of the system.

Figure 1.1 depicts the relationship between Security Objectives, Services, and Controls.

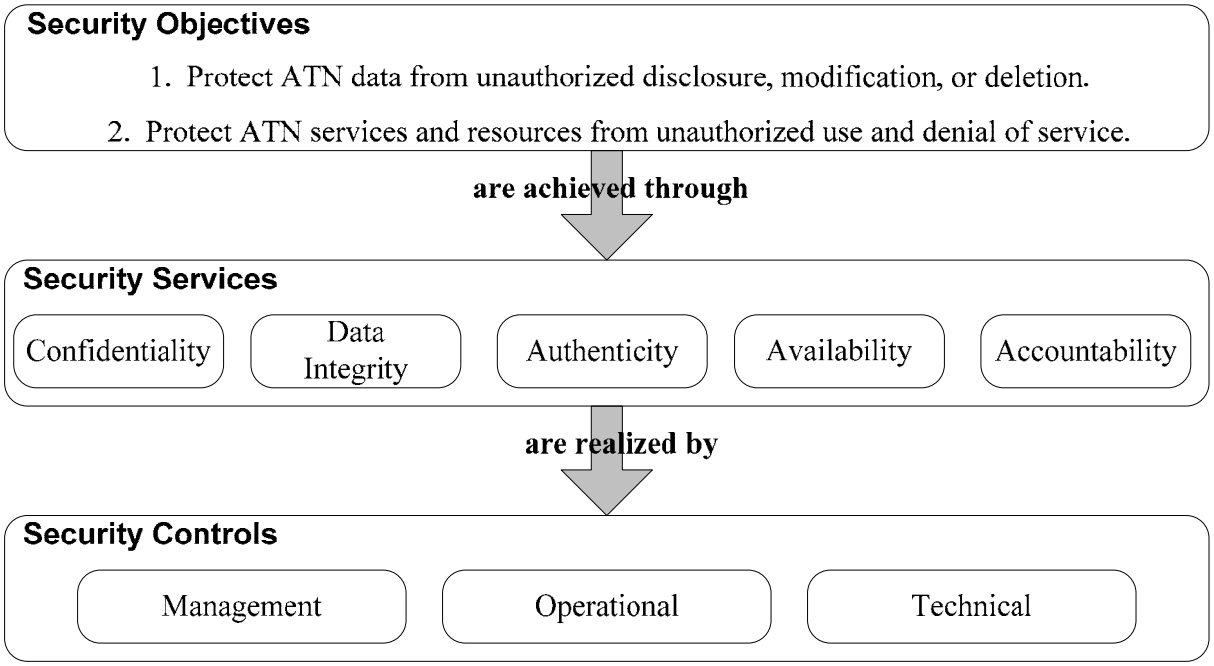


Figure 1-1. Security Objectives, Services, and Controls

1.2 Document Organization

In addition to this introduction, this document contains 4 major sections.

Section 2 provides a description of the 17 control families in the three Management, Operational, and Technical control classes. This section also provides a mapping from the high-level services to the control families.

Section 3 provides guidance on control families in the Management class. This section describes best practices for the management organization in an entity participating in the ATN.

Section 4 provides guidance on control families in the Operational control class. It describes procedures which constitute an effective security operation.

Section 5 provides guidance on control families in the Technical control class. Section 5 describes how technical controls are applied to various components of an ATN system. It gives specific examples of controls applied to each component.

2. SECURITY CONTROL FAMILIES

2.1 Description of Control Families

Access Control (AC) is the capability of the system to limit access to authorized users, processes acting on behalf of authorized users, and devices (including other systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT) ensures that operational personnel are aware of the security risks associated with their activities and the security policies which apply to their systems, and ensures that personnel are adequately trained to carry out their duties and responsibilities.

Audit and Accountability (AU) is the capability of the system to generate audit records that may indicate unauthorized or inappropriate system activity and that may be used to ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, Accreditation, and Security Assessments (CA) ensures that the organization's management assesses the security controls in their system and authorize (accredit) the system for operation.

Configuration Management (CM) ensures that operational personnel control changes to their system's configuration.

Contingency Planning (CP) ensures that operational personnel have a plan for continued operation to maintain availability of critical user and system-level information in emergency situations.

Identification and Authentication (IA) is the capability of the system to identify and verify (i.e., authenticate) system users, processes acting on behalf of users, or devices.

Incident Response (IR) ensures that operational personnel handle security incidents and promptly report incidents to appropriate authorities.

Maintenance (MA) ensures that operational personnel perform preventative and regular maintenance on their system.

Media Protection (MP) ensures that operational personnel restrict access to system media to authorized personnel and physically control system media in controlled areas.

Physical and Environmental Protection (PE) ensures that operational personnel limit physical access to systems and protect systems against environmental hazards.

Planning (PL) ensures that the organization's management develops and implements a security plan for the system.

Personnel Security (PS) ensures that operational personnel are trustworthy and meet security criteria for their positions.

Risk Assessment (RA) ensures that the organization's management assesses the risk and magnitude of harm that may result from security attacks on the system.

System and Services Acquisition (SA) ensures that the organization's management allocates the resources required to adequately protect their system.

System and Communications Protection (SC) is the capability of the system to monitor, control, and protect communications and includes architectural controls, confidentiality, data integrity and interoperability.

System and Information Integrity (SI) ensures that operational personnel remediate system flaws, provide protection from malicious code and other attacks on the system's integrity, and monitor alerts and advisories and take appropriate action in response.

2. 2 Realization of Security Services through Controls

Table 2-1 depicts a mapping from the Asia/Pacific System Security Policy to the controls identified in section 2.1.

Table 2-1. Mapping of Controls onto Asia/Pac System Security Policy

Asia/Pac System Security Policy	Technical Controls	Operational Controls	Management Controls
Confidentiality			
(a) ATN data shall be protected from unauthorized disclosure during processing, transmission, and storage commensurate with the designated sensitivity of the data.	System and Communications Protection (SC)	System and Information Integrity (SI) Physical and Environmental Protection (PE)	System and Services Acquisition (SA)
Data Integrity			
(a) ATN data shall be protected from unauthorized or undetected modification during transmission, storage, and processing.	System and Communications Protection (SC)	System and Information Integrity (SI) Physical and Environmental Protection (PE) Configuration Management (CM)	System and Services Acquisition (SA)
Authenticity			
(a) ATN users and processes shall be uniquely identified.	Identification and Authentication (IA)	Personnel Security (PS)	
(b) ATN users and processes shall be authenticated before being granted access to ATN data, services, and resources.	Identification and Authentication (IA) Access Control (AC)	Personnel Security (PS)	
(c) ATN data, services, and resources shall be protected from unauthorized use or tampering.	Access Control (AC)		
(d) ATN users and processes shall have access only to those ATN data, services, and resources for which they have authorization.	Access Control (AC)		
Availability			

Asia/Pac System Security Policy	Technical Controls	Operational Controls	Management Controls
(a) ATN data, services, and resources shall be available for use by authorized users and processes.	System and Communications Protection (SC)	System and Information Integrity (SI) Contingency Planning (CP) Incident Response (IR) Physical and Environmental Protection (PE) Personnel Security (PS)	System and Services Acquisition (SA)
Accountability			
(a) An audit trail of use of ATN data, services, and resources by ATN users and processes shall be maintained.	Audit and Accountability (AU)	Personnel Security (PS)	
Verification			
a. ATN systems shall be verified to have system security commensurate with the risk and magnitude of harm resulting from unauthorized disclosure, modification, or deletion of ATN data, or unauthorized use and denial of service of ATN services and resources.			Planning (PL) Risk Assessment (RA)
Authorization			
a. ATN systems shall be formally approved for operation by the cognizant Designated Approving Authority (DAA).			Certification, Accreditation, and Security Assessments (CA)
b. Significant changes to ATN systems shall require another formal approval (or re-authorization).			Certification, Accreditation, and Security Assessments (CA)

3. MANAGEMENT CONTROL GUIDANCE

As defined in section 1.1, Management Controls are safeguards or countermeasures that focus on the management of risk and the management of system security.

3.1 Certification, Accreditation, and Security Assessments (CA)

The Asia/Pacific System Security Policy requires that ATN systems be verified to have system security commensurate with the risk and magnitude of harm resulting from unauthorized disclosure, modification, or deletion of ATN data, or unauthorized use and denial of service of ATN services and resources. This requirement essentially says that a system should have controls in place to meet the fundamental objectives for system security as noted in section 1.1. Verification of system security is more generally termed certification. This is where an organization conducts a risk assessment (see 3.3) and an assessment of the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome in terms of meeting the fundamental system security objectives. Management may use the Asia/Pacific System Security Checklist [Asia/Pac SSC]as a general guide in assessing security controls.

The Asia/Pacific System Security Policy also requires that ATN systems be formally approved (i.e., accredited) for operation by an individual responsible for security in the organization. This individual is called the Designated Approving Authority (DAA). The DAA is a senior organizational official that signs and approves the security accreditation thereby authorizing operation of the system.

3.2 Planning (PL)

A system may be authorized for operation by the organization's management even though there are controls not in place or controls which could be enhanced as determined by the security verification process. In this situation the organization would develop and implements a security plan for adding or enhancing controls in the system.

3.3 Risk Assessment (RA)

A formal risk assessment is the process by which an organization determines the risk and magnitude of harm resulting from unauthorized. The general process of risk assessment is depicted in Figure 3-1 from [NIST 800-100]. The process begins (1) with a characterization of the system. This involves identifying the data, resources, and services, that constitute the system and determining the importance of these items to the organization. The next steps are to identify threats to (2) and vulnerabilities of (3) the data, resources, and services. Identifiable threats (e.g., disclosure, modification, or loss of data) will have some probability of occurring and causing loss or damage to a system. An analysis (4) of the threats and vulnerabilities should

be conducted following a structured approach to analyze controls, estimate likelihood of threat occurrence, and assess the potential impact of the threats to arrive at a general risk determination. Risk analysis are generally and qualitative (e.g., high, medium, low). For each identifiable threat one or more controls should be recommended (5). The nominal controls in the Asia/Pacific System Security Checklist [Asia/Pac SSC] may be used as a general guide; however, additional system specific controls may also be necessary. The overall results of the risk assessment should be formally documented (6).

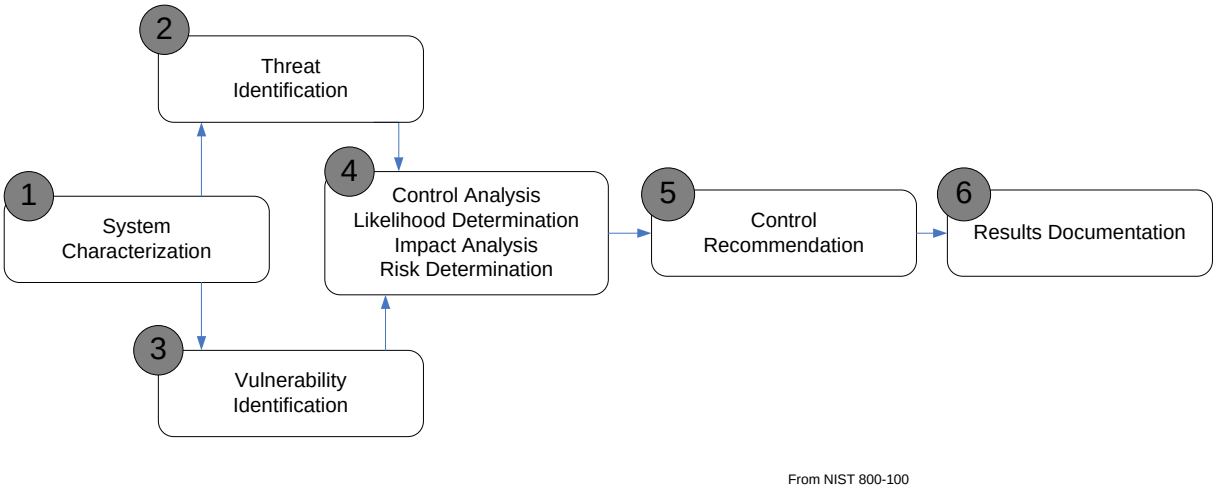


Figure 3-1. Risk Assessment Process

3.4 System and Services Acquisition (SA)

System and Services Acquisition (SA) is the control whereby an organization's management allocates the resources required to protect the system to level commensurate with the risks to the system. This activity should be applied as part of an on-going security policy for the organization. Specific resources should be allocated as a result of the CA and RA activities.

4. OPERATIONAL CONTROL GUIDANCE

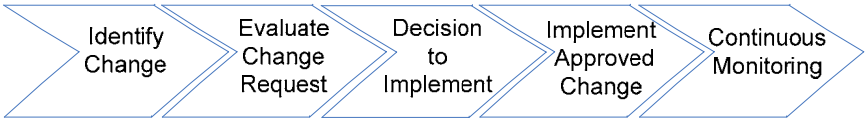
As defined in section 1.1, Operational Controls are safeguards or countermeasures for a system that are primarily implemented and executed by people.

4.1 Awareness and Training (AT)

Awareness and Training (AT) is the control for disseminating security information that management and operational personnel need to do their jobs. Awareness and Training ensures that management and operational personnel understand their security responsibilities and therefore are able to properly use and protect the system data, resources, and services.

4.2 Configuration Management (CM)

Configuration Management (CM) is the control that ensures that operational personnel control changes to their system's hardware components, software components and system adaptation parameters. Figure 4-1 depicts the Configuration Management process.



From NIST 800-100

Figure 4-1. Configuration Management Process

The first step in the process is to identify the need for the change. There can be various reasons for change such as the need to support more bandwidth on a communication channel, the need to upgrade to a new Operating System if the current is no longer supported, and general functional enhancements or corrections to the system. The change should be submitted to a decision-making body in the organization, e.g., to a Configuration Control Board (CCB).

The next step is to evaluate the change request. An impact assessment should be conducted to determine the effect of the change to the system under change or to other interrelated systems. For example a change in the routing policy could affect all systems in the network. Thus a change needs to be evaluated to determine if it is technically correct and if the gains (performance, new functionality, etc) are cost effective.

Next the CCM must make a decision to implement. The CCB may approve, deny, or otherwise defer implementation of the change.

If a decision to implement the change is made, then it should first be tested in an off-line or test environment. Once tested, the change may be placed into the operational system and the associated configuration control documentation is updated.

Configuration Management does not actually start and stop with incremental changes. Rather it is an on-going process that requires continuous monitoring. Configuration Management requires that operational personnel are always aware of their current baseline (for example a specific software release) and that the system is observed in operation to determine if there is any degradation in functional or performance capabilities as the system baseline is changed. In addition to managing software releases, application of fixes (i.e. "patches") to the system and changes in adaptation parameters must also be managed and continuously monitored.

4.3 Contingency Planning (CP)

Contingency Planning (CP) is the control that ensures that operational personnel have a plan for continued operation to maintain availability of critical user and system-level information in emergency situations. Figure 4-2 from [NIST 800-34] depicts the Contingency Planning Process.

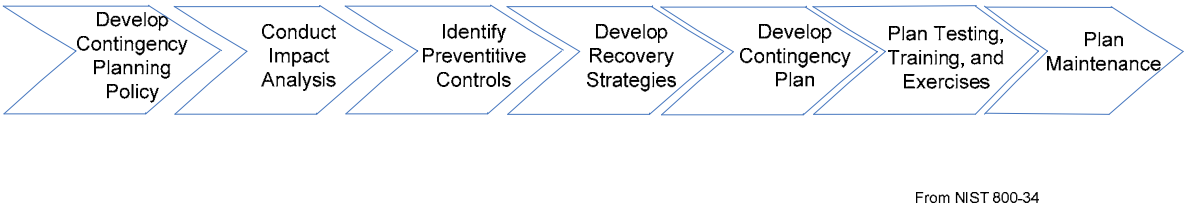


Figure 4-2. Contingency Planning Process

The organization should firstly have a policy for contingency planning that establishes the overall contingency objectives. There should be an impact analysis that evaluates the potential loss of a system or service. This may be the same as the system characterization in the Risk Assessment. The Preventive Controls are a subset of the overall CA controls which address the specific loss of systems and services. A recovery strategy should exist for each potential system/service loss. All the previous steps go into developing a formal Contingency Plan. Attachment A contains an outline for a Contingency Plan. Operational personnel should plan to test the Contingency Plan. Training should be conducted as necessary and actual exercises such as operation of backup systems should be conducted. As the system changes the contingency plan must be updated as part of a Plan Maintenance program.

4.4 Incident Response (IR)

Incident Response (IR) is the control that ensures that operational personnel handle security incidents and promptly report incidents to appropriate authorities. Figure 4-3 from [NIST 800-61] depicts the Incident Response Life Cycle.

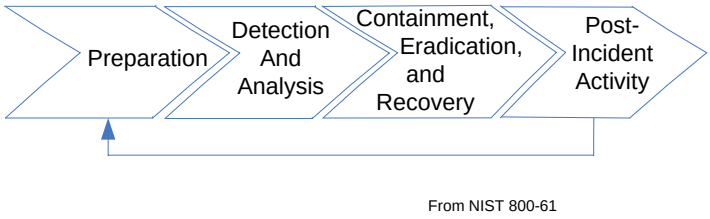


Figure 4-3. Incident Response Life Cycle

As depicted in Figure 4-3, Incident Response has several phases ranging from initial preparation through post-incident analysis which feeds back into the preparation phase. During preparation the organization selects and implements controls based on their risk assessment. The controls however cannot guarantee absolute protection and there will always be some residual risk. Therefore detection is required to alert the organization that an incident has occurred. Detection is primary through the technical controls described in section 5. When detected appropriate personnel within and external to the organization must be promptly notified. When an incident does occur, operational personnel can minimize the impact by firstly containing it before it spreads and does further damage. Measures should be taken to eradicate it as soon as possible so that recovery to normal services can be achieved. The post-incident analysis should attempt to identify the source of the incident as well as determine what additional controls can be implemented to prevent future occurrences, i.e., to apply “lessons learned” from the incident.

Attachment B contains an outline for an Incident Response Plan.

4.5 Maintenance (MA)

Maintenance (MA) is the control ensures that operational personnel perform preventative and regular maintenance on their system.

4.6 Media Protection (MP)

Media Protection (MP) is the control ensures that operational personnel restrict access to system media to authorized personnel and physically control system media in controlled areas.

4.7 Physical and Environmental Protection (PE)

Physical and Environmental Protection (PE) is the control ensures that operational personnel limit physical access to systems and protect systems against environmental hazards.

4.8 Personnel Security (PS)

Personnel Security (PS) is the control that ensures that operational personnel are trustworthy and meet security criteria for their positions.

4.9 System and Information Integrity (SI)

System and Information Integrity (SI) is the control that ensures that operational personnel remediate system flaws, provide protection from malicious code and other attacks on the system's integrity, and monitor alerts and advisories and take appropriate action in response.

5. TECHNICAL CONTROL GUIDANCE

5.1 Technical Controls

As defined in section 1.1, Technical Controls are safeguards or countermeasures that a system executes through mechanisms in the hardware or software components of the system itself. The technical controls addressed in this section are:

- AC - Access Control
- AU - Audit and Accountability
- IA - Identification and Authentication
- SC - System and Communications Protection

For the Management and Operational controls, general guidance was provided for each control. In this section Technical Controls are described in terms of the hardware or software components of the system to which they apply.

5.2 Technical Controls Applied to Information System Components

Technical Controls are best applied following a *Defense-in-Depth* strategy whereby multiple overlapping protection approaches are implemented. For the Asia/Pac ATN, this section provides guidance on the application of controls to the network, equipment, operating system, applications, and data. Figure 5-1 depicts the concept of Defense-in-Depth.

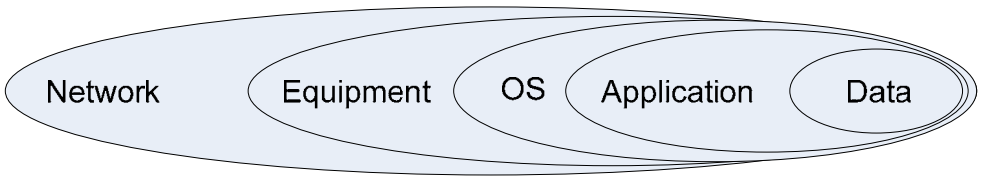


Figure 5-1: Defense-in-Depth

Figure 5-2 depicts the general technical controls applied to information system components.

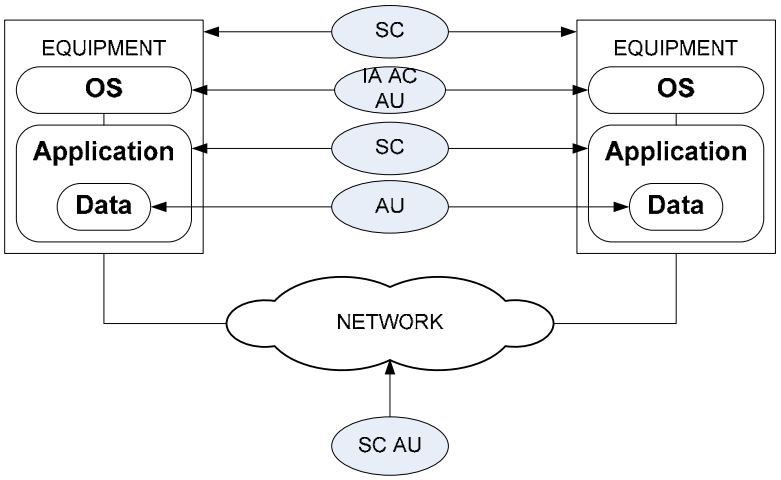


Figure 5-2: Technical Controls to ATN Component Mapping

As is depicted in Figure 5-2, the System and Communications Protection (SC) and Audit and Accountability (AU) control families apply to the Network. Note that network is used in a logical sense here so that protocol software in host systems is part of the network.

The System and Communications Protection (SC) control family also applies to equipment. This generally refers to architectural controls.

The Access Control (AC), Audit and Accountability (AU), and Identification and Authentication (IA) control families apply to the Operating System.

The Systems and Communications Protection (SC) control family applies to Applications.

The Audit and Accountability (AU) applies to Application Data.

5.2.1 Controls Applied to the Network

This section identifies network controls which may be applied in the Asia/Pac ATN in support of AMHS. Figure 5-3 provides an overview of the controls.

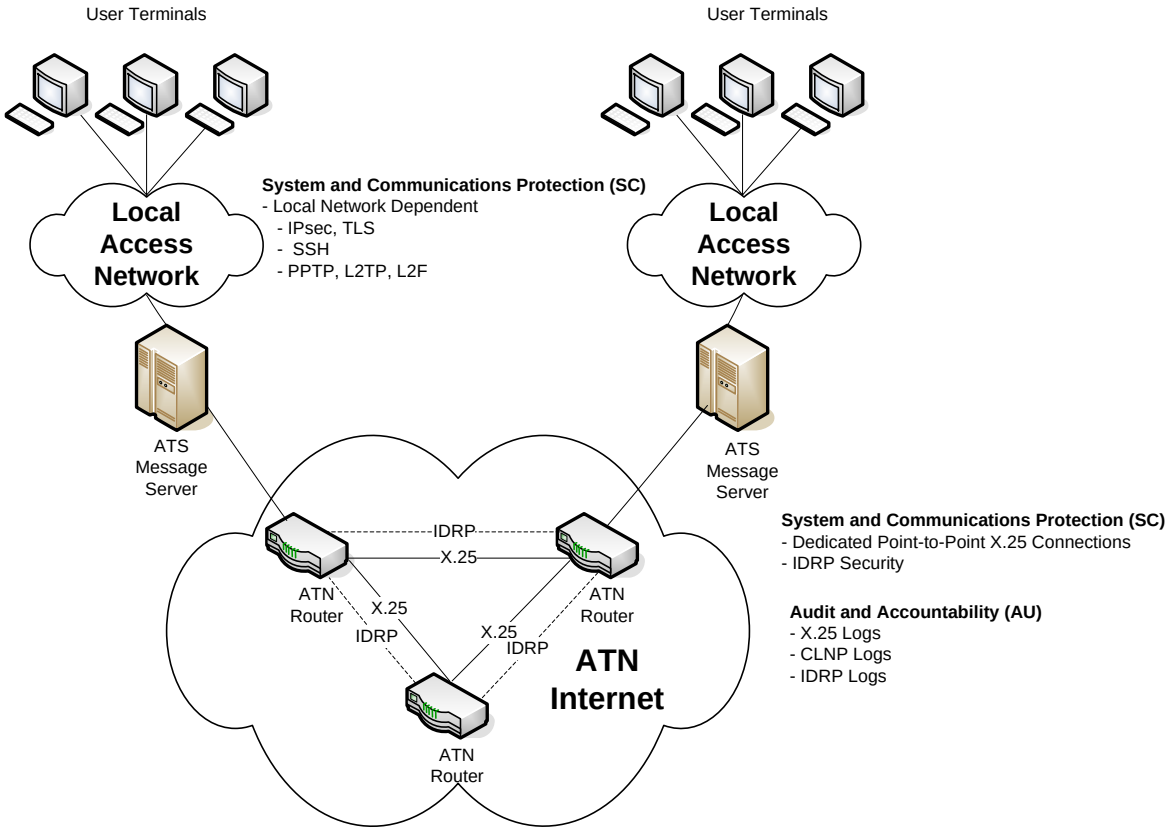


Figure 5-3: Network Controls

5.2.1.1 System and Communications Protection (SC)

5.2.1.1.1 Dedicated Point-to-Point X.25 Links

Currently interconnectivity in the Asia/Pac ATN Internet is through the use of dedicated point-to-point X.25 circuits. This limits access since X.25 circuits are associated with a specific physical port.

5.2.1.1.2 Inter-domain Routing Protocol Security

The Inter-domain Routing Protocol (IDRP) has defined options for authentication of routing data. Edition 3 of Doc 9705 defined a method of authentication using the HMAC keyed message authentication code. Edition 3 allows for two ATN routers to exchange public keys in public key certificates during the IDRP open exchange.

Rather than exchange certificates and implement a supporting Public Key Infrastructure (PKI) it is recommended that the routers derive a shared session key from a pre-shared value.

5.2.1.1.3 Local Access Network Security

The connection of User Terminal to the AMHS switching systems is a local matter. These connections may be secured in a number of ways.

One common method is to use the Secure Shell (SSH) protocol. SSH contains secure replacements for several unencrypted application protocols such as telnet, rcp, and FTP.

An alternative to SSH for HTTP type applications is to use Transport Layer Security (TLS). All major web-browsers support TLS. TLS authentication is typically one way, authenticating the client to a server.

If the local access network is an IP network then an IPsec Virtual Private Network may be used to secure Terminal to AMHS communications.

If the local access method is not a layer 3 network, then various Level 2 protocols may be used. Options include the Point-to-Point Tunneling Protocol (PPTP), the Layer 2 Tunneling Protocol (L2TP), and Layer 2 Forwarding (L2F).

5.2.1.1.4 IPsec with the IP SNDCF

In the ATN Internet of the future the Internet Protocol Subnetwork Dependent Convergence Function (IP SNDCF) may be used to interconnect ATN routers in place of X.25 links. In this case, it is recommended that the IP Security (IPsec) protocols be used. This may be with manual key establishment or dynamically using the Internet Key Exchange (IKE) protocol. IKE may be used with pre-shared keys or using public key certificates.

5.2.1.2 Audit and Accountability (AU)

5.2.1.2.1 System Logs

It is recommended that the communication logs of Asia/Pac ATN Routers be reviewed for anomalous activity. Specifically the following logs should be reviewed:

- X.25 Logs
- IDRP Logs
- Connectionless Network Protocol (CLNP) Logs

5.2.2 Controls Applied to Equipment

5.2.2.1 System and Communications Protection (SC)

5.2.2.1.1 Redundancy

Equipment may be configured redundantly to limit the effects of many attacks on systems including Denial-of-Service attacks.

5.2.3 Controls Applied to the Operating System

5.2.3.1 Identification and Authentication (IA)

5.2.3.1.1 User IDs and Passwords

System Administrators may configure the allowed users of the system. There are at least two classes of accounts which may be configured: normal system users and super-users.

5.2.3.2 Access Control (AC)

5.2.3.2.1 User Access

Once users have been identified and authenticated using IA controls, the system administrator may limit their operating environment, that is, an administrator may limit the types of transactions and functions that authorized users are permitted to exercise.

5.2.3.2.2 OS Checklists

The National Institute of Standards and Technology (NIST) maintains a Security Configuration Checklist Repository for various products and systems including all major Operating Systems. (http://checklists.nist.gov/repository/category.html)

5.2.3.3 Audit and Accountability (AU)

5.2.3.3.1 OS System Logs

The operating system logs should be reviewed on a regular basis for abnormal activity. This may be done manually or using automated tools such as TRIPWIRE.

5.2.4 Controls Applied to Applications

5.2.4.1 System and Communications Protection (SC)

5.2.4.1.1 AMHS Security

Figure 5-4 depicts AMHS Security which is applied from an originating ATS Message User Agent to a destination ATS Message User Agent.

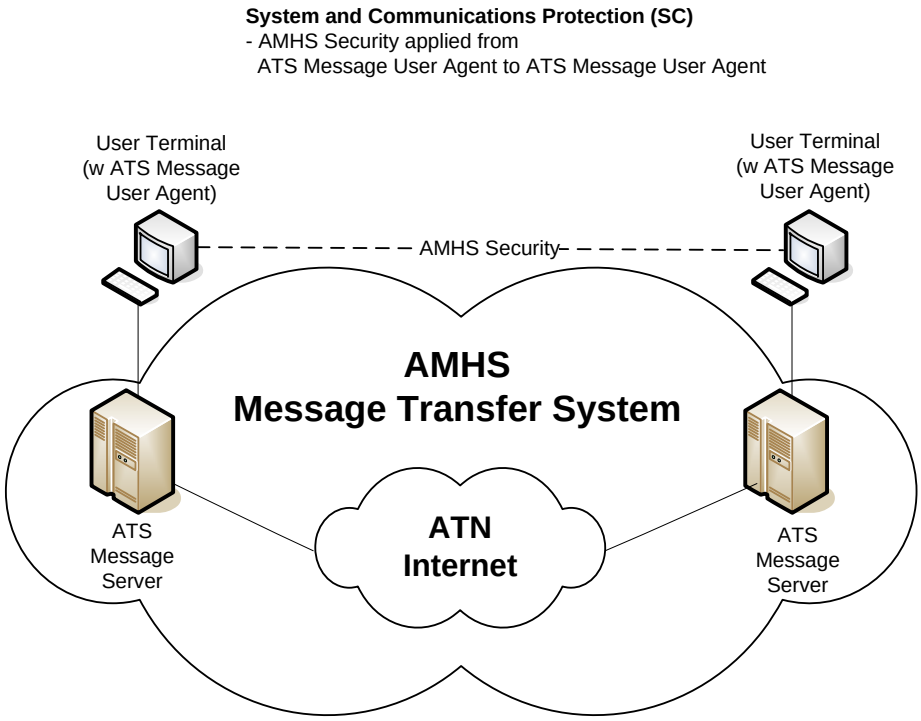


Figure 5-4: AMHS Security

AMHS security begins with the originating ATS Message User Agent digitally signing an Interpersonal Message using its Private Key. The message is sent through the ATS Message Transfer System to the recipient ATS Message User Agent. The recipient UA retrieves the Public Key of the originating UA from a public key certificate using a supporting directory service. With the originators public key the recipient UA can verity the signed message.

5.2.5 Controls Applied to Data

5.2.5.1 Audit and Accountability (AU)

5.2.5.1.1 AMHS Traffic Logging

Traffic Logging is required as part of the basic AMHS service. Specifically, Doc 9705 requires that "an AMHS Management Domain shall be responsible for long-term logging of all messages in their entirety which are originated by its direct AMHS users, for a period of at least thirty days."

6. References

[Asia/Pac SSP] ASIA/PAC Aeronautical Telecommunication Network System Security Policy, Second Edition, September 2008

[Asia/Pac SSC] ASIA/PAC Aeronautical Telecommunication Network System Security Checklist, First Edition, May 2009

[NIST 800-34] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, "Contingency Planning Guide for Information Technology Systems"

[NIST 800-53] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems"

[NIST 800-61] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, "Computer Security Incident Handling Guide"

[NIST 800-100] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100, "Information Security Handbook: A Guide for Managers"

ATTACHMENT A
CONTINGENCY PLAN OUTLINE

1. INTRODUCTION

1.1 Purpose

1.2 Applicability

1.3 Scope

1.4 References

[NIST 800-34]	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, "Contingency Planning Guide for Information Technology Systems", June 2002

2. CONCEPT OF OPERATION

2.1 System Description

2.2 Line of Succession

2.3 Responsibilities

3. NOTIFICATION/ACTIVATION

3.1 Notification Procedures

3.2 Damage Assessment

3.3 Plan Activation

4. RECOVERY

4.1 Sequence of Recovery Activities

4.2 Recovery Procedures

5. RECONSTITUTION

ATTACHMENT B
INCIDENT RESPONSE PLAN OUTLINE

1. INTRODUCTION

1.1 Purpose

1.2 Applicability

1.3 Scope

1.4 References

[CSIRT] Carnegie Mellon Software Engineering Institute "Handbook for Computer Security Incident Response Teams (CSIRTs)", April 2003

[NIST 800-61] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, "Computer Security Incident Handling Guide", January 2004

[RFC 2196] Fraser, B. Ed., "Site Security Handbook", September 1997

[RFC 2350] Brownlee, N., and E. Guttman, "Expectations for Computer Security Incident Response", June 1998

2. Contact Information

2.1 Name of the Team 1

2.1.1 Team Member 1

Address

Time Zone

Telephone Number

Facsimile Number

Other Telecommunication

Electronic Mail Address

Public Keys and Encryption Information

Other Information

2.1.n Team Member n

2.x Name of the Team x

3. Charter

3.1 Mission Statement

3.2 Constituency

3.3 Sponsorship and/or Affiliation
