Version 3.1, March 2005

Defense Information Systems Agency (DISA)

Voice Networks Information Assurance Test Plan (IATP)

March 2005

1. Introduction

In early 2002, the DISA Center for Information Assurance was asked to create a security test program for DSN telecommunications switches to be implemented at the DISA Joint Interoperability Test Command (JITC). Telecommunications switches must be certified by the JITC as interoperable per the requirements spelled out in the Generic Switching Center Requirements Document (GSCR 2003). The JITC uses a test plan generated from the requirements in the GSCR called the Generic Switch Test Plan (GSTP).

The GSCR has a section devoted to security, section 13. Previously, there was no testing done for these security requirements. Rather, a letter from the vendor on compliance with the Telcordia GR-815-CORE security requirements was accepted by JITC, primarily because the mission of the JITC was that of interoperability and not security.

In CJCSI 6215.01B dated September 23, 2001, the DSN Single Systems Manager was given the following responsibilities:

"The DSN SSM is designated as the voice standards and voice processing/transport technology migration coordinator to ensure end-to-end global voice quality, interoperability, and visibility for all voice C2 services. As such, all CINC, Service, and agency post, camp, or station voice transport and processing initiatives should be coordinated with the DSN SSM. The DSN SSM will provide an annual assessment of the impact of emerging voice processing/transport technologies on global end-to-end voice performance and C2 services to the Joint Staff and the DSN CCB."

The DSN SSM in accordance with the above responsibilities recognized that VoIP technologies were being considered for support of local C2 telephony services and that these technologies had significant security risks that were not experienced with the Circuit Switched Time Division Multiplex technologies employed in the DSN. In addition, the DSN SSM had initiated a major effort to gain an Authorization to Operate (ATO) under the DITSCAP process.

This test plan is the culmination of efforts to rectify the lack of security testing for DSN telecommunication switches and to meet the requirements of DITSCAP and DoDI 8100.3.

2. Purpose

The purpose of the IATP is to provide security features test criteria for telecommunications switches connected or planned for connection to the DSN. The IATPs supports evaluation of security features within the existing DSN and critical areas involving Military Unique Features (MUF) and new telecommunications technology. The IATPs also addresses security features between new technologies; new technologies and the existing network; and the performance impact of these new technologies on MUF. The IATP is based on DISN and DSN STIGs and is required to be conducted prior to the connection and operation of telecommunications switches to the DSN.

The DSN STIGs provide the technical security policies, requirements, and implementation details for both the security features required for telecommunications switches, as well as the implementation guides for operating telecommunications switches by the DoD components. The STIGs support lease or procurement, testing and operational implementation procedures and assist DSN sites in meeting the minimum requirements, standards, controls, and options for protecting telecommunications switch operations.

This test plan and more importantly the testing program it implements is specifically aimed at testing DSN telecommunications switches based on or relying heavily on new and possibly more exploitable VoIP technologies for vulnerabilities.

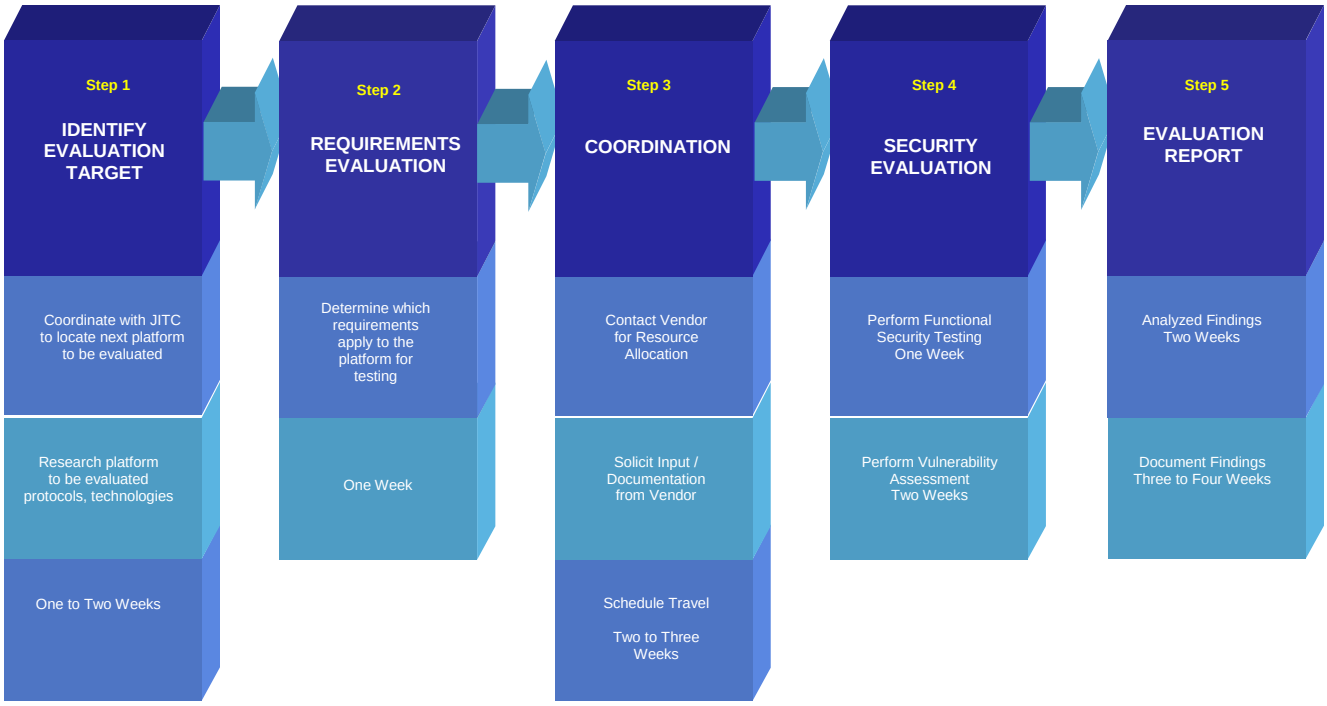
3. Scope

This IA test plan covers both traditional telecommunications switches (pure TDM) and those that are IP-enabled or IP-Centric. This test plan begins with a set of preliminary actions. These actions must take place prior to implementing the remainder of the test plan. The remaining test plan is divided into two phases, a functional security phase and a vulnerability assessment phase. The functional security phase focuses on functional requirements the system. The overall system may be subjected to multiple sets of requirements as listed in the section that describes the first phase of the testing. The set of applicable functional security requirements is determined by the overall system functionality and the functionality of the individual system components.

The second phase of the test plan calls for a vulnerability assessment carried out against the platform under test following the guidelines found in NIST SP 800-42 (references). This half of the test plan identifies candidate tools that may be used during an assessment. DISA reserves the right to use any security tool in these tests, so long as the nature of electronic attack remains creative and highly adaptive. The goal of the second phase of testing is to determine the resilience of a voice solution to common types of attacks (Denial of Service, malformed/fragmented packets/requests, etc.). The results may range from total disability of the system to degraded call-processing abilities for the duration of a given attack or imperviousness to the attack.

The security testing will be performed by DISA's Center for Information Assurance VoIP Security Engineering (GE446) on equipment brought to the JITC by vendors for Interoperability certification and Information Assurance Certification and Accreditation testing. The results of the testing are compiled in a report that identifies and categorizes risks and is released to DISA, the sponsoring Service/Agency, and the vendor. The sponsoring Service/Agency in conjunction with the vendor shall correct all risks via mitigation strategies and resubmit for testing.

The following diagram shows the general process for the security testing of a given telecommunications switch platform:



4.0 Policy and Guidance

This section discusses the testing approach employed in the Defense Information Systems Agency (DISA) Defense Switched Network (DSN) VoIP Information Assurance Test Plan. It provides a description of the policies and guidance documents that help define the test requirements, objectives and procedures.

4.1 Department of Defense and Industry Standards

The number of DoD regulations, policies and guidance documents for security related activities has grown significantly over the last several years as the DoD community has tried to devise standard Information Assurance (IA) practices to protect its assets and information. Government regulations now cover all aspects of IA, including the acquisition, deployment, and use of IA and IA enabled Information Technology (IT) products.

The National Security Telecommunications and Information Systems Security Policy (NSTISSP) 11 dated January 2000, as part of the National Security Telecommunication and Information Systems Security Committee (NSTISSC) dictates the national policy governing the acquisition of IA and IA-enabled IT products. NSTISSP 11 defines compliance requirements for Government Off the Shelf (GOTS) and Commercial Off the Shelf (COTS) acquisition by government entities. Effective January 1, 2001, acquisition preference was given to GOTS and COTS IA and IA enabled IT products that comply with one of the documents listed below. Effective July 1, 2002, all newly acquired GOTS and COTS IA and IA-enabled products are required to be compliant with at least one of these documents:

- The International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement;

- The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program;

- The NIST Federal Information Processing Standard (FIPS) validation program.

While NSTISSP 11 regulates what IA and IA-enabled products can be acquired as well as mandates CC, NIAP or FIPS compliance, there are several DoD documents that define policy and guidance for the protection of voice signaling and bearer traffic. These documents are DODD 8500, DISA DSN System Technical Implementation Guide (STIG), and CJCSI 6215.01B. The following sub-sections discuss the various Federal regulations, policies, and guidance documents that will provide testing requirements, objectives, and procedures for the DSN VoIP Information Assurance Test Plan.

4.2 Protection Profiles and Common Criteria

The International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement standard is used to evaluate and rate security architectures. The CC standard replaces the retiring Trusted Computer System Evaluation Criteria (TCSEC) DOD 5200.28-STD, dated December 1985, more commonly referred to as the Orange Book. CC rates the levels of security based on compliance to an Evaluation Assurance Level (EAL) standard. This standard has levels ranging from EAL 1 (the lowest level of compliance) to EAL 7 (the highest level of compliance). CC EALs are performance measures that were derived from the compilation of several assurance classes including configuration management, delivery and operation, development, guidance documents, life cycle support, formal testing of security targets, vulnerability assessment, assurance and maintenance. The two draft Protection Profiles help define the minimum-security requirements for PBX, end office, small end office, and multi-function voice switches used by U. S. Government organizations, specifically the Department of Defense. These Protection Profiles are used in handling unclassified or sensitive but unclassified information for various Mission Categories (i.e. Mission-Critical) in different risk environments. The following is a list of the protection profiles that provide the requirements for this test plan:

- NIAP Draft PBX Protection Profile.
- NIAP Draft Telecommunications Switch Protection Profile

The protection profiles define the assumptions about the security aspects of the environment in which the PBX or telecommunications switch will be used, the threats that are to be addressed by the voice system, implementation-independent security objectives of the voice system and its environment, the functional and assurance requirements to meet those objectives, and provides a rationale demonstrating how the requirements meet the security objectives.

The objectives defined in the protection profiles are used by vendors to write their security targets, which are subsequently used for CC evaluation. In addition, protection profiles determine which EAL rating their voice systems receive. DSN will leverage these objectives to define some of the test objectives in Functional Security Testing section of this test plan.

4.3 DoD/DISA Policy and Guidance

This section provides a description of the various DoD and DISA policy and guidance documents that outline requirements for the DSN VoIP Information Assurance Test Plan. DoDD 8500.1 was released and signed October 2002 while DoDD 8500.2 was released and signed February 2003; these documents provide new requirements for IA related activities within the DoD. The DISA DSN STIG provides technical implementation guidance for protecting DSN voice systems. CJCSI 6215.01B is a document from the Chairman of the Joint Chiefs of Staff, which also provides DoD voice system requirements.

4.3.1 DoDD 8500

The newly signed DODD 8500.1 and 8500.2 define requirements based on Mission Assurance Categories (MAC) and Confidentiality Levels (CL). MACs range from I to III. MAC levels require different levels of robustness for integrity and availability. MAC I requires high confidence levels for both integrity and availability, MAC II calls for high integrity and medium availability, and MAC III requires basic confidence levels for both integrity and availability. CLs are determined by the classification of the information that is processed by the system and determine the level of robustness for confidentiality that is required. In general, CL Low applies to systems that process only public information, CL Medium is for systems that process Sensitive But Unclassified (SBU) or For Official Use Only (FOUO) information, and CL High is for systems that process classified information. MACs and CLs are not dependent upon one another. A MAC I, II or III system can process any classification level of information. After determining the appropriate MAC and CL categories, the appendices of the DoDD 8500 series documents can be referenced for the requirements definitions.

4.3.2 DISA Defense Switched Network STIG, VoIP STIG

The DSN Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to the Defense Switched Network. The STIG addresses three major sub-systems: the Advanced Defense Switched Network Integrated Management Support System [ADIMSS], the SS7 subsystem, and the DSN switching systems.

The policies and guidance provided by the DISA STIG primarily discuss the COTS firewall functional review. This includes requirements for the types of authentication available, the ability to resist attacks, auditing capabilities, and administration capabilities. Tests for these requirements mainly pertain to the functional security testing sections of this document

4.3.3 CJCSI 6215.01B

The Chairman of the Joint Chiefs Staff Instruction (CJCSI) 6215.01B, 23 September 2001 provides joint policy and guidance to DoD components for voice systems. The policy dictates that:

The design and operation of DSN must maximize protection of switches, transmission links, and NM facilities and provide protection against disruption, intrusion, compromise, and denial of service. Based on the mission, priority, and susceptibility of user and switch operations, security countermeasures must be applied to provide, COMSEC, and physical and personnel security protection.

The open-ended vulnerability tests will be performed to gauge a given voice solution's ability to withstand many common attack techniques from the data community.

5.0 Preliminary Actions

This section discusses the actions that are required prior to implementing the test plan.

5.1 Security Technical Implementation Guides

Each system component must comply with the most current applicable Security Technical Implementation Guides (STIGs). For the purpose of this section, the scope of the STIGs is unlimited. Any individual system component may require the application of one or multiple STIGs. STIG applicability is determined by attributes such as the underlying operating system of the system component, applications or services that operate on the system component, and the overall functionality of the system component. A comprehensive list of the applicable STIGs can be found at the URL http://iase.disa.mil/stigs/index.html. This list is current to the time visited, but is updated on a regular basis.

The first preliminary action is to verify that all system components comply with all applicable STIGs. There are two methods involved in verifying STIG compliance. System Requirement Review (SRR) scripts are developed for the purpose of automating STIG compliance verification. The other method to verify STIG compliance is manual verification. Many STIG verifications require the use of SRR scripts and manual verification.

6.0 Functional Security Testing

The first phase of testing is aimed at verifying functional security requirements of the system and its' components.

6.1 Voice Handset Security Requirements

The National Telephone Security Working Group (NTSWG) provides functional security guidelines for legacy and VoIP capable handsets. The guidelines address requirements such as on-hook audio emanation levels and handset management methods. All voice handsets may be subjected to these requirements.

6.2 Operations Administration, Maintenance and Provisioning Security Requirements

If the system is a telecommunications management network (TMN) the system will be tested for baseline security requirements for a management plane. The verification of security requirements will involve the use of documents such as the

ANSI T1.276-2003, *Operations, Administration, Maintenance and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane*.

6.3 Generic Switch Center Requirements

This phase of testing is aimed at determining the security functionality of a telecommunications switch in accordance with the GSCR. Refer to Section 13 (security) of the GSCR. It refers mainly to Telcordia GR-815 Issue 2 dated 2002. Telecommunications switches shall be compliant with Requirements, Conditional Requirements, and Objectives spelled out in GR-815. Part of this phase of testing involves verifying through vendor documentation that the switch being assessed is compliant with GR-815 where appropriate.

The DoD standard for addressing security features and requirements for IA and IA-enabled products is a common-criteria based protection profile or security target. Currently, there are no accepted protection profiles for PBXs or Telecommunication switches. However, there are draft protection profiles for these platforms. These protection profiles were written with the help of the authors of GR-815, and the requirements are the same, just not as thorough in the protection profile. Functional security testing for telecommunications switches will make use of the protection profile test methodologies that accompany these draft protection profiles. These protection profile test methodologies are essentially uniform test procedures for assessing the security of a given switch under evaluation. The reports that result from these IA assessments shall include a requirements traceability matrix that maps the requirements from the draft protection profile over to the requirements from Telcordia's GR-815 issue 1.

During this part of the testing, the requirements from GR-815 and the draft NIAP PBX or Telecommunications Switch Protection Profiles are verified, as is any other security feature available in the platform under evaluation. For example, if cryptographic protection of RTP streams is offered, it will be evaluated for functionality. A more formal cryptographic evaluation of the particular algorithms and key strengths used is beyond the scope of these assessments and are covered more thoroughly in other programs.

This part of the testing focuses on a switch's signaling and operations ports. Signaling ports connect to communication media (fiber trunks, copper trunks) to carry user communications. Operations ports are used by craft persons to access the embedded software of the switch for maintenance, troubleshooting, provisioning.

6.1 Protection Profile/GR-815 Requirements Categories

The following list is taken from the NIAP draft PBX/Telecommunication Switch protection profile test methodologies and offers some explanation of the categories of security requirements from those documents as well as GR-815. Several tests are run from each of the categories, found in section 5 of the corresponding document. The concepts behind these categories apply to all systems that process telephony, be it packet-based or circuit-switched.

6.1.1 User Identification

Identification is the process of recognizing a user's unambiguous and auditable identity with the help of an *identifier, which* is typically referred to as the user-ID. In general, the user-ID need not be confidential. It is the unambiguous name of a *user* by which the user can be held accountable. As such, all actions initiated by a user need to be associated with the corresponding user-ID.

6.1.2 User Authentication

Authentication is the process of verifying the claimed identity of a user. Depending on the TOE, there could be different kinds of authenticators such as passwords, tokens, smart cards, key-based authenticators, voice recognition, retina scan, etc. No matter what type of authenticator is used, it is of critical importance to ensure that the authenticator of one user cannot be spoofed by another.

6.1.3 System Access Control

System Access Control authorizes establishment of a session (i.e., login) and continuation of a session until logoff. There are certain restrictions regarding the login procedure, i.e., how a session is established and how it is sustained.

6.1.4 Resource Access Control

Resource Access Control is the capability of a TOE to deny access to a resource of the TOE unless there is proper authorization (e.g., user privilege, channel privilege, terminal privilege, etc.).

6.1.5 Security Log (Audit)

A Security Log provides tools to establish an audit trail, so that if security breech is suspected, investigation can be made as to whether/how the breech occurred.

6.1.6 Security Administration

This feature entails proper activation, maintenance, and usage of the security features of a switch, conducted by an appropriate administrator. It includes overriding vendor-supplied defaults, keeping the security parameters up to date, monitoring suspected activities, and generating security audits when needed.

The Protection Profiles also include tests for packaging and delivery as well as Year 2000 compliance. These tests are beyond the scope of the security assessments.

7.0 Vulnerability Assessment

The second phase of the security assessment focuses on vulnerabilities that can be discovered within the signaling protocols of legacy time division multiplexing (TDM) voice systems and all protocols encompassed by IP enabled systems.

7.1 TDM Vulnerability Assessment

All applicable systems may be subjected to TDM vulnerability tests. These tests include, but are not limited to, injection of malicious signaling data, corrupted

signaling data, and selected customized data. The tests are conducted with the use of commercially available hardware. The hardware will attach to any point of the system that is deemed appropriate by the tester.

7.2 IP Vulnerability Assessment

This section of the vulnerability security assessment follows the guidelines set forth in NIST Special Publication 800-42 (SP 800-42), *Guideline on Network Security Testing*.

This document enumerates nine different types of network security testing techniques, namely:

- Network Mapping
- Vulnerability Scanning
- Penetration Testing
- Security Test & Evaluation
- Password Cracking
- Log Reviews
- File Integrity Checkers
- Virus Detectors
- War Dialing

The security assessments done by DISA's Center for Information Assurance follow the guidelines for network mapping, vulnerability scanning, password cracking, log reviews, and occasionally, penetration testing.

First, the security evaluators will use any of a number of widely available tools to exclusively test any supporting IP network infrastructure in accordance with SP 800-42. The supporting IP network infrastructure will typically be a local area network (LAN) consisting of IP routers and Ethernet switches. All IP enabled hosts that support the system applications will be unattached during this testing. Once this initial testing is complete all IP enabled hosts are re-attached to the IP network infrastructure. The security evaluators will then use the same set of tools to test all aspects of the IP applications in accordance with SP 800-42. www.insecure.org/tools.html offers a list of the "top 75 security tools." Any of the tools from this repository may be used if deemed appropriate. Many of these tools are also discussed in detail in the above-mentioned NIST SP 800-42. The structure of the vulnerability assessment is roughly as follows:

1. Network Mapping using port sweeps, protocol analyzers, etc.
2. Vulnerability Scanning using Nessus, ISS, Retina Scanner, etc.
3. More In-depth testing using Nemesis, HUNT, ISIC, etc.

Given the dynamic threat nature, this portion of the testing shall remain dynamic, utilizing new tools and attacks as they appear.

The object of the second phase of testing is roughly to determine the impact of an electronic attack should it bypass all perimeter and infrastructure security controls. The presence of any well-known vulnerability will be noted in the report, and a mitigation strategy offered if appropriate.

7.2.1 Vulnerability Assessment Tools

The following is a list of tools that may be used in the second phase of testing. It is not meant to be an exhaustive list, and tools may be used that do not appear in this list.

Nmap – A port scanner used to identify active network hosts and associated services. Nmap uses raw IP packets to identify the available hosts on a network, the services or ports that are open, type of operating system and version that hosts are running, type of packet filters and firewalls in use, and other characteristics. Nmap sends a system call provided by the host operating system and attempts to open a connection to any or all ports (user selects) on a remote host. If the port is listening or open, then the request will succeed, otherwise the port is not listening or is in a closed state. Nmap is very configurable with the use of several command flags enabled.

L0pht Crack – A password cracker for Windows NT, XP and 2000 workstations. L0pht Crack uses dictionary brute force attacks to scan hashes traversing to network to discover usernames and passwords. Sometimes only partial passwords and usernames are discovered. And flags can be set to note certain criteria.

Dsniff – A collection of network tools for auditing and penetration testing. Designed to passively monitor a network for interesting data (passwords, e-mail, files, etc.). Arpspoof, dnsspoof, tcpkill and macof facilitate the interception of network traffic normally unavailable to an attacker.

Ethereal – A network protocol analyzer used on Unix and Windows workstations allows users to capture data from a live network or from a file on disk. It can interactively browse the captured data; viewing summarized and detailed information for each packet. Ethereal has several powerful features such as rich display filter language and the ability to view the reconstructed stream of a TCP session.

Netcat – A utility that reads and writes data across network connections, using TCP or UDP protocols. It is a back door port director that can be initiated directly or easily driven by other programs or scripts.

Nessus – A vulnerability scanner operating on Linux that is network based and used to identify security holes remotely on network hosts. Nessus is capable of testing a wide range of network hosts in multiple ranges of ports, looking for a wide range of updateable vulnerabilities at any given time.

Icmpquery – A tool used to send and receive ICMP queries for the destination hosts network mask and current time. This will enable the users to obtain the destination hosts IP address, subnet mask, and local time and may distinguish what Operating System is in use.

SnifferPro – An analysis tool designed to collect data and assist in analyzing network packet streams in real-time analysis. This data can then be modified or duplicated and retransmitted to test hardware and software components.

Nemesis – a firewall integrated inside a router that delivers security at the entry point of the network. Notifies the user when unauthorized attempts to gain access to

the network. It validates users when they connect to an 'allowed' network application. After validation they are free to access network resources without any the performance constraints.

Hping – is a command-line oriented TCP/IP packet assembler and analyzer. The interface is inspired to the ping (8) unix command. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode and the ability to send files between a covered channel.

Retina – is a tool created by eEye for scanning up to 254 IP addresses at once to determine if any are vulnerable. After scanning, it delivers a comprehensive report that displays in order of seriousness (high, medium, low, informational) all vulnerabilities on the systems and suggests appropriate fixes such as downloading related patches, step-by-step instructions or using the automatic repair capabilities.

Appendix A: 2003 GSCR Section 13.

Section 13 – Security

[Required: TS, EOS, MFS, SMEO, PBX1]

The DSN shall meet security requirements in GS-815-CORE, Issue 2, March 2002 and conform to the requirements outlined in *DODI 5200.40, 30 December 1997, 'Defense Information Technology Security Certification and Accreditation Process (DITSCAP)'.*

Appendix B : References