

PACKAGE ID - 000734MLTPL01 SPI/U3.2

KWIC TITLE - Security Profile Inspector for UNIX Systems

AUTHORS - Bartoletti, A.
Lawrence Livermore National Lab., CA (United States)

LIMITATION CODE - UNL **AUDIENCE CODE** - UNL

COMPLETION DATE - 10/01/1994 **PUBLICATION DATE** - 08/01/1994

DESCRIPTION - SPI/U3.2 consists of five tools used to assess and report the security posture of computers running the UNIX operating system. The tools are: Access Control Test: A rule-based system which identifies sequential dependencies in UNIX access controls. Binary Authentication Tool: Evaluates the release status of system binaries by comparing a crypto-checksum to provide table entries. Change Detection Tool: Maintains and applies a snapshot of critical system files and attributes for purposes of change detection. Configuration Query Language: Accepts CQL-based scripts (provided) to evaluate queries over the status of system files, configuration of services and many other elements of UNIX system security. Password Security Inspector: Tests for weak or aged passwords. The tools are packaged with a forms-based user interface providing on-line context-sensitive help, job scheduling, parameter management and output report management utilities. Tools may be run independent of the UI.

PACKAGE CONTENTS - Media Directory; Software Abstract; UCRL-MA-103440, Rev.5; UCRL-MA-118875; Media Includes Source Code, User's Guide, Executable Module, Auxiliary Material, Compilation Instructions;

SOURCE CODE INCLUDED? - Yes

MEDIA QUANTITY - 1 CD Rom

METHOD OF SOLUTION - Various methods are employed to assess the security posture of the UNIX operating system. Critical system and user files are tested for file access permissions, dates, ownerships, and other attributes. System services are examined using a combination of static method (inspection of the given service's configuration files) and dynamic methods (attempt to exploit the given vulnerability to confirm its presence).

COMPUTER - MLT-PLTFM

OPERATING SYSTEMS - UNIX

PROGRAMMING LANGUAGES - Standard C (95%), Bourne Shell Script (5%)

SOFTWARE LIMITATIONS - Disk space required is 7.5 MB during installation, 3.5 MB during routine use. SPI may run out of memory on large servers with small core memory.

PACKAGE ID - 000734MLTPL01 SPI/U3.2

SOFTWARE LIMITATIONS - (CONT)

SOURCE CODE AVAILABLE (Y/N) - Y

UNIQUE FEATURES - The CQL system is 4gl-like language for specifying varied and conditioned queries over the file, user, and group objects of UNIX system security. SPI generates both final reports suitable for viewing, and an intermediate machine readable format amenable to secondary and aggregated analysis. A report generator is provided for format conversion.

OTHER PROG/OPER SYS INFO - For security reasons, many data paths are fixed in the code during the installation (compiling) process. Therefore, SPI must be separately installed on each platform on which it is to be run. SPI output reports and cdt database archives may accumulate. These files should be purged manually as appropriate to the need and available disk space.

HARDWARE REQS - Computer running the UNIX operating system.

TIME REQUIREMENTS - Run time requirements depend highly upon computer load and the nature of the particular inspection being conducted. Many inspections are able to be completed within minutes. However, an extensive test of user passwords, employing large dictionaries, may take several hours. The QSP scan-disk process option requires about 10 minutes per GB of disk scanned.

REFERENCES - T. Bartoletti, S. Cooper, J. Fisher and S. Taylor, Security Profile Inspector for the UNIX Operation System (SPI/UNIX) User's Guide for SPI Version 3.2, UCRL-MA-103440, Rev.5, October 1994; T. Bartoletti, S. Cooper, J. Fisher and S. Taylor, Security Profile Inspector for the UNIX Operation System (SPI/UNIX) Reference Manual for SPI Version 3.2, UCRL-MA-118875, October 1994.

ABSTRACT STATUS - Submitted August 10, 1994. Released screened 4/14/95. Version 3.2 submitted 7/18/95. Released screened 7/21/95.

SUBJECT CLASS CODE - M

KEYWORDS -

COMPUTER PROGRAM DOCUMENTATION
S CODES
SECURITY
INFORMATION SYSTEMS
INTRUSION DETECTION SYSTEMS

EDB SUBJECT CATEGORIES -

990200 990300

SPONSOR - DOE/SA; DOD

PACKAGE TYPE - SCREENED