

PACKAGE ID - 000259IBMPC00 LAVA/CS

KWIC TITLE - Computer Security Risk Assessment

AUTHORS - Massagli, L.
Los Alamos National Lab., NM (United States)

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

COMPLETION DATE - 07/01/1987 **PUBLICATION DATE** - 06/25/1987

DESCRIPTION - LAVA/CS (LAVA for Computer Security) is an application of the Los Alamos Vulnerability Assessment (LAVA) methodology specific to computer and information security. The software serves as a generic tool for identifying vulnerabilities in computer and information security safeguards systems. Although it does not perform a full risk assessment, the results from its analysis may provide valuable insights into security problems. LAVA/CS assumes that the system is exposed to both natural and environmental hazards and to deliberate malevolent actions by either insiders or outsiders. The user in the process of answering the LAVA/CS questionnaire identifies missing safeguards in 34 areas ranging from password management to personnel security and internal audit practices. Specific safeguards protecting a generic set of assets (or targets) from a generic set of threats (or adversaries) are considered. There are four generic assets: the facility, the organization's environment; the hardware, all computer-related hardware; the software, the information in machine-readable form stored both on-line or on transportable media; and the documents and displays, the information in human-readable form stored as hard-copy materials (manuals, reports, listings in full-size or microform), film, and screen displays. Two generic threats are considered: natural and environmental hazards, storms, fires, power abnormalities, water and accidental maintenance damage; and on-site human threats, both intentional and accidental acts attributable to a perpetrator on the facility's premises.

PACKAGE CONTENTS - 2 NESC Notes; Software Abstract; LA-UR-86-2942;

SOURCE CODE INCLUDED? - Yes

MEDIA QUANTITY - 8 5.25 Diskettes

METHOD OF SOLUTION - The LAVA philosophy is based upon the use of a team approach for the vulnerability assessment segment. The quality of the assessment depends upon the breadth of the backgrounds and expertise of the team members. A vulnerability assessment takes a few days of preparation, two to four days of team discussions and interactions while answering the questionnaire, and a day to execute the scoring, print the report, distribute copies to team members, and discuss the results of the assessment. General summary reports for management personnel, as well as detailed reports for use by operations staff, are produced.

PACKAGE ID - 000259IBMPC00 LAVA/CS

METHOD OF SOLUTION - (CONT) The vulnerability scores are given both as quantitative values and linguistic descriptors and are combined with impact measures to provide useful measures of risk.

COMPUTER - IBM PC

OPERATING SYSTEMS - MS DOS or PC DOS 3.1. LAVA/CS has run successfully with versions 2.00 through 3.20

PROGRAMMING LANGUAGES - dBase III and Microsoft Quick BASIC

SOFTWARE LIMITATIONS -

SOURCE CODE AVAILABLE (Y/N) - Y

UNIQUE FEATURES - DISPLAY

OTHER PROG/OPER SYS INFO - The package contains a demonstration diskette to give the user the feel of performing a vulnerability assessment by answering a small subset of the questions. The LAVA/CS program is distributed in compiled dBASE III; consequently, dBASE III is not required for its use. The LAVA/CS SOURCE is supplied only upon request and completion of a special distribution release form.

HARDWARE REQS - LAVA/CS requires an IBM PC, IBM PC-XT, or compatible computer system with at least 512 Kbytes of memory, one flexible disk cartridge drive, and either a second flexible disk cartridge drive or a fixed/hard disk, with an IBM ProPrinter, Epson FX- 80 printer, or a compatible printer. 1.2 Mbytes of disk space are required to install LAVA/CS on the fixed disk.

TIME REQUIREMENTS - The demonstration requires approximately 15 minutes. Scoring the questionnaire takes approximately 1.0 to 1.5 hours to complete. The reports require a couple of hours to print.

REFERENCES - Suzanne T. Smith, Tracy Erkkila, Ray Leonard, David Martinez, Lynn Massagli, John Phillips, Mary Judy Roybal, Richard Tisinger, and Lance Waller, LAVA for Computer Security - An Application of the Los Alamos Vulnerability Assessment Methodology, LA-UR-86-2942, Release Version 1.01, 1987 with Errata-Rev. 1, June 25, 1987; LAVA/CS, NESC No.9579, Description of LAVA/CS Flexible Disk Cartridges, National Energy Software Center Note 88-14, November 29, 1987\ S. T. Smith and J. J. Lim, Framework for Generating Expert Systems to Perform Computer Security Risk Analysis, LA-UR-85-1933, submitted to the First Annual Armed Forces Communications and Electronics Association Symposium and Exposition on Physical and Electronics Security, Philadelphia, August 19-21, 1985; S. T. Smith, D. C. Brown, T. H. Erkkila, P. D. Fitzgerald, J. J. Lim, L. Massagli, J. R. Phillips, and R. M. Tisinger, LAVA - A Conceptual Framework for Automated Risk Assessment, submitted to

PACKAGE ID - 000259IBMPC00 LAVA/CS

REFERENCES - (CONT) Proceedings of the 27th Annual Meeting of the
Institute of Nuclear Materials Management, LA-UR-86-2282, June 1986.

ABSTRACT STATUS - Abstract first distributed November 1987. IBM PC
version of LAVA/CS submitted July 1987. IBM PC version of LAVA/CS
SOURCE submitted October 1987, made available upon special request
August 1988.

SUBJECT CLASS CODE - M

KEYWORDS -

COMPUTER PROGRAM DOCUMENTATION
L CODES
RISK ASSESSMENT
COMPUTERS
SECURITY
INFORMATION
SAFEGUARDS
VULNERABILITY
ADVERSARIES
THEFT
PHYSICAL PROTECTION
SABOTAGE
IBM COMPUTERS
PERSONAL COMPUTERS

EDB SUBJECT CATEGORIES -
990200

SPONSOR - DOE/AO

PACKAGE TYPE - SCREENED