



Vulnerability Analysis Project (VAP)

**Presented at the
19th DOE Computer Security Training
Conference
4/28/97 to 5/1/97
Houston, TX**

by

**William J. Orvis
VAP Project Leader, LLNL
(510) 422-8649 or orvis@llnl.gov
UCRL-MI-123880 Rev. 1**

Work performed under the auspices of the U.S. Department of Energy by Lawrence
Livermore National Laboratory under Contract W-7405-Eng-48



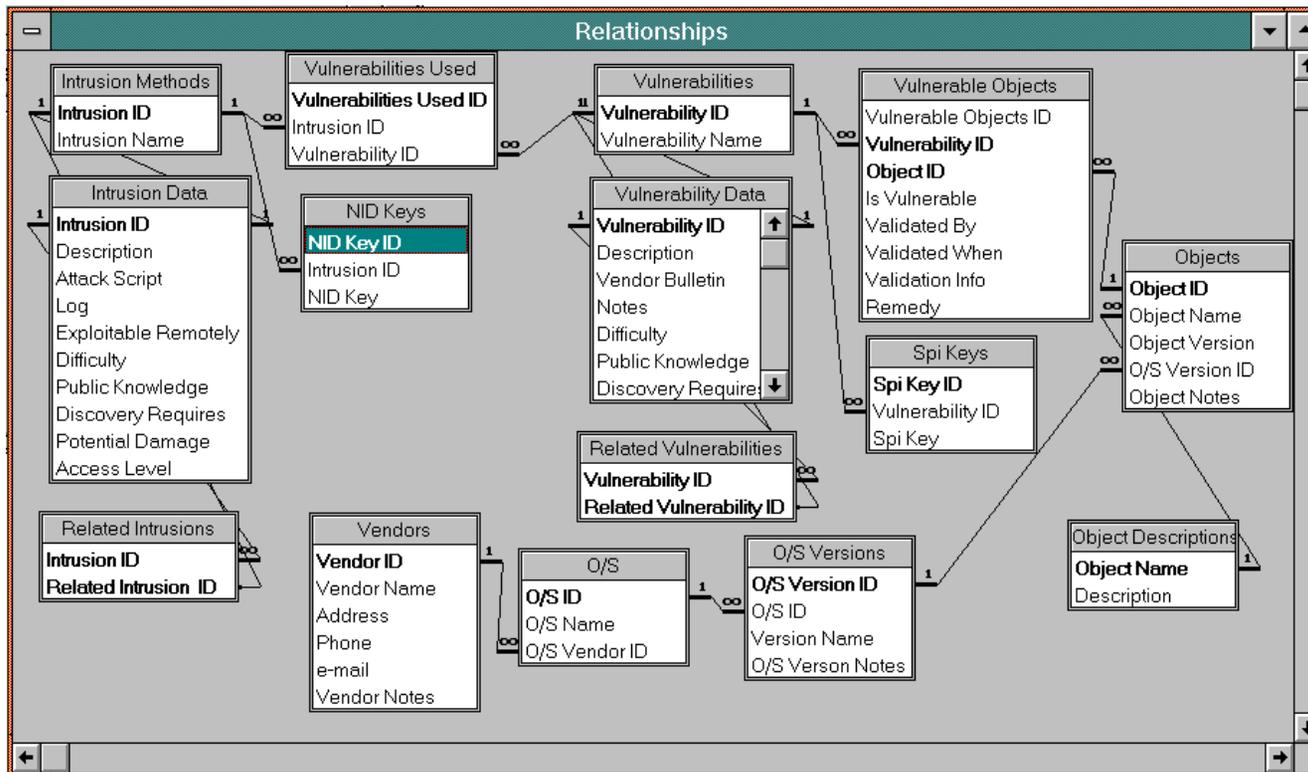
What is VAP?

Vulnerabilities in modern computer systems and networks make it possible for unauthorized people to subvert security for malicious purposes. Systems today have many such vulnerabilities, with more being discovered daily.

- ❖ **VAP is a project to identify and catalog computer system vulnerabilities in a framework that can be used both for analysis of vulnerabilities and for incident response.**
- ❖ **VAP data structures are being coordinated with other response teams.**
- ❖ **VAP will be accessible to DOE security managers.**



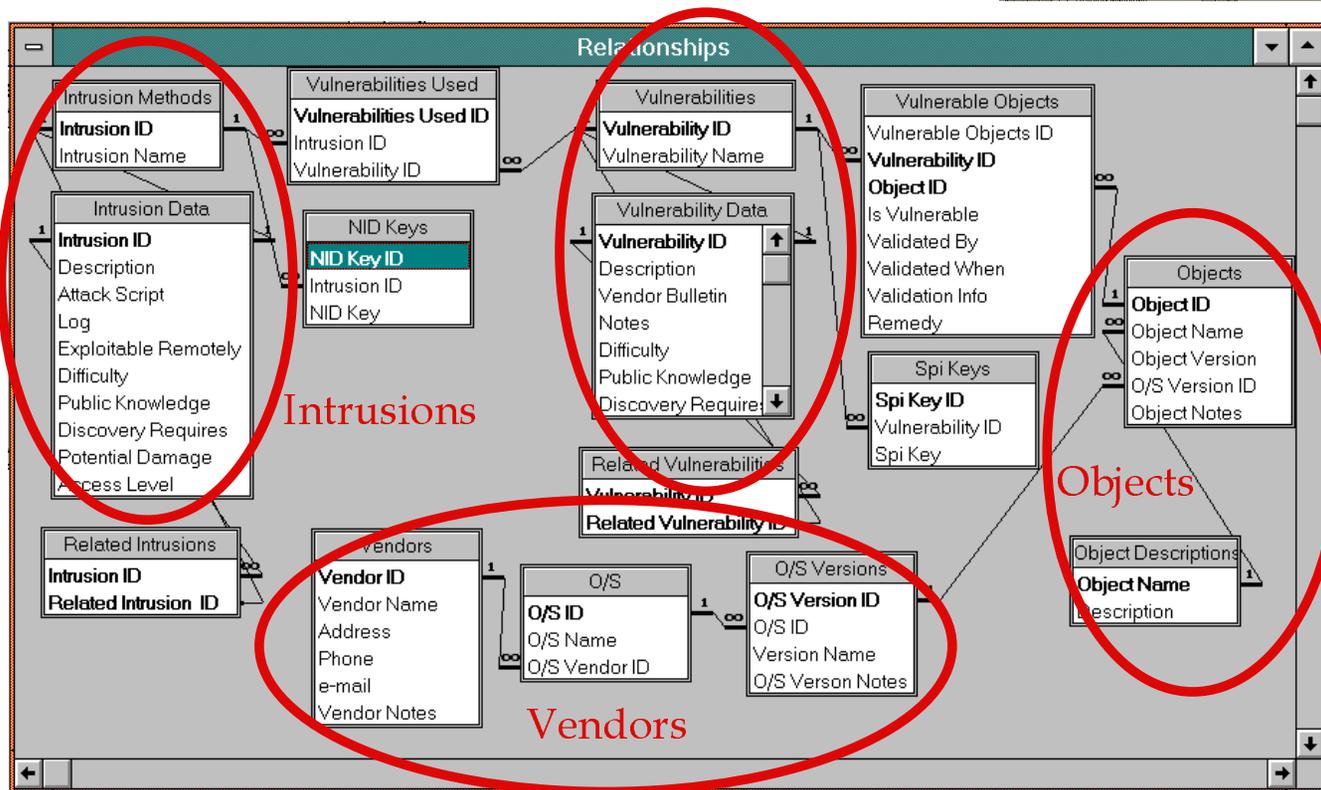
VAP Uses A Relational Database



The Design Partitions the Information Into Four Distinct Parts



Vulnerabilities





First: Vendor Information

- ❖ The vendor information form links the vendors of the computer software with the particular operating systems and version numbers.

Vendors

Vendors

Vendor Name: SUN Microsystems, Inc

Address: 2550 Garcia Avenue MPK03-208 M

Phone: (415) 688-9151 e-mail:

Vendor Notes: FIRST: Mark Graff
Phone: (415) 688-9151
STU!!!: (415) 321-9259

O/S O/S Name: SunOS

O/S Versions Version Name: 4.0.3

O/S Ver. Notes:

Record: 1 of 11

Record: 1 of 11

Record: 5 of 11

Second: Objects

- ❖ The objects are the files or other structures that contain the flaw that allows the vulnerability to occur.

Objects link vendors to vulnerabilities

Objects

Object Name: /private/etc

Object Version: 73

O/S Version

UNICOS	6.0
UNICOS	6.1
UNICOS	UNICOS
BSD	4.3
BSD	BDS
NeXTStep	1.0

Object Notes: Sys 1.0 and /etc/group and /private/etc

Object Description: The directory /private/etc is supposed to be a private directory by default.

Record: 1 of 23

Third: Vulnerabilities

- ❖ **Vulnerabilities show how to exploit the flaw in the object. They also contain patch and risk information.**

The screenshot shows a web-based interface for managing vulnerabilities. The title bar reads 'Vulnerabilities'. Below the title bar are 'New' and 'Save' buttons. The main form contains the following fields:

- Vulnerability Name:** Sendmail direct deliver to file
- Access:** All (dropdown menu with options: Sensitive, Cray)
- Vendor Restricted:**
- Description:** This vulnerability allows a hacker to use sendmail to login to another user's account without password. A hacker can append his username to the victim's .rhost file by sending an electronic mail message directly to
- Vendor Bulletin:** SUN bug#1028173
- Vulnerable Obj Notes:** Recent versions of UNIX systems other than SunOS contains a sendmail fix. CIAC encourages you to consult with your vendor about this problem.
- Difficulty:** Shell Script (dropdown menu with options: N/A, Shell, Shell Script, C, Difficult C, Kernel)
- Public Knowledge:** Occasionally Seen (dropdown menu with options: N/A, Theoretical, Never Seen, Occasionally Seen, Common, Rampant)
- Discovery Requires:** Access to Protocol (dropdown menu with options: More than distribute, Source Code, Advanced Distribut, Standard Distribut, Access to Protocol, Public Access)
- Change Log:** On March 14, 1996, this entry was made. GHK

At the bottom, there is a table for 'Vulnerable Objects':

Object	Version	O/S	Version
/usr/lib/sendmail	66	SunOS	5.3

At the very bottom, there is a 'Delete Object' button and a status bar showing 'Record: 1 of 23'.

Fourth: Intrusions

- ❖ Intrusions show how to exploit the vulnerabilities to gain unauthorized access. Intrusions also contain risk information.

The screenshot shows a window titled "An Intrusion" with a tab labeled "Intrusions". The window contains the following fields and controls:

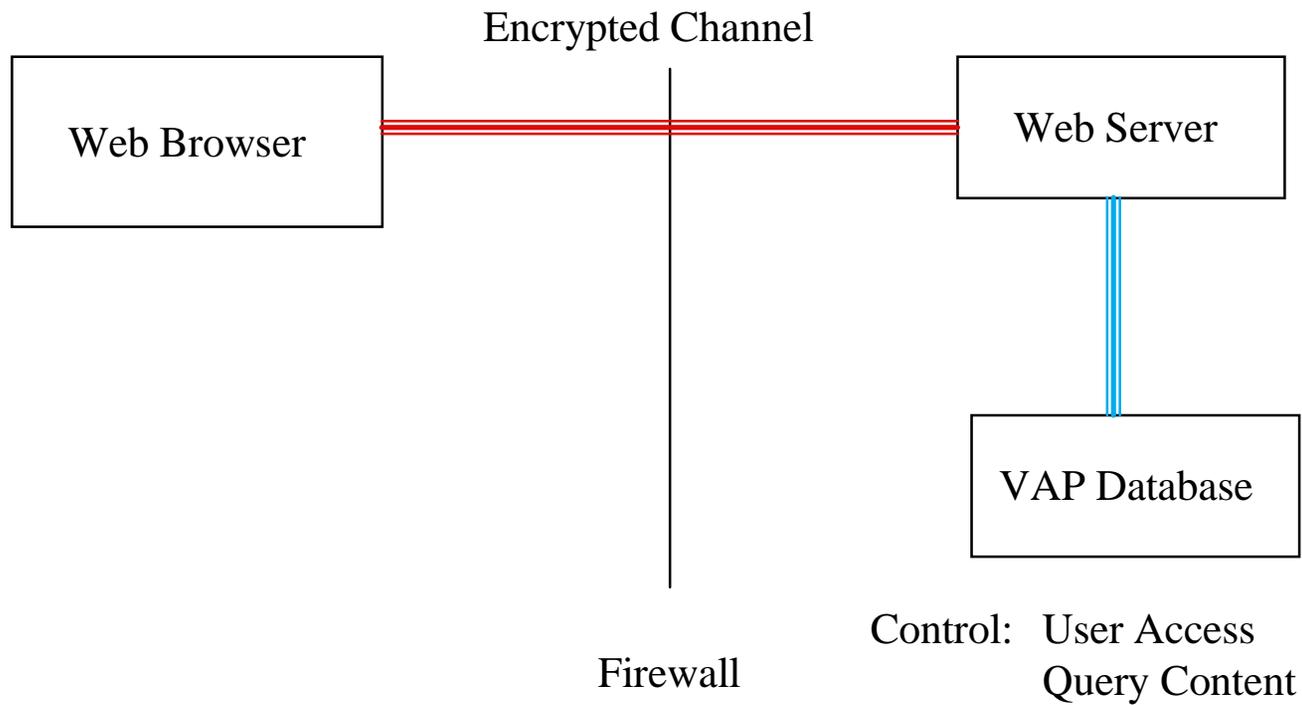
- Intrusion Name:** Bugs in 4.3BSD UNIX
- Access:** All (dropdown menu with options: Sensitive, Cray)
- Exploitable Remotely:**
- Description:** Several bugs exist in the operating system. For details, obtain the files from the UC system at "ucbarpa.berkeley.edu".
- Attack Script:** Depends on particular bug.
- Log:** This information was obtained on June 12, 1991.
- Difficulty:** N/A (dropdown menu with option: Shell)
- Public Knowledge:** Occasionally Seen (dropdown menu with option: Common)
- Discovery Requires:** Advanced Distribut (dropdown menu with option: Standard Distribut)
- Potential Damage:** Damage depends on the particular bug.
- Vulnerabilities Used:** Bugs in 4.3BSD UNIX | 11 | 35

Buttons: New, Save, Open Vulnerability, Delete From Used

Footer: Record: 1 of 23



External Access Will Use A Secure Web Server





Initial External Access Will Be Site Security Managers

- ❖ **Site security managers as defined by Phil Sibert's database.**
- ❖ **As the database of site security personnel goes online, the site security managers will be able to update/change the list of computer security personnel. One option will be to allow access to the VAP database.**
- ❖ **Access to the database will be allowed as soon as the policy is completed.**



External Access Will Be Through A Series Of Canned Queries

- ❖ **Vulnerabilities given a vendor or O/S.**
- ❖ **Vendors and O/S given a vulnerability.**
- ❖ **Vulnerabilities and O/S given an object.**
- ❖ **Objects and O/S given a vulnerability.**
- ❖ **Other queries as requested by the users.**



VAP Is A New Security Resource

- ❖ **It will be available soon to DOE security managers.**
- ❖ **They will be able to search for vulnerabilities by name, system type, and other criteria.**
- ❖ **Access will be via a browser that supports the secure socket layer (SSL) protocol.**
- ❖ **Access to users outside of this group will be on a case by case basis. Users must agree to adhere to our policies.**