



# *Computer Security Technology Center*

**SSDS - Secure Software Distribution System**

**by**

**Lauri Dobbs**

**SSDS Project Leader, LLNL**

**(510) 423-8590 or e-mail [dobbs1@llnl.gov](mailto:dobbs1@llnl.gov)**

**sponsored by**

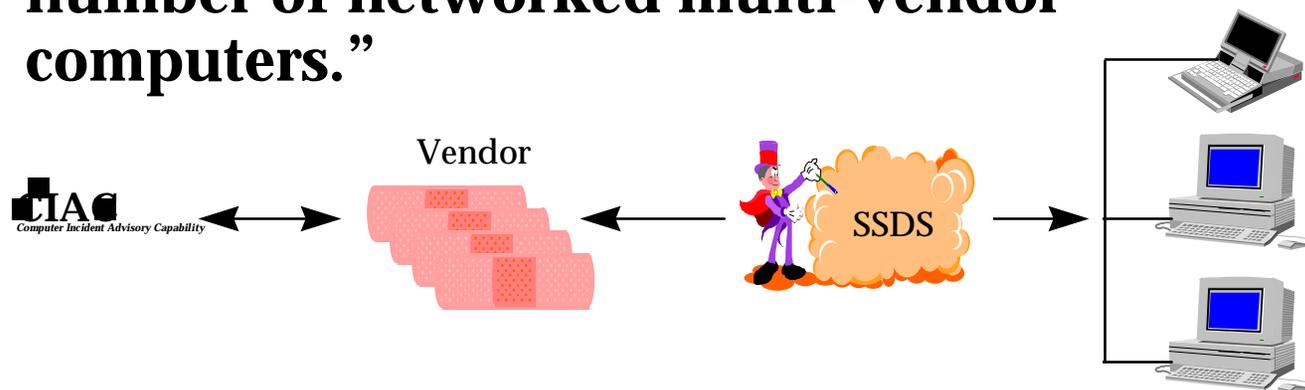
**DOE Energy Research**

**This work was performed under the auspices of the U.S. Dept. of Energy at LLNL under contract no. W-7405-Eng-48.**

**UCRL-MI-127241**

# The Goal of SSDS

**“To provide an automated means to rapidly evaluate, distribute, and install software security patches in a secure fashion on a large number of networked multi-vendor computers.”**



## Results:

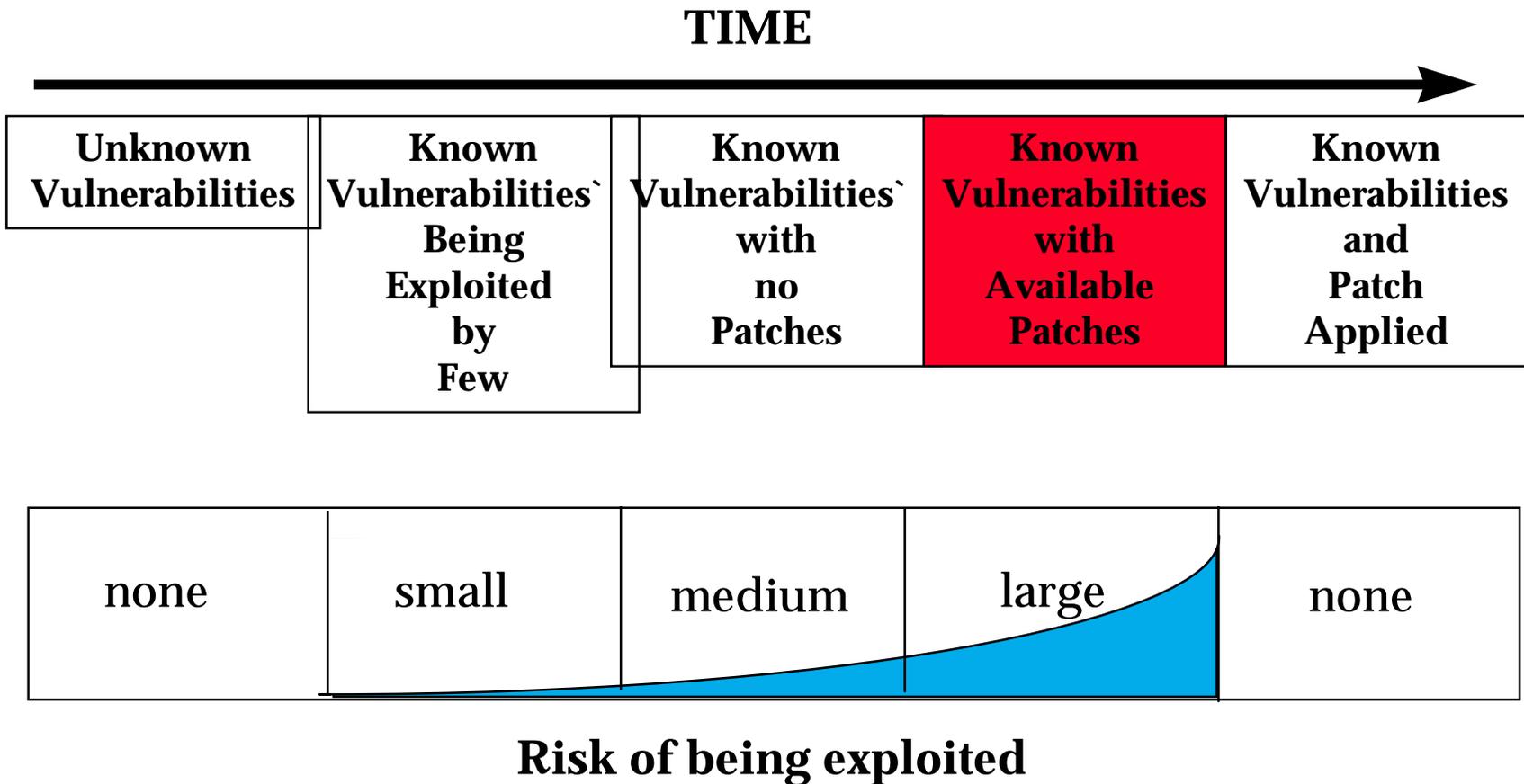
**Greatly enhanced system security and integrity.**



# ***SSDS Motivation***

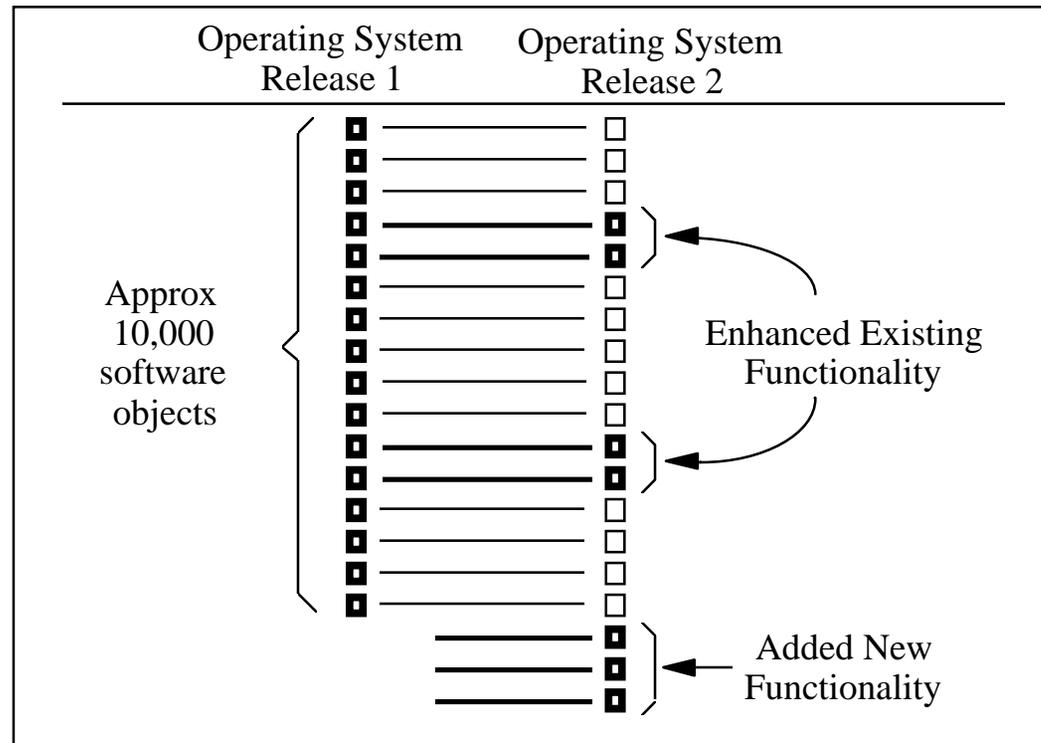
- ❖ **Maintenance of computer systems is a significant portion of the cost of ownership. SSDS reduces the this cost by providing transparent system administration.**
- ❖ **Multi-vendor computing environments are the norm not the exception. SSDS is vendor independent: it will work with any vendor's computing systems.**
- ❖ **System administration is labor intensive and requires specialized knowledge. SSDS leverages the skills and time of system administrators.**
- ❖ **Networked computer systems are vulnerable to viruses, trojan horses, and other malicious software. SSDS provides a comprehensive mechanism to evaluate and validate system's software of networked computers.**

# Software Vulnerability Timeline





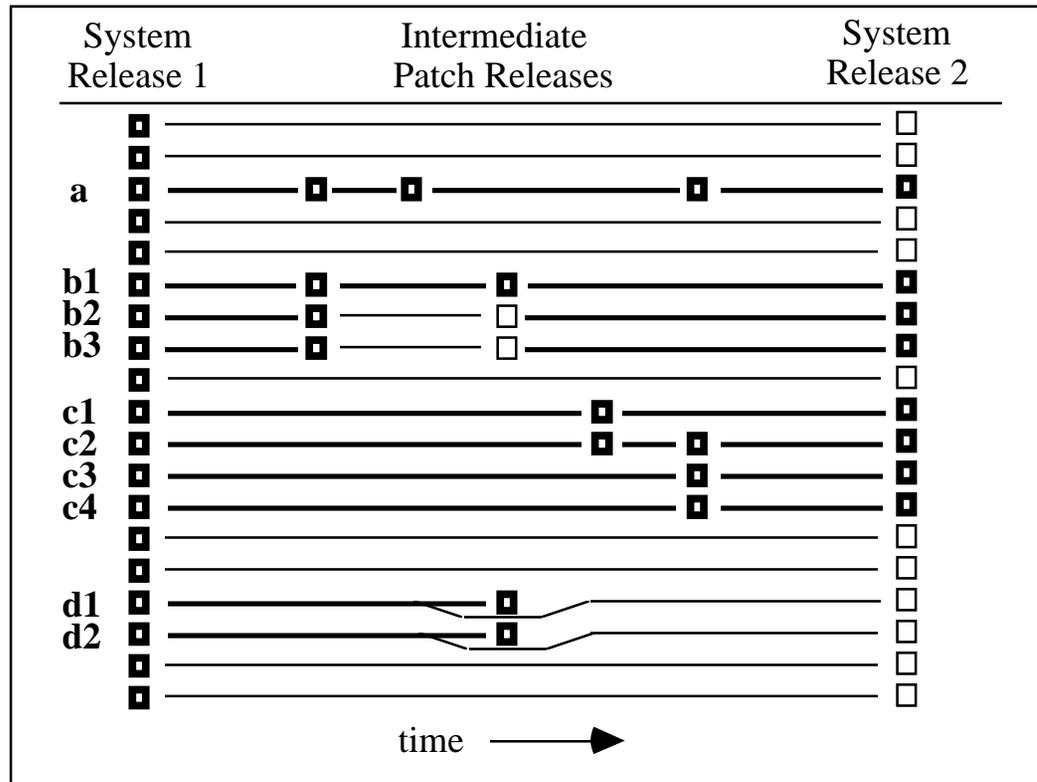
# Operating System Upgrade



**Hundreds of software modules added or modified**



# Upgrades - The Ugly Reality



**Patch conflicts and contingencies abound**



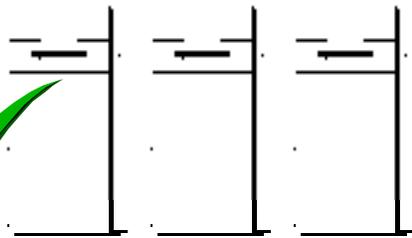
# ***SSDS Objective***

**A centralized service providing intelligent and flexible automation in ...**

- ❖ Notification of new vendor security patches**
- ❖ Determination of patch applicability**
- ❖ Installation of security patches/software**
- ❖ Ability to cleanly “back-out” patches/software**
- ❖ Rapid site-wide patch status metrics and queries**

**with authenticated and data-protected connections to the target systems.**

# SSDS Approach



- + Secure communications.
- + Largely automated process.
- + Flexibility to configure to your environment.
- + Cost effective solution.

Monitor Vendor's sites for the latest patches and store them in a *non-vendor specific* format.

Evaluate untrusted target systems on a scheduled basis and install patches as needed.



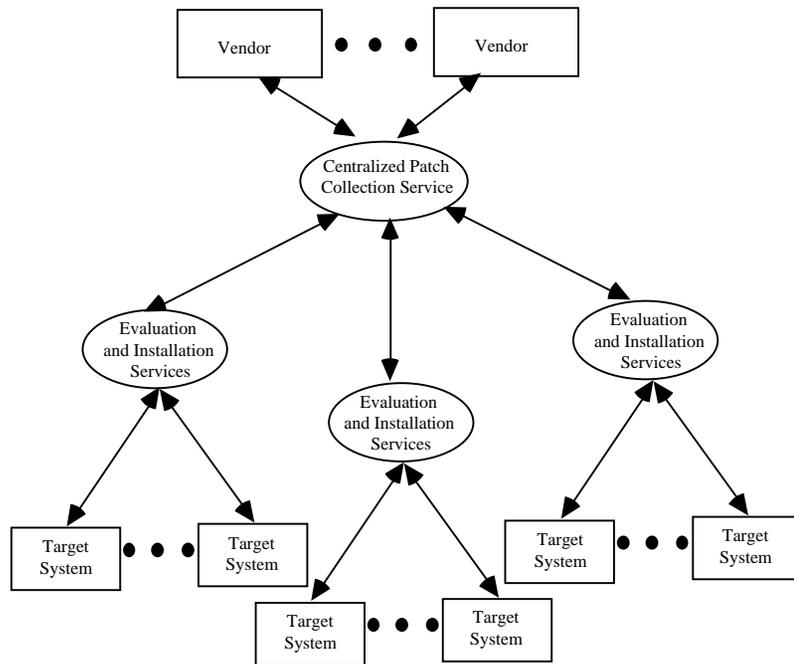


# ***SSDS Advantages***

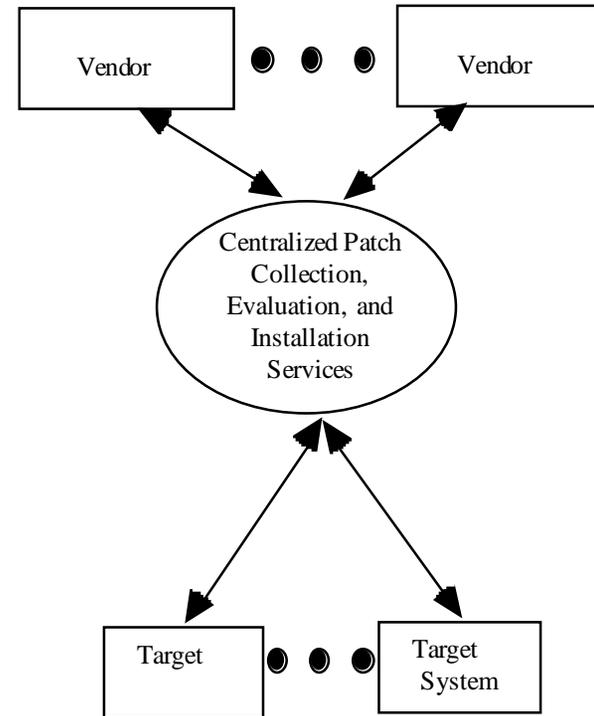
- ❖ **Centralized service.**
- ❖ **Largely an automated process.**
- ❖ **Flexible to fit any environment.**
- ❖ **Vendor independent.**
- ❖ **Ensures the integrity of the system software.**
- ❖ **The price is right!**

# SSDS Fits Any Environment

❖ Many networks and hundreds of computers.



❖ One network and few computers.

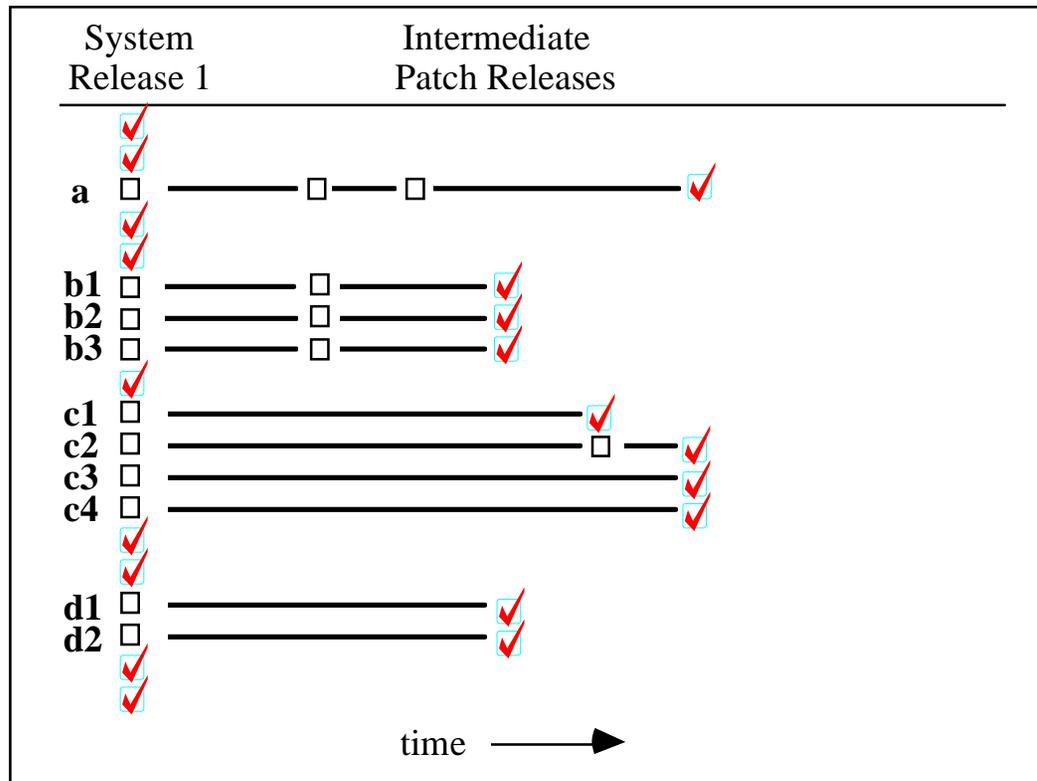




# ***SSDS is Vendor Independent***

- ❖ **Vendor's patches are converted to a standard machine-readable patch format.**
  - **We are starting to work with the vendors to adopt a patch standard format.**
  
- ❖ **SSDS is implemented in Java.**
  - **"Write once, Run anywhere."**
  - **Tested prototype on Sun Solaris.**
  - **Test on other UNIX flavors when Java 1.1 is released.**

# SSDS Ensures the System Software Integrity



Obsolete

Latest release



## *Where are we today?*

- ❖ **Completed a proof-of-concept prototype.**
  - Detect patch deficiencies on Sun systems running Solaris 2.3 and higher.
  - Report patches needed to be installed and what is currently installed.
- ❖ **Developed a machine-readable patch specification format.**
- ❖ **Developed a prototype interface for managing SSDS.**



## ***What are we working on now?***

- ❖ **Building a complete history of Sun Solaris patches.**
- ❖ **Distribute SSDS prototype to alpha users by October 1997.**
- ❖ **Develop tools to monitor and collect Sun patches.**
- ❖ **Broaden range of vendor systems to HP and Digital.**
- ❖ **Address secure communications between networked processes.**
- ❖ **User documentation.**



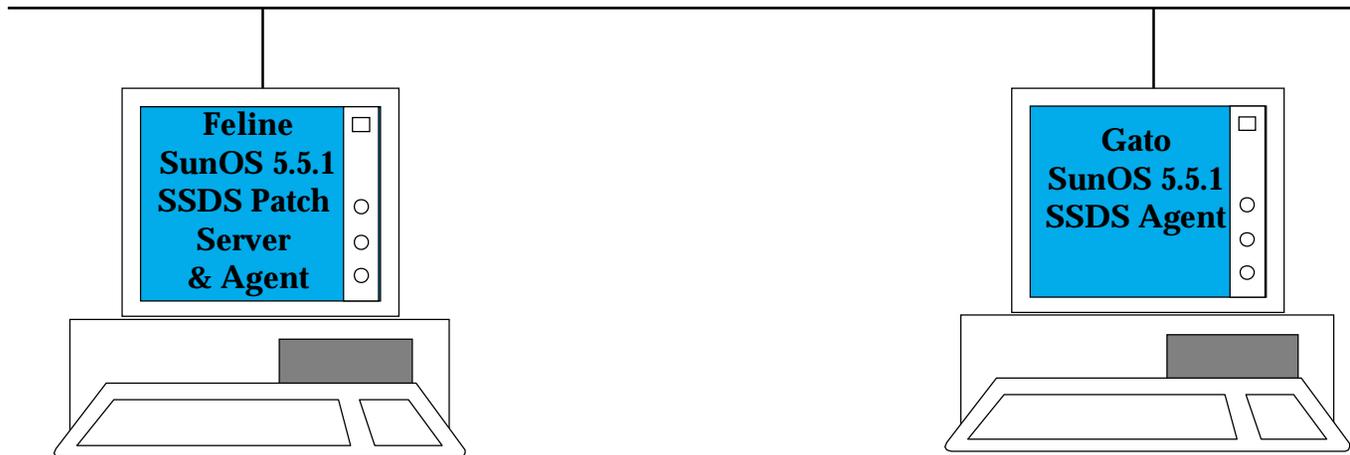
## *Where are we headed?*

- ❖ **Automated** installation of patches.
- ❖ Ability to “back out” installed patches.
- ❖ Develop tools to monitor and collect patches from other major UNIX vendors.
- ❖ **Broaden range of patch types to include:**
  - Patches that require editing of configuration files.
  - Patches that replace objects in run-time libraries.
  - Kernel patches.



## Patch Database

102971-01 SunOS 5.5 vipw fix  
103300-02 SunOS 5.5 OpenWin 3.5 ff.core  
103468-01 SunOS 5.5 statd problem  
103279-02 SunOS 5.5 nscd breaks password shadowing with NIS+  
103279-02 SunOS 5.5 rdist suffers from buffer overflow  
103696-01 SunOS 5.5.1 /sbin/su patch  
103686-01 SunOS 5.5.1 rpc.nisd\_resolv rebuild for BIND 4.9.3  
103817-01 SunOS 5.5.1 rdist suffers from buffer overflow  
103680-01 SunOS 5.5.1 nscd/nscd-nischeck rebuild for BIND 4.9.3  
000001-01 SunOS 5.5.1 TEST PATCH



**Patch 000001-01 installed**

**All SunOS 5.5.1 patches not installed**

- **Install patch 000001-01**
- **Trojan object foo of patch 000001-01**