GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Practical Assignment Version 1.4b

Trusted Operating Systems and Their Evolving Non-Trusted Counterparts

Stephen Radford

January 23, 2003

Long ago, in a place far away, operating systems were open…wide open. When the customer received a new system from a vendor, most security was turned off. Only the bare bones required security mechanisms were implemented. Along came the crackers, and the government, and suddenly there was an outcry for security….lots of security. The outcry resulted in "Trusted Operating Systems". However, trusted operating systems were VERY well secured to the point of being almost unusable. Now what? How about a "middle ground"…operating systems that are well secured but usable?

This paper will address the lax security common before the age of crackers. Characteristics of trusted operating systems and the problems that make them difficult and expensive to use will then be discussed. Specific trusted operating systems will be reviewed as well as a trusted Webserver. Finally we will look at what vendors are doing today to provide the consumer with "non-trusted" operating systems that are incorporating many of the same security features found in their "trusted" counterparts.

The Good Old Days

Most computer vendors ship new systems with a pre-installed operating system. The intent of the "pre-install" is to get the user up and running as quickly as possible, with as little hassle as possible since most Sales and Marketing departments proclaim that their systems are quick and easy to install as well as easy to learn and use.

Traditionally, only the most essential security mechanisms were implemented in the default "pre-install". Passwords were not required and if used, there were no limitations on length or content of passwords. Even the "all-powerful" root user was not required to be password protected. Quite often, the users used their name or user id as their password. Often the password was posted on the keyboard or monitor. Administrators commonly used the system name or an easily guessable password such as "system" or "password" as the root password. It was not at all unusual to see the system root password taped to the system console.

File security was very basic: read, write, and execute permissions for owner, group, and others. Files such as *.rhosts* and *hosts.equiv* were in widespread use to ease system administration and general use of the systems. Security patches

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

were available yet install of the patches was not given proper attention by vendors or system administrators.

System security logging was poorly utilized…if utilized at all. When utilized, there was no simple, user-friendly method of reviewing the logs therefore possible security breaches could be overlooked.

Likewise, the network interface for computers was not well secured. Software firewalls and host intrusion detection software on the computer were non-existent. Communications between computers were transmitted in cleartext. Shared or exported filesystems were mountable by anyone with access to the network.

With the prevailing lack of emphasis on security, it was quite easy for an intruder to break into a system and acquire confidential data or steal computer-processing resources. Fortunately, there were very few intruders. As the number of intruders, or crackers, increased during the 1980's, changes in the way vendors and users looked at computer security became necessary.

Trusted Operating Systems

As the numbers of attacks began to rise, researchers began to look at ways to better protect systems. In the early 1980's, the concept of the "Trusted Operating System" was developed. "Trusted" is a term coined by the United States Government to apply to systems capable of securely handling classified materials. In 1984, National Security Agency first evaluated and approved trusted operating systems.[2] Trusted operating systems are distinguishable by the following characteristics.

- Mandatory Access Control – Access Control Lists are used to control what users or processes are allowed to do. Access Control Lists are lists of users or groups and what permissions they have for various files or directories. Access Control works on the concept of least privilege…if access is not specified, then it is denied. Not only is the initial call to a privileged system function validated, but also each subsequent call is re-verified. System services can be compartmentalized and only certain users or applications can access them.

- Concept of least privilege – This concept works hand-in-hand with mandatory access control. Activities that a process can perform are limited to what is required to accomplish the task. This concept can be applied to files and directories also. Only users, groups or processes requiring access, get access. Moreover, those users, groups and processes only get the bare minimum privilege needed to accomplish the required task.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Auditing – All suspicious activities are logged. These activities include, but are not limited to, access violations, logins/logouts, and unsuccessful network connections.

- No “all-powerful” administrator – Administrative functions are divided among users limiting the damage if an attacker breaks the super user account, certain sensitive functions may require actions by multiple users and/or the entry of an activity password. Privileges can also be controlled according to which device the administrator logs in to. For example, logon to a local device may be required rather than access from the network or a dialup connection.

- Kernel level enforcement - Security decisions are made at a low level where users or applications cannot interfere with them.

- Evaluation - Security evaluation is performed by an independent laboratory such as the National Institute of Standards and Technology, the United States Department of Defense National Security Agency, and the National Information Assurance Partnership, which is a collaboration between the National Institute of Standards and Technology and the National Security Agency.

The above characteristics make a system very difficult to penetrate yet there is a price to pay for the increased level of security. As described above, relatively simple system functions on a non-trusted operating become much more difficult in a trusted environment. For example, in a non-trusted environment, the root user simply enters a command to add the user, then another command to set the user’s password. In a trusted environment, adding a user may require two administrative users to enter commands and a user addition activity password may be required. Administrators must be retrained in the new processes. Productivity will suffer during the learning curve. Access Control Lists must be setup and implemented. Additional personnel may be required to perform the increased administrative workload.

In many cases, the trusted operating system is more costly to purchase than the standard operating system. Sun Solaris is an example of this pricing model. The standard Solaris operating system is essentially free whereas Trusted Solaris cost several thousand dollars per processor.

Because of the issues above, trusted operating systems are not suitable for all computing environments. Trusted operating systems are best used in situations where security is essential such as financial or military environments. Health care environments could also be appropriate due to the legal ramifications of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Trusted Operating System Product Offerings

Several computer vendors have produced Trusted Operating Systems. Each of these companies has implemented “trust” in their own way and market their version based upon its strengths. However, each must include the characteristics of the trusted operating system discussed above.

Sun is the producer of Trusted Solaris. The current shipping version is Trusted Solaris 8. Trusted Solaris 8 is a superset of standard Solaris 8 with a similar look and feel. Although a different kernel from Solaris 8, Trusted Solaris 8 is based upon the same code base with security extension. Trusted Solaris 8 is offered on both Sparc and Intel processors. Sun touts Trusted Solaris 8 as a significant improvement of previous trusted versions of Solaris. Trusted Solaris 8 is easier to administer and applications do not require recompiling before use. Trusted Solaris 8 provides security in both the operating system and the windowing system. Trusted Solaris 8 is certified at the United States Department of Defense National Security Agency Trusted Computer Security Evaluation Criteria (Orange Book) B1 security level “out of the box”.

Some features of standard Solaris are not included in Trusted Solaris 8. Although all standard desktops are supported, only CDE (Common Desktop Environment) supports the trusted windowing system security capabilities. Remote file systems cannot be mounted during installation. Upgrade installations are not supported in Trusted Solaris 8. In addition, Solaris Web Start installations are not supported in Trusted Solaris 8.

Sun’s goal is to release a “trusted” version of a release within six months of the same “standard” version of the release. The trusted release is actually ready much sooner than six months, but the certification process for the trusted version adds to the lag between standard operating system release and trusted operating system release.

As noted earlier, trusted operating systems come with a price. In the case of Solaris, part of the price is financial. Whereas standard Solaris is provided at only the cost of the media, the cost of Trusted Solaris varies from approximately $2,500 to around $12,000 depending on the number of processors on the installed system.[9]

Silicon Graphics offers Trusted IRIX 6.5, which is based on SGI’s standard IRIX 6.5. Trusted IRIX 6.5 is evaluated by the National Information Assurance Partnership's Common Criteria Evaluation and Validation Scheme to conform to National Security Agency Information Systems Security Organization’s Labeled Security Protection Profile, which corresponds to the Trusted Computer Security Evaluation Criteria B1 security level.[5] Trusted IRIX 6.5 includes the features of a “trusted” system listed above such as mandatory access control, concept of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

least privilege, auditing, no “all-powerful” administrator, kernel level enforcement and security evaluation.

TrustedBSD is a work in progress offered by the FreeBSD Foundation. It is an extension to the FreeBSD code to incorporate the trusted operating system characteristics defined above.[6] TrustedBSD is supported at least partially or is targeted for support on a variety of processor platforms including Intel x86, Compaq Alpha, Intel IA-64, SGI MIPS, Apple PowerPC, Sun UltraSPARC, and AMD x86-64.[7]

Hewlett-Packard offers HP Virtualvault as a trusted Webserver. Unlike general-purpose trusted operating systems, which can support various applications, Virtualvault is designed to support web applications only. The Apache Webserver is built upon the HP Virtualvault Operating System 11.04. Virtualvault Operating System 11.04 is a security enhanced, binary compatible version of HPUX 11.0, which meets security level B1 of the National Security Agency Trusted Computer Security Evaluation Criteria.

Hewlett-Packard’s marketing arm advertises Virtualvault as an “entire DMZ in one box”.[4] Virtualvault’s operating system supports standard trusted operating system features such as mandatory access control, the concept of least privilege and audit trails. As is required in a trusted environment, the powers of the traditional Unix root user have been eliminated, replaced by fifty distinct privileges, which can be independently assigned to different users thus limiting the damage, which can be done if an administrative user is compromised. Each user or process is only assigned privileges needed to accomplish specific tasks in accordance with the concept of least privilege. Audit trails and alarms can be customized using Hewlett-Packard’s Openview product. HP Virtualvault attempts to ease the administrative burden by adding a Netscape Navigator interface to ease administrative tasks.

As noted above, Virtualvault is a secure web server utilizing a partitioned web runtime environment. Data partitioning separates intranet applications from the front-end accessible to the Internet. All files and programs are placed in one of the following compartments:

- System – contains system files and html files
- Inside – contains databases, CGI programs, Java Virtual Machine, and middleware servers
- Outside – contains the Webserver

Privileges are required to communicate between compartments. The Trusted Gateway Proxy receives all Internet requests and forwards valid data therefore applications do not have to be redesigned for security.[4]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Security Enhancements for Standard Operating Systems

We have established that trusted operating systems vastly improve security yet due to resulting cost, complexities, and overhead, are not appropriate for all applications. So what about the rest of the world? How do we improve the security of systems that are not conducive to trusted operating systems? Most vendors are addressing security issues in their standard product offerings. Vulnerabilities are being addressed not only in product releases but also in the emphasis vendors are now placing on correcting security vulnerabilities found after release of the product.

Sun's latest standard operating system, Solaris 9, includes significant security enhancements over previous standard Solaris releases including:

- A firewall which Sun touts as "commercial grade"
- A version of Secure Shell which supports SSHv1 and SSHv2 protocol versions
- Internet Key Exchange (IKE) protocol to automate key management for IPSec
- Kerberos Key Distribution Center (KDC) and Administrator Tools for authentication, privacy and integrity
- NFS security improvements with the addition of Kerberos V5
- Kerberos password aging and interoperability with MIT Kerberos and Windows 2000
- Communication encryption enhancement by replacing Solaris Encryption Kit CD-ROM with Kerberos V5
- LDAP client-based security
- Secure IPv6 datagrams between machines
- Role-Based Access Control
- Encrypted connections for Xserver
- A Generic Security Services Application Programming Interface allowing the programmer to better secure applications

Considering Sun's goal of releasing a trusted operating system version within six months of the release of the corresponding standard operating system version, Trusted Solaris 9 should be available soon.[17]

SGI has addressed various aspects of security in their latest standard offering, IRIX 6.5. IRIX 6.5 has been evaluated according to the National Information Assurance Partnership's Common Criteria Evaluation and Validation Scheme to conform to the National Security Agency Information Systems Security Organization's Controlled Access Protection Profile. The requirements defined in the Controlled Access Protection Profile are consistent with the C2 security level specified by the National Security Agency Trusted Computer Security Evaluation Criteria.[5]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Hewlett-Packard's latest standard offering is HPUX 11i. Like SGI IRIX 6.5, HPUX 11i is certified to conform to the National Security Agency Information Systems Security Organization's Controlled Access Protection Profile, or Trusted Computer Security Evaluation Criteria security level C2. HPUX 11i security enhancements include:

- Stateful firewall software – IPFilter/9000
- Secure IP - IPSec/9000 (Supports AES, DES and 3DES encryption)
- Kerberos server
- Secure shell - SSH-1 or SSH-2 protocols
- Host intrusion detection software – IDS/9000
- AAA server – RADIUS support
- Stack buffer overflow protection
- A security hardening/lockdown tool - Bastille HP-UX
- Cryptographic hardware support
- Security patch check – Perl script [3]

The latest standard operating system release from the FreeBSD Foundation is FreeBSD 5.0. FreeBSD 5.0 includes support for the same Mandatory Access Control facility found in TrustedBSD. The software is considered "experimental" and is not enabled by default. Also included is experimental hardware cryptographic acceleration. As with Mandatory Access Control, this feature is not enabled by default. As with TrustedBSD, FreeBSD is supported at least partially or is targeted for support on a variety of processor platforms including Intel x86, Compaq Alpha, Intel IA-64, SGI MIPS, Apple PowerPC, Sun UltraSPARC, and AMD x86-64.[7]

OpenBSD is an interesting player in this discussion. Although it is not "certified" as a "Trusted Operating System", it includes many of the features previously mentioned as features of trusted operating systems. OpenBSD is coded by volunteers led by Theo de Raadt. From its beginnings, the emphasis in OpenBSD has been security rather than functionality. Therefore, many features that other Unix variants include are not available in OpenBSD. This limits the usefulness of OpenBSD, but in specific situations, it can be quite valuable. These situations include the applications previously listed for trusted operating systems such as government environments. It is also quite useful running firewalls or data warehousing applications. Although it has many uses, OpenBSD would not be the best option for the desktop.[12]

OpenBSD is supported on Digital Alpha-based systems, Hewlett-Packard HP 9000 Series 300 and 400 workstations, standard PC and clones based on the Intel i386 architecture and compatible processors, Motorola 680x0-based Apple Macintosh with MMU, Apple PowerPC-based machines, Motorola 680x0-based VME systems, Sun SPARC and UltraSPARC systems, and Digital VAX-based systems. Porting efforts are underway for Hewlett-Packard Precision Architecture

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

(PA-RISC) systems and Motorola 881x0-based VME systems. Ports for IBM RT/PC systems and SGI MIPS-based workstations may be forthcoming.[13]

Another interesting player in the discussion is SELinux (Security Enhanced Linux). SELinux is a Linux security module created with participation by the National Security Agency. It can be integrated almost seamlessly into the Linux operating system. SELinux implements Mandatory Access Controls. The result is a more secure system that provides binary compatibility with existing Linux applications.[8]

Microsoft, long criticized in the security arena, is also expressing increased concern in the security realm. A new initiative code-named Palladium is a combination of security components to be built into not just the Windows operating system but also into hardware. The initiative, still in its early stages, is a push towards security standards in both hardware and software. Microsoft is partnering with hardware vendors including AMD and Intel. One of the features of Palladium is a security chip providing a set of cryptographic functions. A goal is to isolate trusted code from the rest of the system to protect it from destructive software. Another goal is to allow the user to determine what information about the user or their hardware to reveal to the network world. Software agents utilizing cryptography can be used to deploy secure services.[16]

Microsoft representatives state the following of Palladium:

"When combined with a new breed of hardware and applications, these features will give individuals and groups of users greater data security, personal privacy, and system integrity. In addition, Palladium will offer enterprise customers significant new benefits for network security and content protection."[16]

Microsoft Palladium is not welcomed by everyone though. Some in the computing world are concerned that this is an attempt by Microsoft to gain more control by creating a proprietary computing environment. Some regard trusting Microsoft with security is similar to the proverbial fox guarding the hen house. In spite of their fears, many users believe that Microsoft's Palladium will succeed based not on technical merit but on marketing power.[15]

Where Do We Go From Here?

Operating system security will continue to evolve. The security gap between the trusted operating system and the standard operating system will narrow and eventually cease to exist as standard operating systems incorporate the features that currently make an operating system "trusted". The price of security, from initial license fee through administrative training and headcount, will be accepted as normal. Although this will be a significant change from the open systems and networks of fifteen to twenty years ago and even the improved security of today, this will become the norm due to the consequences of insecurity. The

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

cybersecurity landscape has changed immensely over the past twenty years and operating systems must also change.

It must be noted that not even the most secure operating systems will prevent all security breaches. Users can still post even the best passwords on their monitor or keyboard. Nevertheless, a combination of a secure operating system and well-defined security practices can greatly enhance the security of a computing environment.

Citation of Sources

[1] Scheier, Robert L.. Trusted Operating Systems: The Ultimate Defense. Computerworld. November 6, 2000. http://www.computerworld.com/securitytopics/security/story/0,10801,53293,00.html

[2] Jacobs, Charles. Trusted Operating Systems. SANS Reading Room. May 14, 2001. http://rr.sans.org/securitybasics/trusted_OS.php

[3] HP-UX 11i Security. Hewlett-Packard. Date unknown. http://www.hp.com/products1/unix/operating/security/index.html

[4] HP Virtualvault Datasheet / Product Brief. Hewlett-Packard. Date unknown. http://www.hp.com/security/products/virtualvault/papers

[5] Emmen, Ad. SGI Trusted IRIX offers secure operating system for government and commercial sectors. Primeur Monthly. May 23, 2002. http://www.hoise.com/primeur/02/articles/monthly/AE-PR-07-02-11.html

[6] Costello, Chris. The TrustedBSD Project. Daemon News. August, 2001. http://ezine.daemonnews.org/200110/trustedbsd.html

[7] Long, Scott. FreeBSD 5.0-RELEASE Announcement FreeBSD. FreeBSD.org. January 19, 2003. http://www.freebsd.org/releases/5.0R/announce.html

[8] McCullagh, Declan and Zarate, Robert. Super-Secure Linux, Inch by Inch. June 11, 2002. http://www.wired.com/news/linux/0,1411,53004,00.html

[9] Galvin, Peter Baer. Can You Trust Trusted Solaris 8?. Sys Admin. 2002. http://www.samag.com/documents/s=1769/sam0112i/0112i.htm

[10] Trusted Solaris[tm] 8 OE: The Only Operating System Common Criteria Certified in a Networked Environment. Sun Microsystems. 2002. http://wwws.sun.com/software/sunone/cover/2002-0507/index.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[11] The OS Redefined. Sun Microsystems. May 22, 2002. http://uk.sun.com/software/solaris

[12] Koerner, Brendan I.. The World's Most Secure Operating System. The Industry Standard. August 21, 2000. http://www.thestandard.com/article/display/0,1151,17541,00.html

[13] OpenBSD Platforms. OpenBSD.org. December 31, 2002. http://www.openbsd.org/plat.html

[14] Hachman, Mark and Rupley, Sebastian. Microsoft's Palladium: A New Security Initiative. ExtremeTech. June 25, 2002. http://www.extremetech.com/article2/0,3973,274309,00.asp

[15] Morrissey, Brian. Is Microsoft's Palladium a Trojan Horse?. Internetnews.com. June 28, 2002. http://www.internetnews.com/ent-news/article.php/1378731

[16] Carroll, Amy; Juarez, Mario; Polk, Julia; Leininger, Tony. Microsoft "Palladium": A Business Overview. Microsoft PressPass. August, 2002. http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp

[17] Security Enhancements. Sun Microsystems. Date unknown. http://docs.sun.com/db/doc/806-5202/6je7shk4l?a=view

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Last Updated: February 28th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS San Jose 2017	San Jose, CA	Mar 06, 2017 - Mar 11, 2017	Live Event
Community SANS Chicago SEC401	Chicago, IL	Mar 06, 2017 - Mar 11, 2017	Community SANS
SANS Secure Canberra 2017	Canberra, Australia	Mar 13, 2017 - Mar 25, 2017	Live Event
SANS Secure Singapore 2017	Singapore, Singapore	Mar 13, 2017 - Mar 25, 2017	Live Event
SANS London March 2017	London, United Kingdom	Mar 13, 2017 - Mar 18, 2017	Live Event
SANS Tysons Corner Spring 2017	McLean, VA	Mar 20, 2017 - Mar 25, 2017	Live Event
Mentor Session - SEC401	Orange County, CA	Mar 21, 2017 - Apr 20, 2017	Mentor
SANS Abu Dhabi 2017	Abu Dhabi, United Arab Emirates	Mar 25, 2017 - Mar 30, 2017	Live Event
SANS Pen Test Austin 2017 - SEC401: Security Essentials Bootcamp Style	Austin, TX	Mar 27, 2017 - Apr 01, 2017	vLive
SANS Pen Test Austin 2017	Austin, TX	Mar 27, 2017 - Apr 01, 2017	Live Event
Mentor Session - SEC401	Milwaukee, WI	Mar 29, 2017 - May 31, 2017	Mentor
Community SANS San Francisco SEC401	San Francisco, CA	Apr 03, 2017 - Apr 08, 2017	Community SANS
Mentor Session - SEC401	Hollywood, CA	Apr 07, 2017 - May 05, 2017	Mentor
SANS 2017	Orlando, FL	Apr 07, 2017 - Apr 14, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201704,	Apr 11, 2017 - May 18, 2017	vLive
Community SANS Cleveland SEC401	Cleveland, OH	Apr 17, 2017 - Apr 22, 2017	Community SANS
Community SANS Norfolk SEC401	Norfolk, VA	Apr 24, 2017 - Apr 29, 2017	Community SANS
SANS Baltimore Spring 2017	Baltimore, MD	Apr 24, 2017 - Apr 29, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Apr 26, 2017 - Jun 07, 2017	Mentor
Community SANS Salt Lake City SEC401	Salt Lake City, UT	May 01, 2017 - May 06, 2017	Community SANS
SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
Community SANS Las Vegas SEC401	Las Vegas, NV	May 08, 2017 - May 13, 2017	Community SANS
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
Community SANS Baton Rouge SEC401	Baton Rouge, LA	May 15, 2017 - May 20, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	May 15, 2017 - May 20, 2017	Community SANS
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event