

Solaris 10 Security

Ravi Iyer 2004-04-19

1. Introduction

In recent years, IT organizations have endured relentless and increasingly sophisticated attacks to their infrastructure and data. Most of these attacks are launched from the Internet, but increasingly, security violations are reported from inside the organization. These attacks, which include viruses, worms and buffer overflow exploits, exponentially increase the risks corporations face in conducting business.

Over the years, the cost of acquiring and managing security technologies has skyrocketed. The Blaster worm in 2003 shutdown the systems of freight operator CSX and the operations of Air Canada, costing these companies millions of dollars. The "SQL Slammer" worm of 2003 was estimated to have caused the failure of 13,000 Bank of America ATM machines [ref 1] and cost companies nearly \$1.2 billion [ref 2] in lost productivity in its first five days despite a readily available security patch. This illustrates that managing security patches can be as complex as managing the risks of a worm attack. Additionally, the Beagle, MyDoom and a host of other viruses reported in February 2004 reportedly cost businesses around \$80 billion [ref 3].

2. Sun's "built in" security strategy

Sun takes a holistic approach to security. Security is part of Sun's technology foundation and culture, rather than an afterthought. Sun continues to drive security innovation through open standards. Additionally, through various partnerships with key technology companies, such as Tripwire and Symantec, Sun is working to further the development of open standards and systems interoperability.

Sun has always emphasized that building higher walls, and wider moats does not effectively mitigate security risks. Those strategies increase the complexity of systems and the cost of managing them while crippling business agility on the Internet. Sun has pursued a strategy of Infinite Access through technology. As part of this strategy, Sun advocates that security be integrated into the existing infrastructure but remain invisible to those who manage and use it. Sun has consistently implemented this strategy with innovative technologies built into its operating systems. Sun continues to integrate security technologies and tools into the operating systems to help mitigate the risks of conducting business on the Internet while significantly

reducing the overall cost of deploying and managing IT security.

3. Solaris 10 security enhancements

With Solaris 10 for SPARC, x86 and AMD Opteron systems, Sun believes it has broken new ground with OS security. Solaris 10 offers key technologies designed to protect enterprises from internal and external attacks, while reducing the cost of management and protecting existing investments. Solaris 10 includes a variety of innovative technologies, including process and User Rights Management, N1 Grid Containers, an Automated Patch Tool and the Solaris Cryptographic Framework.

The following is a detailed overview of these five key technologies in Solaris 10 that contribute to increased security across the IT infrastructure.

3.1 N1 Grid Containers

N1 Grid Containers are a key new technology in Solaris 10. They reduce the proliferation of systems by enabling multiple execution environments within a single Solaris instance. These virtualization environments enforce security isolation, resource isolation and fault isolation.

1. **Security Isolation:** N1 Grid Containers are shielded from the outside world and the tenants of a container are assured that no other users of a container on the same system can "see" what they are doing, or derive or compromise information. Additionally, an administrator, such as the traditional 'root' user, inside of a container only has authority over his own container, so if the container is illegally accessed, the container isolates the intruder inside the boundary.
2. **Resource Isolation:** Applications running in an N1 Grid Container share resources from a resource pool defined by the system administrator. N1 Grid Containers are not allowed to exceed their preassigned limits in a given pool.
3. **Fault Isolation:** In Solaris 10, a fault or a process in one container does not adversely affect processes running in other containers. Implemented in software, N1 Grid Containers offer this high degree of security protection on both the SPARC, IA-32 x86 and Opteron platforms on systems with any number of processors.

N1 Grid Containers offer improved service availability by minimizing fault propagation and security violations between applications. The ability to dynamically reconfigure these containers offers increased flexibility in operations and optimized resource utilization.

3.2 Process Rights Management

Despite making significant investments in various security technologies, administrators must contend with vulnerabilities in applications over which they have no direct control. These application vulnerabilities, when exploited [refer to Buffer Overflow Exploits sidebar] have the potential to cause significant system and network outage, which can raise the costs of maintenance of the applications and the systems.

Process Rights Management is implemented using Solaris privileges. Privileges in Solaris 10 are essentially permissions granted to a process to perform a set of actions. Frequently these actions access or modify a shared resource. For example, allowing a process to search a directory whose permission bits or access control lists would otherwise disallow doing so is a privilege. Traditionally, developers wrote applications in an environment not as conscious about security as we do today and assumed super-user privileges (UID=0) for most of their applications. This means that applications had access to all system privileges, regardless of whether an application requires all those privileges to do its task. The alternative was to assign the application a non-zero UID which meant that some privileges required were not available to them.

In Solaris 10, Sun introduces a more granular privilege use model that helps developers and system administrators ensure that application vulnerabilities cannot be exploited and lead to widespread system damage. The privilege-based security model in Solaris 10 provides developers the opportunity to restrict an application's operations by assigning a granular, predefined set of privileges. This provides applications with necessary and sufficient access to the operations they need to perform their task, without increasing the exposure to additional security breaches.

Should the application be compromised, it will not be possible to escalate the application's existing privileges to other privileges on the system. The move to a privilege-based security model for applications

Buffer Overflow Exploits

Developers sometimes allocate buffers in applications but do not always check the size of the data coming into these buffers. An attacker can overflow such a buffer and by placing a pointer to a piece of code under the attacker's control can take control of the application with the privileges assigned to that application. Buffer overflow exploits are most common on the stack and not very common on the heap (since heap memory allocation is different and hence harder to exploit). Solaris 9 introduced the option to

will contribute significantly to limiting the cascading effects of security vulnerability exploits, and contribute to greater uptime of applications and systems. The enforcement of Process Rights Management is enabled by default and cannot be turned off.

For example, assume a mail server running on a Windows or Linux server is compromised by a hacker. This hacker will normally be able to assume the privileges of the mail server and in many instances increase his/her operating privileges on the system if local exploits are also available. If successful, this scenario will provide the hacker complete control of the system and frequently the network.

Let us compare the same scenario in Solaris 10: Even if the mail server is compromised the privileges available to the hacker will be very restricted and the hacker will be unable to increase his/her operating privileges. This will limit the risk of unknown changes that can be caused by the hacker. Process Rights Management allows for applications to be executed in an environment where they run with only the bare minimum privileges required to do their task.

While Process Rights Management includes the necessary APIs for developers to provide fine-grained privileges in their applications, existing applications can also benefit from the new privilege based security model. By implementing user rights management implemented as role based access control (RBAC) in Solaris 10, a policy can be specified where applications are granted explicit additional privileges or can have their default privileges reduced. The policy can take into account the user or role running the service. Additionally when applications take advantage of Process Rights Management they will be implicitly compatible with the Trusted(TM) Solaris Operating System 10 and can target the high-margin markets that demand higher assurance and multi-level security.

The Process Rights Management feature combined with the `noexec_user_stack` switch introduced in Solaris 7, provides some of the most powerful mechanisms of preventing and limiting the damage

disable execution of user programs on stack and assist in lowering the likely hood of exploit from stack based buffer overflows, this feature is only available on SPARC and AMD64 systems because it requires hardware support that is not available in current Intel 32bit CPUs. This can be done by employing a system wide parameter for example. Introducing the line **'set noexec_user_stack=1'** in the `/etc/system` file. Another option is to have the application's stack be defined **non-executable** using the new mapfile segment descriptor.

The ability to prevent stack buffer overflow exploits along with Process Rights Management introduced in Solaris 10 provides a powerful mechanism to strengthen the security environment for

caused by hackers when they exploit application vulnerabilities. It is important to note that N1 Grid Containers have lower maximum privilege sets and for example, don't have access to devices.

3.3 User Rights Management

Similar to the privileges assigned to applications, users on a system can also be assigned authorizations, which control their operations on the system. Solaris 10 implements User Rights Management with RBAC technology. Continuing Sun's strategy of integrating strong security and ensuring all users are held accountable for their actions, Solaris 10 enhances the RBAC functionality included in Solaris 8 and Solaris 9 by providing higher levels of granularity for user actions in roles. The use of RBAC helps organizations mitigate attacks from trusted insiders. This is done by ensuring that users who are required to perform certain administrative tasks on the system are only assigned those privileges necessary to perform those tasks, without having to assume 'super-user' (root) level privileges. Additionally, any privileged actions they perform can be audited to provide strong accountability of their actions.

3.4 Automated Patch tool

Solaris 10 includes Automated Patch tools that verify the integrity of signed patches and allow for easy patch removal and restoration. Security patches require quick action on the part of the administrator and depending on the volume of systems and the number of patches, can quickly become a complex, time-consuming task. Patches can also be categorized and their installation automated based on specific criteria. For example, it would be possible to automatically install all security patches that do not require a restart of the system. These Automated Patch tools will save administrators the time of updating systems with security patches and will hence reduce the costs associated with system management and downtime. The automation is under the control of system administrators at all times. Compare this with the Microsoft Windows platform, which gives limited control to the system administrator, once the patch install is initiated.

3.5 Solaris Cryptographic Framework

applications. It relieves the IT administrator from the burden of worrying whether an application on one of the systems can compromise the rest of the system and the network due to buffer overflow exploits. It provides the IT administrator with a global switch to disallow even poorly written applications to be susceptible to stack buffer overflow attacks.

Solaris 10 introduces the Solaris Cryptographic Framework based on the industry accepted PKCS#11 standard. This enhances performance and centralizes management of cryptographic operations. The Cryptographic Framework in Solaris 10 includes the ability to hide the complexity of cryptographic functions (implemented in hardware or software) from the applications. Application developers are encouraged to write to a common API, which will interface with the underlying crypto algorithm chosen by the IT organization. This helps IT organizations protect their investment in applications and helps Sun partners write applications without worrying about the underlying cryptographic implementation. Administrators can set policy on which algorithms are allowed from a given cryptographic provider, enabling such things as enforcement of hardware key storage.

4. Conclusion

Overall, Solaris 10 offers many new technologies to enhance the overall security of the IT infrastructure. Innovation in rights management for processes and users, N1 Grid Containers, cryptographic infrastructure with already strong features in authentication and access control has the potential to make Solaris 10 the most secure operating platform in the market.

References

1. "Computer worm grounds flights, blocks ATMs," CNN.com, (Jan. 26, 2003) <http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/>
2. Robert Lemos, "Counting the cost of Slammer," CNET News.com (Jan. 31 2003) <http://zdnet.com.com/2100-1104-982955.html>
3. "February Sees Record Virus Damages," Web Host Industry Review (Feb. 19 2004) <http://thewhir.com/marketwatch/feb021904.cfm>

About the author

Ravi Iyer is the Group Manager for Security in the Systems Software Marketing group at Sun Microsystems, Inc. and has overall responsibility for Solaris Security and Trusted Solaris. Ravi Iyer was the Product Line Manager for Solaris Product Marketing. He contributes to the development of Sun's overall security strategy, including the Solaris and Trusted Solaris Operating Systems. Prior to joining Sun, Iyer was an engineer at Bell Labs. Iyer has more than 15 years of experience in the technology industry.

Feedback and reprint requests can be sent to the [editor](#).

This article is Copyright 2004, Sun Microsystems and SecurityFocus.

[Privacy Statement](#)

Copyright 2006, SecurityFocus