WHITEPAPER | MARCH 8, 2016

ENHANCED DATA CENTER SECURITY WITH ORACLE SPARC AND ORACLE SOLARIS

COALFIRE℠

North America | Latin America | EMEA
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

Section 1 – Introduction

This paper provides guidance to organizations interested in researching Oracle's SPARC M7 and Oracle Solaris 11 security features and capabilities. It will also provide a high level overview of some of the noteworthy features that these two product offerings bring to the market. We will review industry best practices in information security as it relates to these Oracle products in the context of a secure implementation. This paper is not meant to be an in depth technical paper, position paper, or security implementation guide. It will instead endeavor to deliver a foundational level of knowledge of the SPARC M7 processor and server technology and the function set within Oracle Solaris 11 that are primarily relevant to information security as it is currently understood. The information used to compose this paper was collected from a variety of open sources, interviews with Oracle subject matter experts, and reviews of OEM (Original Equipment Manufacturer) documentation and specifications.

Current State

Over the last few years, we have seen a number of grievous security breaches where an attacker was able to access critical information in a client's database. These internal file servers and databases contain the majority of data that cyber attackers target. Whether user lists, client databases, or other valuable business data, their information soon enters markets on the dark web. These critical systems also tend to receive a significantly smaller portion of the funding and attention than is allocated to securing other information assets. Typical spending patterns put the majority of focus on network protection such as Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), firewalls, and Security Event and Incident Management, also known as SEIM (1). It is not uncommon for an organization to spend the bulk of their information security budget on the perimeter and spend relatively little in securing what they consider business critical applications. This spending and focus gap leaves the risk to these critical systems unexamined and unaddressed and consequently increases the risk exposure for businesses that require the utmost in terms of their server and database confidentiality, integrity and availability. Likewise, we have also seen reports of various security vulnerabilities (e.g. Venom, Heartbleed, Shellshock, etc.), that when exploited would lay bare companies' data to an attacker.

In the last few years, we have seen a number of high profile breaches where attackers gained access to unpatched servers and largely unencrypted databases. These known vulnerabilities were all listed as causes for breaches at such large organizations as JP Morgan Chase (76m records lost) (2), Premera Blue Cross (11m records lost) (3) and Anthem (80m records lost) (4), and the infamous Office of Personnel Management (OPM) data breach (21.5m records lost) (5). While the nature of the threats that companies face are constantly changing and evolving based on the predominant security measures in place, the targeted areas have been consistent over the years.

It is into this environment that Oracle introduced their latest server and OS offering in the form of the SPARC M7 and SPARC T7 servers and Oracle Solaris 11.3. The SPARC M7/T7 servers use the new SPARC M7 processor. These new technologies when combined create a vertically integrated environment that is designed to be secure by default. In addition to the steps Oracle has taken to create an environment it has been calling an 'information fortress', they have also made great strides in creating an environment designed for applications and businesses that require secure systems with high availability, confidentiality and an impressive amount of processing power. It should be noted that the SPARC M7 processor and Oracle Solaris 11 is just part of a comprehensive suite of Oracle security products.

Section 2 – SPARC M7 Processor

SPARC M7 Capabilities

The Oracle SPARC M7 processor has exciting capabilities in the encryption arena. While databases constitute a large surface area for attack and a prime target for attackers, they have historically been difficult to secure through encryption. This lack of encryption ultimately comes down to performance cost for having data continuously encrypted and decrypted in the course of conducting regular business activities. Reduced performance caused by encryption can cause a significant decrease in overall operations depending on the implementation and type of encryption solution (columnar, tablespace, etc.). Any sort of performance degradation in a critical application or database is unwelcome to most organizations. In order to compensate for this general lack of data-at-rest encryption, most organizations assume the additional risk of operating with their data in the clear (unencrypted). Other organizations manage this vulnerability by implementing an array of compensating controls such as encrypting archived data, offline backups, or some other measure.

Oracle has a long history of implementing hardware based cryptographic acceleration in their servers and the SPARC M7 processor benefits greatly from this knowledge and history. Oracle has engineered the cryptographic accelerators not as co-processors, as some other manufacturers do, instead they are placed in line with the instruction pipeline making for an improved implementation of hardware level encryption and increasing the overall efficiency of the encryption/decryption process. This advancement removes the high bar of entry to operating in a fully encrypted environment that existed otherwise (see figure 1). The SPARC M7 has a Cryptographic Instruction Accelerator for each of the processors' 32 cores. The cryptographic accelerators have built in functionality to handle 15 commonly used cryptographic algorithms including: AES (GCM and CCM in 128, 384, 256 bits), Camellia, CRC32c, DES, 3DES, DH, DSA, ECC, MD5, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512, thereby ensuring usability across a wide range of implementations and applications.

By leveraging hardware-based encryption acceleration, as opposed to software-only based encryption, the speed of the encryption/decryption process is dramatically increased. An additional benefit of this hardware based encryption design is it reduces the possibility of an encryption application compromise. As hardware based encryption does not rely solely on an encryption software package, it provides an additional layer of protection from malicious code that could compromise an encryption application. Put more simply, encryption software can be compromised and circumnavigated by an attack, hardware generally cannot. This design also reduces the need for interaction with the host system processes and resources. By reducing the need to interact with the host system process in order to encrypt/decrypt data, the SPARC M7 servers reduces the typical computational load of encryption on the core processors.

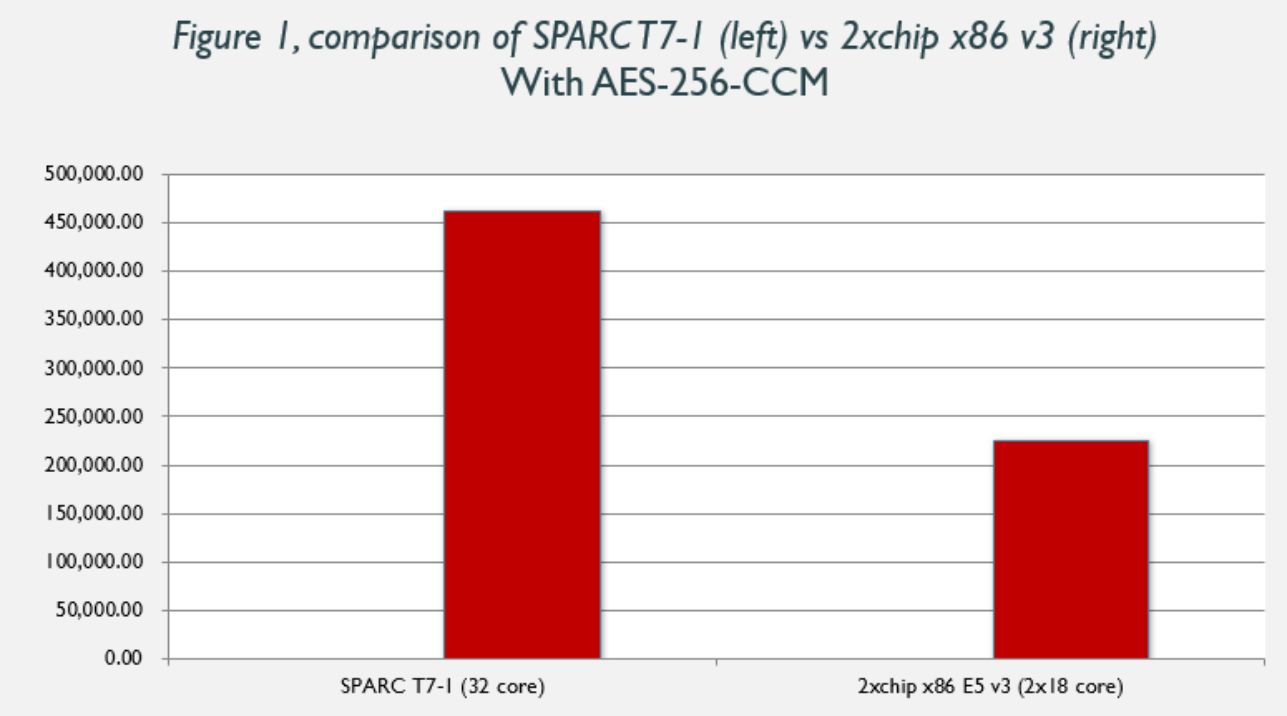

Figure 1, Y axis is IO operations per second. Results show performance while running encrypted ZFS file system. T7-1 using 1xM7 processor and 256GB of memory with Oracle Solaris 11.3 compared to 2x E5 v3 with 256GB of memory.

This efficiency and associated performance increase is additionally leveraged by Oracle Solaris 11.3 ZFS file system and its encryption option. The ZFS files are encrypted using AES, using key lengths of 128, 192, or 256 bits. Another way in which Oracle has leveraged the small performance footprint of operating while encrypted is the ability to move Virtual Machines (VMs) while encrypted. This new capability is a major boon to organizations that have security concerns and operate in a mission-critical and high availability environment. The SPARC M7 processor technology opens the way for more organizations to operate in a fully encrypted environment, whether it be utilizing encrypted databases or operating in a heavily virtualized environment or private cloud.

There have also been some notable advancements in the processors themselves. The 32 cores used in the SPARC M7 processor have out-of-order execution units and also have dynamic threading capabilities to go from one to eight threads per core. This means that if a particular processor needs additional resources for a particular thread, the chip can dynamically allocate resources to it and speed the completion. Memory bandwidth for the processors is 333Gb/second. This high access speed when coupled with the exceptionally large caches means even more performance can be drawn out of the server as the necessary data is far closer to the processors performing the work. As an added element of future proofing Oracle has also included support for NVMe (Non Volatile Memory express). NVMe provides for greatly improved performance with lower latency as well as higher throughput performance. Overall the SPARC M7 chipset shows marked improvements in workload capacity, speed, security, and has a number of enhancements that vastly improve its capabilities when dealing with encryption, security, virtualization and databases. The large cache size and high bandwidth also makes it far less resource intensive to load and manipulate encrypted data thereby removing yet another obstacle to implementing encryption throughout the environment.

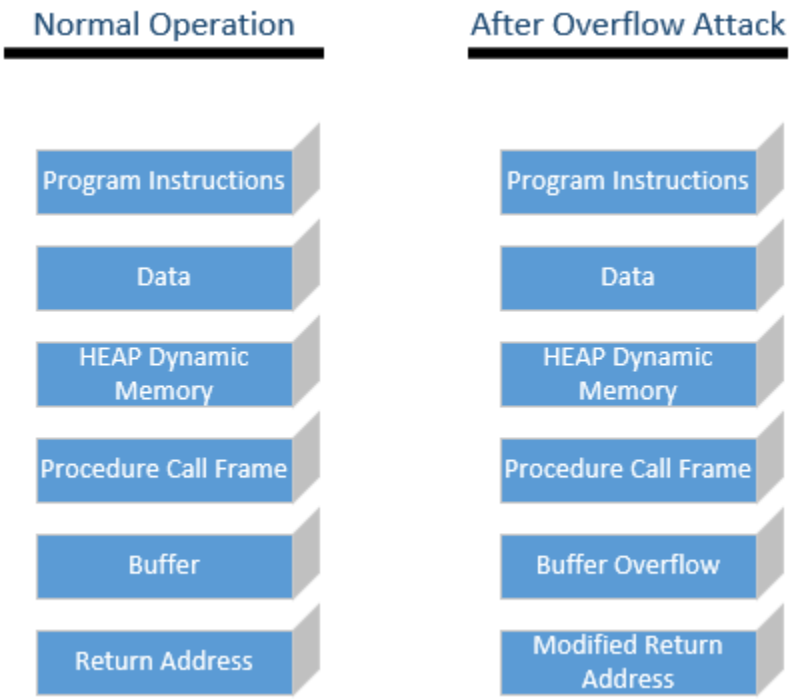

Figure 2, Illustration of buffer overflow attack.

Silicon Secured Memory

While the SPARC M7 processor has a lot of new technology in it, one of the truly notable aspects is its use and implementation of what Oracle is calling 'Silicon Secured Memory'. In order to better understand this feature and what its benefits are we first need to review how memory and pointers normally operate. In a standard computer environment, when code is executing it utilizes pointers and either stacks or heaps. A stack is a reserved area of memory, this memory is used to keep track of a program's internal operations (functions, memory addresses, parameters, etc.). A pointer is a register used to indicate where in the allocated memory to get data from. In a normal environment a program will use a pointer to find the next section in the assigned memory and execute the instructions in that section. While the concept is fairly straightforward, the execution of this process can become more complex. Poorly written code for example can result in pointers attempting to access memory that is not in their allocated memory. When this standard behavior is maliciously exploited it is called a buffer overflow or over-read attack. In a buffer overflow or buffer over-read, an attacker takes advantage of code that does not implement bounds checking and overruns the buffer's boundary. This allows the attacker to write adjacent memory locations in the memory in a buffer overflow attack (see figure 2), or obtain data in other sections of memory in the case of an over-read attack. An over-read or overflow can alter program behavior, cause a crash, execute malicious code, return exploitable information to an attacker, or otherwise breach system security. The Heartbleed vulnerability (CVE-2014-0160) is one of the more notable and recent examples. The Heartbleed vulnerability took advantage of a lack of bounds checking within TLS/DTLS and allowed an attacker to over-read the buffer and request the information in adjacent memory. Through this method, attackers were able to gather user login information and other sensitive data from exploited systems. Likewise Venom (CVE 2015-3456) affected QEMU, Xen, and KVM hypervisors that had a buffer overflow vulnerability that allowed an attacker to compromise the VM environment. Under this vulnerability attackers were able to overrun buffers and either cause crashes or execute arbitrary code or malicious payloads, otherwise known as malware. These types of inherent issues can exist in nearly any code when it is not securely or properly developed.

Silicon Secured Memory places a 4-bit 'key' into the pointer and a corresponding 4-bit 'lock' on the memory in the stack. In order to more easily understand the concepts behind this security feature, Oracle refers to it as 'color coding' (no actual colors are used, just bit codes). When this feature is utilized it provides a 'color' randomly to the pointer, using 4 unused bits and provides a corresponding 'color' to the allocated memory buffer. If the executing pointer's color does not match the color of the memory address it's attempting to access, the operation fails. Oracle's engineers took the added effort to use map theory in order to prevent two memory buffers with the same bit code from ever being adjacent. This color coding process would not only prevent critical vulnerabilities such as Heartbleed and Venom, but it would also help ensure that secure coding and best practices are followed as even an unintentional overwrite or over-read would fail. The corresponding marked increase in security by reducing this potential attack

surface area would be vital to any organization that is operating a highly critical system or utilizing Oracle servers for their private cloud infrastructure. While nothing is ever truly 'hack-proof', when Silicon Secured Memory is combined with best practices for information security, an attacker's job becomes significantly more difficult. Silicon Secured Memory is natively supported in Oracle Database 12c and other applications can leverage SSM without recompiling once the relevant Oracle Solaris libraries have been downloaded and linked. For developers, Oracle has also made Silicon Secured Memory APIs available in order for them to leverage this additional layer of security with their applications.

Section 3 – Oracle Solaris

Oracle Solaris

Oracle Solaris 11.3, the operating system for SPARC M7 and SPARC T7 servers, has new features and functionality that enhance the ability of users and administrator to safeguard their data and systems. These features include everything from the ability to create electrically-isolated partitions, sometimes referred to as a PDOM or Physical Domain, up to and including the option to dedicate resources to virtual partitions (sometimes referred to as a LDOM or Logical Domain), to containers (called Oracle Solaris Zones) and a type-2 hypervisor (called Oracle Solaris Kernel Zones) that can be made read-only (called Immutable Zones and Immutable Kernel Zones). While most system administrators are familiar with RBAC (role based access control), Oracle Solaris has taken it a step further with allowing a high degree of granularity in granting permissions and access. The normally contentious issue of patching, important for mission-critical security, has also been addressed.

Patching

As was seen in Verizon's Data Breach Incident Report for 2015 (6) many of the breaches exploited were well known vulnerabilities. In many cases, patches that remedied those vulnerabilities were also well known and had existed for some time (years in some cases). Often administrators are slow to patch systems in order to maintain uptime, or because there is significant concern regarding patches causing breaks in applications. Often administrators find the process of creating rollback plans to be onerous and prohibitive. There is no shortage of IT professionals who have a 'set it and forget it' mentality when it comes to server maintenance. In order to alleviate this persistent issue, Oracle has also improved the patching process.

The Oracle Solaris team has made the process of patch delivery as painless as possible. As anyone who has ever had to patch a critical server knows, there is usually a high degree of concern over downtime, functionality, and rollback plans. Now, when an administrator goes to patch the system they will no longer have to follow the method of painstakingly reviewing all software and firmware versions currently in place followed by manually checking dependencies in the update package. The Oracle Solaris Image Patching System (IPS) now has built in functionality to perform dependency checking on its own and provides a simple 'Go/No Go'. Once a 'Go' message is received by the dependency check, the patching process will take a snapshot of the system, copy it and apply all of the changes to the snapshot. If the patch requires a reboot, it will perform a fast reboot, meaning that the drives do not stop spinning and that re-initializing the hardware components is not necessary. Due to this process some reboots can take only a few minutes. If there is an issue, the rollback process is a single step and rolls back to the snapshot the system took earlier in the process before the patch was applied.

Access, Auditing, & Compliance

Oracle Solaris 11 has taken some noteworthy steps in how it manages auditing and the methods of managing access permissions. In the process of granting permissions an issue often encountered (and which is familiar to UNIX users everywhere) is that in order to perform some basic tasks and actions, root level access is often required. Oracle Solaris 11 has instituted a granular delegation process where you can grant selected personnel root-like privilege for particular tasks, files or folders instead of having to provide them blanket access. This means that there is no longer a need to provide unrestricted root level

permissions to all individuals who may only need this highest level for a specific purpose, thereby eliminating a significant security loophole. Oracle Solaris 11 also provides administrators the ability to institute time-based restrictions on access. In some breach cases, where compromised credentials are used, they are used after hours or when a given employee would not otherwise be working. By using a time based access scheme, an employee who is normally working a defined shift would not be able to surreptitiously log in after hours. This time-based access scheme also helps control general server activity without having an undue impact on personnel who may be working late to fix critical issues as the time-based scheme will not terminate logged in users.

Likewise Oracle has greatly simplified the auditing process. In the standard attack cycle, one of the tasks an attacker will perform is to edit or alter the audit logs in order to hide their activity. Oracle Solaris 11 addresses this by providing administrators the option of offloading the audit logs to a separate file server over an encrypted network connection or to the host OS without being written to local disk. This offloading of audit logs adds an additional layer of defense to systems as it presents another obstacle for an intruder to overcome to hide their malicious activity. When combined with the granular permissions of Oracle Solaris 11's delegation model it also provides the opportunity to separate duties further by limiting access to logs and audit trails. This type of layering and separation is a large portion of what constitutes the information security concept of defense-in-depth. When properly implemented, even if a server were to suffer a root-level breach, logs can be kept safe.

Oracle Solaris 11 also has a tool in order to ease the administrative burden of assessing and reporting on system configuration compliance. With the Oracle Solaris 11 compliance tool you are able to build out a variety of framework requirements (PCI DSS is available out of the box) and run it against the system. The tool then checks the system configuration and implementation and compares it with the designated framework. The end result is a report that shows the appropriate controls matched against the system along with remediation steps if necessary. This is a vital tool and would greatly speed up the work of an audit as personnel would have the necessary documentation readily at hand, thereby increasing efficiency and helping reduce unnecessary costs to say nothing of the capability to discover and remediate possible issues before an audit even begins.

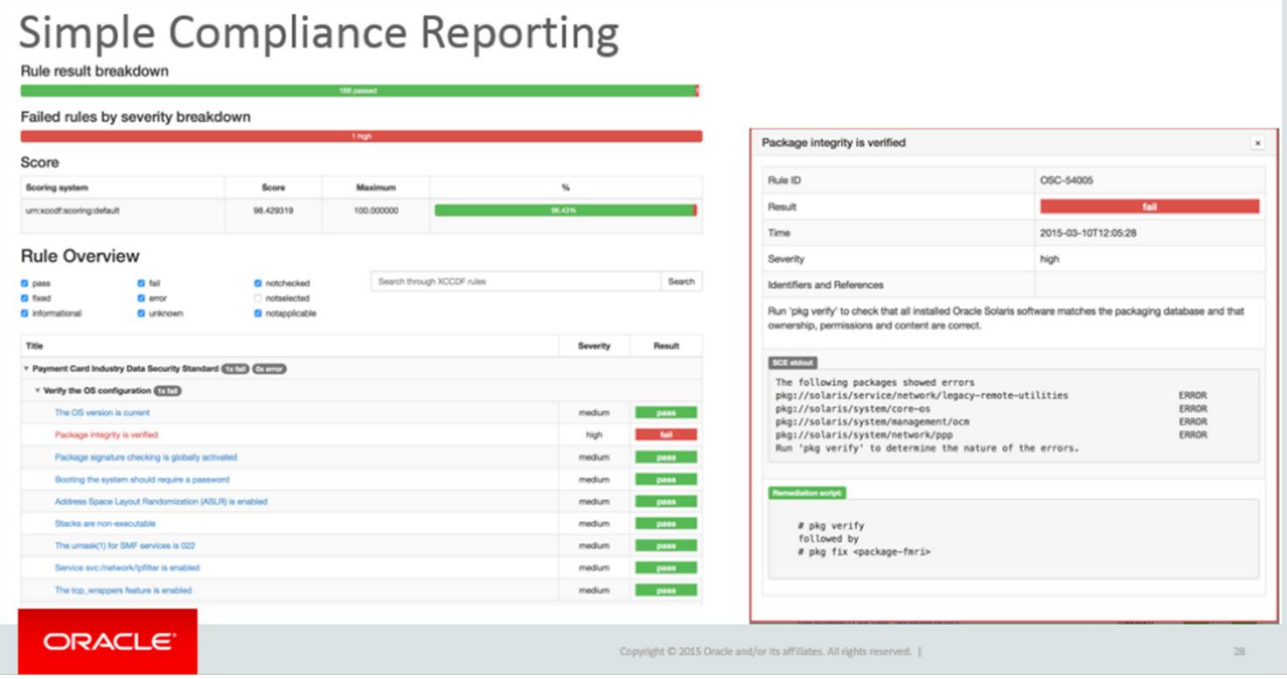

Figure 3, Image of Compliance Reporting tool.

Section 4 – Combined Security Features & the Information Fortress

Virtualization & Segmentation

Oracle Solaris 11 has also made advancements in virtualization and segmentation in its ability to manage virtualized networks, virtual network segmentation, ZFS and Immutable Zones (containers). Immutable Zones is the Oracle Solaris feature whereby an administrator can lock down a VM and prevent changes to it. This provides an added layer of protection as all created virtual machines using the Immutable Zone feature are secured-by-default, meaning that VMs are entirely locked down until an administrator with appropriate privileges makes changes to enable particular features from outside the Zone. This prevents administrators from being able to make modifications that could accidentally leave vulnerable ports open or unnecessary protocols on. The ability to have a locked down system configuration while intentionally allowing certain applications creates an added layer of defense for organizations that must host potentially vulnerable or exposed applications (such as a web server or application). The immutable zone feature can also be used to create a VM with a known vulnerable application (like many web servers), and keep the rest of the system locked down in order to mitigate potential harm if the exposed application is compromised. This includes even preventing any writes to disk, thereby preventing an attacker from uploading malicious code. Under this configuration, even if the web application is compromised, the severity of the compromise is diminished by the Immutable Zone limiting the attacker's access.

For segmentation and virtualization, Oracle Solaris 11 leverages the architecture of the SPARC M7 processor and its multiple cores. One concern involved with commonly available virtualization technology is the shared reliance on processing cores. This concern arises from the possibility of a single VM becoming compromised and allowing an attacker to access and control the kernel. Since the kernel is shared among multiple VMs in those architectures, it means gaining kernel access compromises all VMs using it. Oracle has addressed this concern through allowing a very deep level of segmentation up to and including the ability to segment off a core in order to create an environment that is fully isolated. With Oracle Solaris 11 and SPARC M7 combined, a wide array of segmentation tools become available. Everything from Immutable Zones to Physical Domains (PDoms) that can divide and isolate the usage of hardware itself to Oracle VM Server for SPARC Logical Domains (formerly known as LDoms) that are virtual servers that are managed, configured and rebooted independently. Whatever the type and degree of isolation and separation required, Oracle Solaris and SPARC M7 have a viable option.

Oracle Solaris 11 has also instituted a granular level of control over the flow of data through the networking and hardware resources a particular host uses. With these granular flows in place, an administrator is able to quickly isolate and segregate suspicious traffic. In a security context, this is an excellent tool that aids in incident response. One of the aspects of incident response that slows remediation is the isolation of corrupted databases, applications, or malicious traffic. Having this level of control over the flow of data alleviates concerns with causing outages to other systems if an administrator has to shut down suspected malicious activity.

Transparent Data Encryption

Transparent data encryption (TDE) is the industry term for the encryption of data within databases at the file level. It fulfills encryption requirements for several compliance frameworks and originally became an Oracle offering with the Oracle 10g database. TDE allows for near real-time decryption and encryption of data and log files. In the case of the SPARC M7/T7 servers, it also leverages the high I/O bandwidth to accelerate this process. The encryption is symmetric and stores the master key to the encryption in an external security module. Once a user has authenticated to the system and has verified their permission to access the data, they are able to view the unencrypted data. In essence this means that the encryption is invisible to authenticated users. Again, one of the pieces that makes TDE so unique in the SPARC M7 environment is the sheer speed in which this happens. With the mass of processing power and the in line cryptographic accelerators used for the server, there is no longer a marked difference in speed of operations with the use of encrypted databases.

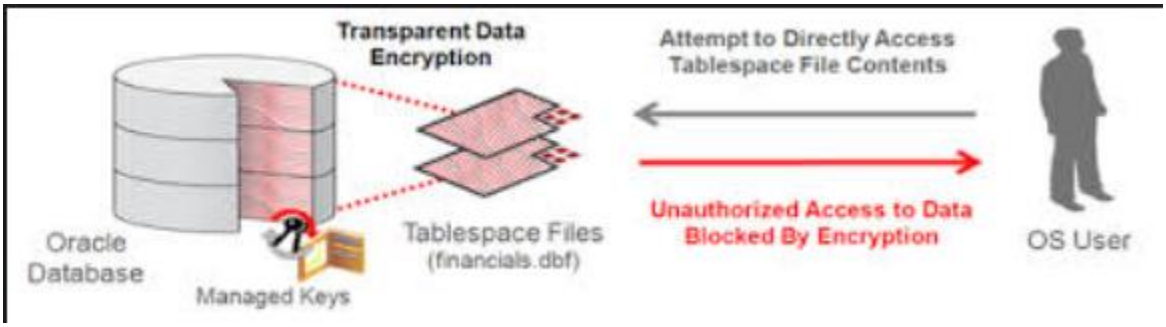

Figure 4, Illustration of Oracle's Transparent Data Encryption

Securing your Information

Security program managers often think of information security in terms of frameworks, collections of controls geared towards a particular purpose. PCI focuses on payment cards and cardholder information, HIPAA focuses on electronic Protected Health Information (ePHI), and so on. While each security framework has its own set of controls and standards, most of these frameworks have a number of common elements. Network segmentation, access controls, audit controls, protection from malicious code, and encryption are all recurring themes. Oracle's offerings of the SPARC M7/T7 server technology and Oracle Solaris 11 address each of these, and provides a wide array of tools to do so. Pervasive encryption becomes an easily achievable goal with the introduction of cryptographic accelerators and Oracle Solaris transparent data encryption. Transparent data encryption leverages the cryptographic accelerators in order to provide near real time encryption and decryption of the Oracle Database. This removes the high performance overhead that previously existed in an environment with pervasive encryption and also allows organizations to more readily meet a number of compliance controls where encryption is often desired, if not required. Oracle Solaris also provides a range of controls and tools in order to address access controls and auditing. Being able to provide a granular level of access based upon factors such as job duties or time-based access alleviates common security concerns and lowers overall risk. This refined level of permission granting can also be applied to several other controls contained within commonly used frameworks that deal with controlling access to critical or sensitive systems. The ability to offload audit logs into a separate secured server provides another level of protection in a defense in depth strategy and can be leveraged to also provide an additional separation of job duties. The implementation of Silicon Secured Memory (or memory color coding as it's referred to in some Oracle documents) easily lends itself to providing a high degree of protection against malicious code execution. In addition to Silicon Secured Memory aiding in the protection against malicious code, it also helps propagate and reinforce best practices with code design and execution as when implemented it will prevent poorly written code (specifically code that lacks proper bounds checking) from executing. For networking and segmentation, the SPARC M7 processor and Oracle Solaris provide the capability to create a fully segmented virtual system that can even be isolated onto its own core.

When the SPARC M7 and Oracle Solaris 11 are integrated, they provide a wide and deep set of tools and options to secure your data from many of the common vulnerabilities that have so often put organizations on data breach lists. Thanks to Oracle's co-engineering of the SPARC M7 and Oracle Solaris, there is a synergistic effect that creates an array of options and capabilities difficult to achieve with servers and software that are designed independently or for different vendors. Ultimately, protecting your information breaks down into several key areas. The perimeter, the operating environment (servers, applications, etc.), the data itself, and your personnel. While the perimeter is secured by firewalls and IDS/IPS, Oracle Solaris and the SPARC M7 servers include protections that safeguard data, personnel and the environment.

Section 5 – Sources

All documentation used for this paper was gathered from open sources as well as documentation provided by Oracle. Additionally interviews were conducted with a number of Oracle personnel involved with Oracle Solaris and SPARC M7. The Documentation utilized is listed below.

Figure 1 – Figure derived using data from https://blogs.oracle.com/BestPerf/entry/20151025_aes_t7_2. 10/26/2015.

Figure 2 – Figure provided by Coalfire Systems 03/2016.

Figure 3 – Image from Oracle Presentation. “Secure Cloud Infrastructure”. Oracle. 11/20/2015.

Figure 4 – Transparent data encryption. Oracle. http://www.oracle.com/technetwork/database/options/advanced-security/index-099011.html.

1. Mello, John. “Security pros say their companies invest in the wrong technologies”. CSO Online, 02/13/2013.
2. JP Morgan Chase (2014). SEC Form 8-K. Retrieved from http://investor.shareholder.com/jpmorganchase/secfiling.cfm?filingID=1193125-14-362173.
3. Reuters. “Premera Blue Cross Says Data Breach Exposed Medical Data”. New York Times, 03/17/2015.
4. Hiltzik, Michael. “Anthem is warning consumers about its huge data breach”. LA Times, 03/06/2015.
5. Sciutto, Jim. “OPM government data breach impacted 21.5 million”. CNN, 07/10/2015.
6. Verizon Data Breach Incident Report 2015. Verizon. 2015.
7. Oracle’s SPARC T7 and SPARC M7 Server Architecture. Oracle 2015.
8. The Fully Encrypted Datacenter. Oracle. October 2015.
9. Next Generation SPARC Processor Cache Hierarchy. Ram Sivaramakrishnan, Sumti Jairath. Oracle 2014.

THE AUTHORS

Deepa Saldanha | Senior Director
Brett Larsen | IT Security Senior Consultant
Jacob Harlin | Information Security Consultant

THE NATION'S CYBER RISK MANAGEMENT AND COMPLIANCE LEADER

With more than 15 years in IT security and compliance and ASV-certified since inception, Coalfire is a leading provider of IT advisory services, helping organizations comply with global financial, government, industry, and healthcare mandates while helping build the IT infrastructure and security systems that will protect their businesses from security breaches and data theft.