THE CLIPPER GROUP
Navigator™
Navigating Information Technology Horizons℠
Published Since 1993 Report #TCG2010049 October 18, 2010

Hardware-Enforced Security — A Good Foundation

Analyst: Anne MacFarland

Management Summary

Most of us, when climbing in steep mountains, look for good, safe paths. When we climb a rock face, we rely on the security of harnesses, ropes, and pitons. Without the right strategy and equipment, danger –and the likelihood of failure – increase. In recreation, risk may be part of the allure. In business, it is seldom a good thing.

However, all businesses must take risks from time to time. They appreciate firm, secure foundations that can mitigate those risks. In technology implementations, security must be pervasive in extent. When precipitated into more granular system elements, system agility and support for a high rate of change are improved. New tools, such as automated discovery, support the use of localized control elements, which are part of this new blended kind of security strategy.

With secure foundations, other layers of security can be added – where they are needed. The need to secure data in a sharing and participative world can vary widely. The need to secure process is more rigorous. The need to assure an uncorrupted operating system is downright implacable. Assuring security in hardware and in operating system elements reduces the risks that must be addressed.

Oracle, with hardware from its Sun acquisition, now offers new extensions to hardware-based security that can mitigate the risks inherent in many situations, including multi-tenant situations, such as those found in clouds. Tools to address these risks are also built into *Oracle Solaris*, as it now is called, which is secured by the hardware elements. The containers and labeling that Solaris now supports can further limit the scope of the risks that remain. Like badly equipped climbers, many kinds of malicious software cannot find a footing from which to mount an assault.

With the hardware assets from Sun, Oracle can forge a basic hardware-based security layer. Considerable additional security is furnished by Oracle Solaris, an operating system that Oracle sees as the glue between the hardware and the applications. The foundation of Oracle Solaris' security stems from the world's first Internet worm attack and has been central to the operating messaging and design ever since. Secure-By-Default behavior, auditing, and the ability to segregate and compartmentalize data (both in flight and at rest) all are part of Solaris' DNA. Solaris security and encryption permeate every aspect of the Solaris experience.

Like the United States after the Louisiana Purchase, Oracle now has lot more with which to work. For a brief survey of this new landscape, please read on.

Oracle Solaris — The Master Builder Approach to Security

Solaris code and core assets (binaries, libraries, drivers, etc.) each have a digital signature. A facility in Solaris can periodically report on signature discrepancies. This allows Solaris to be a secure space from which the following features can be deployed.

IN THIS ISSUE

Solaris Containers and Logical Domains

In *Solaris 10*, Sun added the concept of container to its more classic logical domains. *Solaris Containers* are somewhat like the virtual machines of VMware, but they are more focused on isolation, not management of guests. Applications in Solaris *Containers*, by design, have fewer privileges. They are easier and quicker to restore, and easier to migrate, because they are contained. Containers are good for extending the life of older applications. The benefits of Solaris Containers are similar to those of containerized shipping.

Oracle VM Server is another, hypervisor-based flavor of isolation that is available for both SPARC and AMD/Intel processors. On SPARC, as an evolution of Solaris' Logical Domains, Oracle VM Server is a hypervisor that supports multiple independent Solaris instances. On x86 architectures (both 32-bit and 64-bit), Oracle VM Server supports *Linux*, *Windows*, and *Open Solaris*.

The compartmentalization that Solaris offers has the following benefits:

- Isolated memory space.
- Separation of applications from the physical attributes of the server.
- No access to raw kernel memory in Solaris Containers. (This does not apply to Oracle VM Server.)
- Ability to limit memory utilization and CPU utilization.
- Prevention of interface snooping in shared NICs.[1]
- Isolation and extended life of legacy applications running on earlier versions of Solaris.
- Limiting the scope and impact of Trojans and other malicious software.

This is a strategy is similar to urban life, where strangers abound, people move frequently, and caution is a regular practice. If your apartment is properly secure, you feel free to enjoy all the city can offer.

Solaris Trusted Extensions

Isolation is good for basic security, but, without the proper hooks for management, isolated parts can become a nightmare. Therefore, as part of *Solaris 10*, Oracle supports a layer of security: *labeling*. These labels are used to restrict the release of information on a need-to-know basis. In addition to preventing users and processes from accessing data for which they are not authorized, the system enforces a mandatory access policy that limits what they can share with others.

In large and dynamic data environments, the ability to delegate administrative responsibility into the functional roles reduces the risk of accidental or intentional mis-configurations. Solaris 10 implements fine-grained user and process right management, which forms the basis for Role-Based Access Control (RBAC). Rather than relying on a boot or super-user account, authorized users assume customizable roles to perform security-relevant actions. The system prevents users from escalating their privileges and audits their actions. This facilitates policies, such as separation of duty, where administrative and policy controls can be assigned to different individuals.

Collectively, the security features of Solaris have been independently evaluated and certified to conform to three protection profiles. This is part of the Common Criteria process with an assurance level of EAL4+. The evaluation was based on the Controlled Access Protection Profile, the Role-Based Access Control Protection Profile, and the Labeled Security Protection Profile.

DTrace and DLight

DTrace, a physical visualization tool used to locate and trace physical faults in hardware, was introduced in Solaris 10. DTrace is an analysis tool used to observe system behavior, such as performance bottlenecks. It is unique in its ability to monitor complex interactions while the system is operational. With each succeeding version of Solaris, it has been made easier to use – you no longer have to be proficient in *D*. Now, *DLight*, a visualization tool in *Oracle Solaris Studio*, takes the DTrace concept to new dimensions, using profiles derived from operational metrics. This visualization can come in a variety of contexts – the element, the stack, the business process, a pair of interactive processes, etc. These can be aggregated into role-based views, supporting a better understanding of the infrastructure as a system.

Project Crossbow

Project Crossbow, just recently coming to fruition, builds out internal virtual resources and

[1] In Solaris, NIC management can also be a separate domain.

aggregates their joint management within the Solaris OS. Solaris now can emulate the entire stack through the L2 switches. It supports multi-threading from hardware to application – each thread in a VPN-like isolation.

Putting more of the software stack under the control of the operating system has many benefits when data privacy regulations, such as PCI-DSS, are involved. Since Solaris's integrity can be checked, the system elements running within it are protected.

Project Crossbow has involved a complete rewrite of the *STREAMS* data-sharing stack that does encryption and networking functions on the processor, in order to build a virtual stack within the operating system. Why would you want this, when people are saying operating systems are dead? For the same reason you want an adequate number of pitons, extra carabiners, and an ice ax in your climbing equipment. You cannot make up for inadequacy. Other benefits include:

- One network resource manager for a fuller variety of resources, both physical and virtual.
- Guaranteed QoS for applications.
- Virtual NICs (more secure than their physical cousins do).
- Full stack coordination.
- Service properties, such as traffic flow classification and traffic prioritization, that are inheritable and unalterable

Crossbow delivers all of this using standard network protocols, which ensures full visibility into the stack. Visibility not just for Solaris tools delivered with the system for network management, but also standard network management tools that are locked out of other networking virtualization technologies, such as from VMware or Cisco.

Zettabyte File System (ZFS)

The *Zettabyte File System* gives access control to files with considerable precision. *ZFS* has more Access Control Lists (ACLs) than the UNIX File System (UFS), which was based on Sun's Network File System (NFS) 4. It contains a *Basic Auditing Reporting and Tracking* tool (BART), which can be used on both global and non-global zones. It can even create a manifest for each file process. In Solaris 10, ZFS was enhanced to support delegated administration – a basic requirement for global organizations whose operations follow the sun.

ZFS cryptography provides the ability to encrypt your file sets at the file system level, which allows for greater security to prevent against virtual and physical theft. (Note that hard-drives disappearing from laptops or severs are not an issue.) Additionally, with the delivery of the T3 SPARC chip, there is a crypto-accelerator per core to ensure a minimal (close-to-nothing) overhead. This saves customers money by not requiring them to use a third-party file system encryption program.

Additional Oracle Security Features

Advanced Security

Encryption of data *at rest* and *in motion* is supported by the SPARC processor architecture. The processor also authenticates both users and IT processes. This approach does not require triggers, views, or changes in application code, though it can respond to these if they are an inherent part of the application.

A new *Crypto-Accelerator* supports Elliptic Curve Cryptography (ECC). It is sited in the processor on both MAU (Modular Arithmetic Units) and SPU (the STREAMS Processing Unit). Coordination[2] of these separate processor areas assures that the performance penalty of encrypting all kinds of data is minimized. By contrast, a PCI-card based approach is an offload that exacts a more significant performance penalty.

These security standards are supported.

- Kerberos
- Radius (integrated in Oracle DB)
- SSL (digital certificates)
- Entrust (PKI)

Service Processor

The service processor is also secure. It supports the following:

- Network encryption using any AES, RSA, RC4, DES, or Triple DES.
- A Hardware Security Module (HSM) that allows IT administration to manage keys outside of the database, or to use third party services.
- Encrypted backup (via RMON).
- Encrypted Data Pump Exports.

[2] Coordinated management is provided in MAU by the Niagara Crypto Provider device driver (NCP) and in the SPU by the Niagara2 Provider Device Driver (N2CP).

The next generation Solaris operating system adds in the ability to protect data at rest using ZFS encryption, as well as protecting data in flight. It has the ability to consume PKCS#11 as a default feature of the operating system and it uniquely and tightly couples with not only the *Oracle Key Management Appliance* but also *Oracle Advance Security* options for the database. Combine this with the FIPS 140-2 Level 3-certified HSM, the Key Manager, and Oracle's 10Kx tape devices, and the result is an OS and hardware stack that is secure, trusted, and protected.

Data Masking

Data Masking is a separate risk-avoidance solution that complements the hardware elements above, and is part of a broader security story. It is targeted at internal unnecessary exposure. The basic premise is that sensitive data should not be exposed unnecessarily to some members of the IT staff, such as developers. This risk becomes greater, if development is outsourced.

There are two components to Oracle's data masking solution:

- A format library contains templates specifying what to mask and how to do so. Templates prevent one-off customization.
- Masking Definitions map the templates to the tables that are to be masked. They are intelligent enough to alert which columns have foreign keys and will extend the mapping to the additional tables if desired.

Once the templates and table associations have been set up, a Pre-Masking Validation process checks for omissions and errors. This validation is a wise move to take before generating scripts. With proper foresight, these scripts will be reusable. It is often recommended that these masking operations be done on a staging server, rather than directly in the development environment, to assure that no real data is ever visible to the development process.

Business and Cloud Value

When taken together, all the security elements described above can sharply diminish the extent and severity of the security challenges that must be addressed. Unlike appliances, these capabilities do not become another element to be managed – and secured. The business value of this kind of approach is significant – and its value multiplies for each independent tenant that is added. Consider this cumulative value in a multi-tenancy situation, such as a cloud.

Conclusion

Thanks to the Internet and the business benefits it confers, businesses now operate in a virtual urban situation, fraught with unanticipated risk. Consider the value and simplicity of security that it built into the hardware and operating system. It may be exactly what you need.

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Anne MacFarland **is a Senior Contributing Analyst for The Clipper Group.** Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group in 2001 after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

- ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial "128" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager**, *Clipper Notes*, and "*clipper.com*" are trademarks of The Clipper Group, Inc., and the clipper ship drawings, "*Navigating Information Technology Horizons*", and "*teraproductivity*" are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosures

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

After publication of a bulletin on *clipper.com*, The Clipper Group offers all vendors and users the opportunity to license its publications for a fee, since linking to Clipper's web pages, posting of Clipper documents on other's websites, and printing of hard-copy reprints is not allowed without payment of related fee(s). Less than half of our publications are licensed in this way. In addition, analysts regularly receive briefings from many vendors. Occasionally, Clipper analysts' travel and/or lodging expenses and/or conference fees have been subsidized by a vendor, in order to participate in briefings. The Clipper Group does not charge any professional fees to participate in these information-gathering events. In addition, some vendors sometime provide binders, USB drives containing presentations, and other conference-related paraphernalia to Clipper's analysts.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.