**POWERful Security!**
**By Jaqui Lynch**

Security has been a very hot topic for some time, but never more so than in the past 12 to 18 months. So much of our personally identifying data is now being stored that the security break-ins that have been happening have most likely affected everyone reading this article. Additionally the penalties now for breaches of the various standards (HIPAA, PCI, etc) are significant, ranging from losing customers to fines and so on. The key point we all need to understand is that good security requires a multi-layered approach that starts with people then physical security and then the various layers. A firewall is not security and nor is locking down a server – it is critical to look at the whole environment and see how security can be applied at each level.

Looking at a typical POWER environment we have multiple layers to think about. Starting with people, we need to think about proper passwords and security practices. Setting password rules to be so complex that people have to write them down makes no sense – pick up someone's keyboard and look under it as you may be surprised! Additionally, not allowing someone to reuse any of their previous 25 passwords, or anything similar, also makes it very difficult, especially if they have to change their password every 30 days. It is important to find a good compromise on this. I have known people to reset their password 20 times in one day just so they can get back to a password they can remember. Additionally, it is important to remind people to do basic things like locking screens or logging off if they are walking away from their screens. And, of course, people need to be educated about phishing attacks – these happen all the time and look legitimate. This may seem simplistic but they are very common.

Then we have physical security. Ensuring doors are kept locked into offices and machine rooms and that people who are supposed to be escorted actually are. Poor physical security and poor password and screen protection make it very easy to get into systems that people should not have access to. Keep this in mind when on planes or in public areas. I fly all the time and am fascinated with the information I pick up from conversations around me. If it is confidential information then an airport is probably not the place to discuss it.

Now let's talk about the actual systems. The network is beyond the scope of this as it is a huge area in and of itself. Suffice it to say that it needs to be secured. The POWER servers themselves have significant security built into the firmware as do the HMCs (hardware management consoles), however attention needs to be paid to securing access to the various LPARs, HMC software and the supporting systems. As an example, many sites lock down their VIO servers, AIX systems and HMCs, but use DNS (domain name services) on Intel (Linux or Windows) to provide lookups and AD (active directory) on Windows to provide authentication. In many sites the Intel team is a separate team and their security requirements may be handled differently. So you can lock AIX down all you want,

but if the AD server gets compromised then the hacker now has a list of all the valid userids on the AIX system. This is why security must be looked at in a holistic fashion and not by silos.

Within AIX and your VIO servers, there are many things you can do to increase the security for that LPAR. These range from using TCP Wrappers to restrict and control who can connect to the LPAR to full blown security using trusted boot, encryption of filesystems, and compliance and security automation and reporting. For the rest of this article we will look at PowerSC to see what it has to offer to enhance security within the LPAR.

***PowerSC***

PowerSC Standard edition provides 6 key functions – trusted logging, trusted boot, trusted network connect and patch management, trusted firewall, security and compliance automation (pscexpert) and real time compliance. In addition, there is a separate product called Trusted Surveyor which looks at network segregation. PowerSC standard is included as part of AIX Enterprise Edition so it is possible you are already licensed for it. PowerSC can be used to manage AIX systems at AIX v6 tl7 or AIX v7 TL1 or higher and VIOS 2.2.1.0 or higher.

***Trusted Logging***

Trusted logging is the component that allows client LPARs to store log files on the VIO server thus ensuring that LPARs cannot modify or remove data from the logs. Under the covers it uses vSCSI shared storage pool technology to create a virtual log device that provides a “concatenate only” capability for the logs. Both MPIO (multipath I/O) and LPM (live partition mobility) are supported with trusted logging.

***Trusted boot***

Being able to ensure that boot files have not been tampered with is an important part of server/LPAR hardening. Trusted boot works with the PowerVM Hypervisor to guarantee the integrity of the operating system kernel – it does the checks during boot before the LPAR can issue any commands. Cryptography is used along with measurements to ensure that the image being booted has not been tampered with. Up to 60 LPARs are supported for each physical system and, when combined with AIX Trusted Execution, security and assurance can be provided for the boot image on the disk, the entire operating system and the application layers.

***Trusted network connect and patch management (TNCPM)***

Patching is a critical function in security management. Some of the security standard mandate how quickly certain types of patches must be applied. In order to manage this it is important to know which systems are backlevel. TNCPM is designed to detect images that do not meet established patch policies. It uses a combination of SUMA (Service update manager assistant) and NIM (Network install manager) to check each LPAR during activation, regardless of whether the

activation is a normal boot, a resumption after suspension, or as the result of an LPM move.

***Trusted firewall***

For many years I have used TCP Wrappers as a pseudo firewall on all my LPARs. It allows me to limit access to network services and it also logs all access – successful or failed – along with IP addresses. Trusted firewall provides firewall services to control network traffic between LPARs, including those within the same server. This means that LPAR to LPAR communication does not have to go to an external firewall but can still be locked down. Specifically, trusted firewall provides a packet filter firewall that lets you filter traffic by IP address, and by TCP or UDP ports and it can deal with inter-VLAN communications.

***Security and compliance automation***

This is a system security hardening tool where the pscexpert command now replaces the aixpert command and is used to deploy security controls on AIX and VIOS LPARs in order to help customers implement regulatory controls to meet compliance standards. It provides for 4 security standards and 1 general purpose database profile. The 4 security standards covered are: PCI-DSS (payment card industry data security standard v1.2), SOX/COBIT (Sarbanes-Oxley Act and Cobit compliance), DoD-STIG (Department of defense security technical implementation guide and HIPAA (Health insurance portability and accountability act). pscexpert can be used to set the security to low, medium, high or any of the four security standards and can lock down and do compliance checks on the network, services, file permissions, firewall and users and groups. A test server can be used to setup the security policies, which end up in an XML profile file. That XML file can then be propagated amongst the LPARs that need to be protected. pscexpert can then be used to report compliance violations and these reports can be scheduled regularly in crontab or by using RTC (Real time compliance). Additionally compliance audit reports in a .csv format can be generated.

***Real time Compliance (RTC)***

RTC provides for real time monitoring of file content, file access and security policy changes. The heart of this is a pseudo filesystem called AHAFS (autonomic health advisory file system). Operating system files get registered in the AHAFS and notifications are produced whenever a registered file changes. As an example, if /etc/security/login.cfg is registered and someone adds a shell to the end then an event would occur and notification of that event would take place.  How the notification occurs depends on what the compliance controls are set to, but could range from logging the event to sending emails.

***Summary***

There are many ways to provide security for a POWER server. Security does not just mean LPAR and server hardening – as we have seen it starts with people and encompasses the whole environment needed to support the application to

be run. However, in terms of LPAR hardening, PowerSC offers some great functionality that can be automated to ensure that your systems meet their compliance goals so that they can pass the audits. With that said don't forget to include firmware (server and adapters) updates in any security compliance plans as many security problems also get fixed at that level. Security needs to be a team, multi silo approach where everyone works together to provide the multiple layers that ensure the systems are as secure as possible.

**References**


Managing Security and Compliance in cloud or Virtualized Data Centers using IBM PowerSC (SG24-8082)
http://www.redbooks.ibm.com/abstracts/sg248082.html?Open

IBM PowerSC Trusted Surveyor Technical Overview (tips0980)
http://www.redbooks.ibm.com/abstracts/tips0980.html?Open

IBM Virtual User Group
July 30, 2015 presentation on AIX Security
http://www.tinyurl.com/ibmaixvug

2013 presentation on AIX Security
http://www.circle4.com/movies/

TCP Wrappers
http://www.ibmsystemsmag.com/aix/administrator/security/TCP-Wrappers-Provide-Robust-Logs/

Trusted Surveyor
http://www.ibmsystemsmag.com/aix/administrator/security/security-trusted-surveyor/