Zeus Web Server and HP Secure Linux

Andy Pearce
andy_pearce@hp.com

HP WORLD 2002
Conference & Expo

Running the Zeus Web Server with HP Secure OS software for Linux

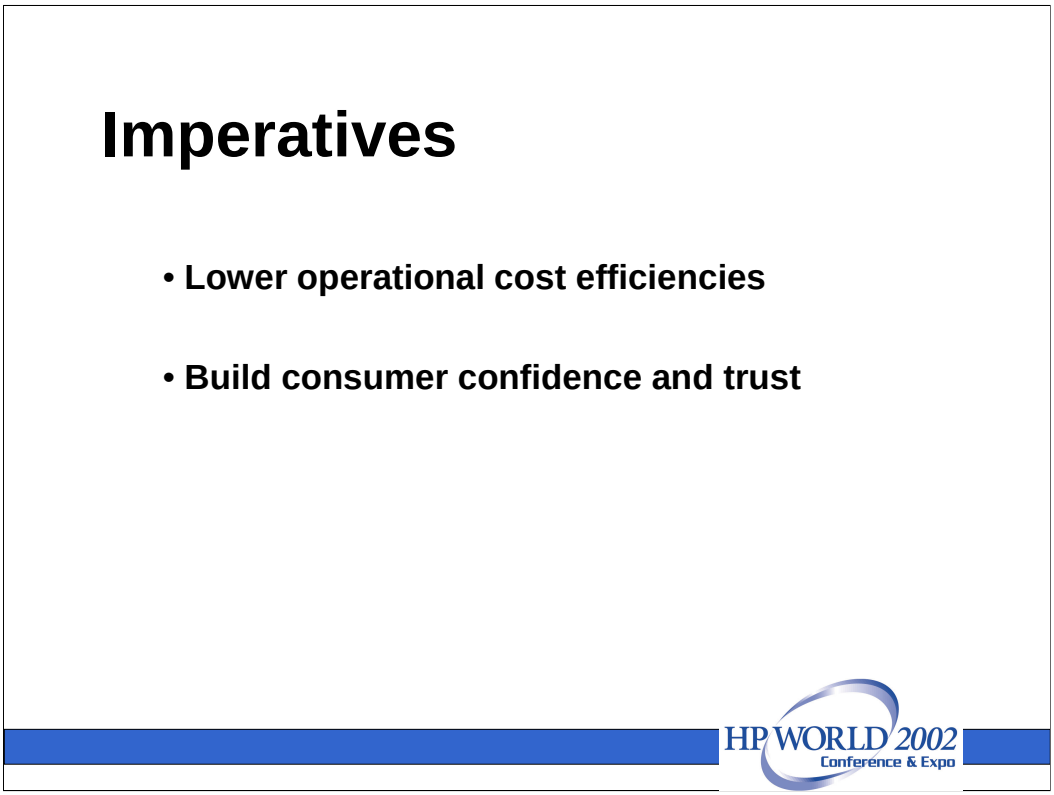
Andy Pearce

There's no let-up in either the revealing of new web server vulnerabilities or the quest for more and better security of web server software. This is the past, and the future.

The web site is the internet front-line for any organization; the face, the first impression we get. Web sites belonging to organizations giving a good impression invariably have two important qualities:

1. Speed (responsiveness)
2. Confidence (in the brand and company or organization)

To create a secure web service solution for general purpose, fast and scalable for the real world, engineers from HP and Zeus Technology have integrated Zeus Web Server (ZWS) into HP Secure OS software for Linux, or HP Secure Linux, environment. Here we will describe the steps needed to protect ZWS components and a database application within HP Secure Linux. We considered security implications of different schemes for separating application components in compartments. This investigation precedes any official release of ZWS for HP Secure Linux.



Responsiveness - the perception of quick response, is a major factor in providing an impressive service. Punters are paying the extra for broadband. Now its time for the busier web sites to do everything they can to offer a high performance service.

Investment in network, application servers and back-end applications often dwarfs the expenditure on the web server itself. However, the web server and intelligent HTTP/HTTPS traffic management can make a remarkable contribution to efficiency improvement, which in turn will reduce operating costs.

Confidence – many people don't really trust the web. They may ask:

- Who am I dealing with here?
- Is my information secure?
- Are they going to rip-off information from my PC and use it against my wishes?
- Could a fraudster get my credit card from this site?
- What happens to my personal details if they go out of business?

… E-commerce requires the building of user trust and confidence in the brand being presented on the web site. Conversely, the publicity from compromised web site security and theft of customer's personal data destroys trust and confidence in that brand.

Risk management - Defensive security of publicly accessible servers calls for risk management analysis [Garfinkel, Spafford, 1991]. But what is the risk? What threat does a "hacker attack" pose?

To some, web site attacks are just an annoyance. Others argue:

•Web site defacement is just the tip of an iceberg of a far greater problem. If these guys can do it for fun, how many more are doing it for criminal gain?

•Individual system administrator's professional credibility is attacked, which may affect your job!

•The brand being attacked can receive negative publicity, which may affect sales and the brand's market value.

•Public trust in the company's ability to manage its own security, and hence security of private customer information, is undermined. If these attackers can stomp all over this web site, they've probably got my credit card number, email, password, and address, right?

•General public, and investor, confidence in the web as a medium for electronic commerce is undermined.

•An insecure web presence cannot survive commercially.

These arguments create uncertainty and slow down growth and investment in web services. Only successful attacks are publicized – no-one hears about the attacks that are thwarted, or the administrators quietly keeping their systems secure year after year.

"… Our servers are now overloaded."

Caution:

Slow web service can ruin your day!

Even large, expensive infrastructures can fail to scale.

HP WORLD 2002 Conference & Expo

Twin Peaks – Business credibility also requires the web site can actually do what its supposed to! Busy web services must be able to scale up …

•How many simultaneous connections can be handled?

•How much headroom is there to handle peaks?

•What's the rate that headroom gets taken up, and is there a suitable capping mechanism?

•How many virtual web sites can be managed in a hosting environment?

The scalability of any e-commerce solution can be affected:

•The network supplied by your ISP or telephone company

•The web server

•The "back-end" and middleware software products; application servers, databases, etc.

Here we look at building a relatively low cost, high performance solution stack that can scale up;

•Zeus Web Server

•PHP (application level)

•MySQL (database)

•HP Secure Linux

Make it snappy!

- **What - too cheap to buy a fast server?**
- **Oh! So wasting my time's not a problem?**
- ***We all hate slow web servers.***

HP WORLD 2002 Conference & Expo

Speed – we hate slow response. Anger and frustration are common reactions to having to wait:

- What? Are they too cheap to buy a decent web infrastructure?

- Do they think wasting my time is better than upgrading to something that can respond half quickly?

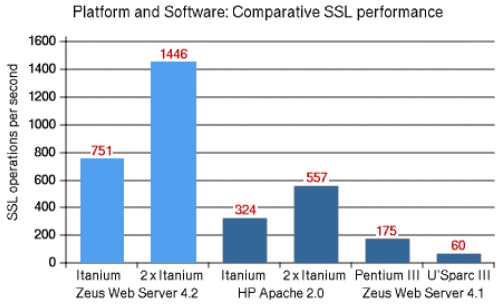
… Broadband makes slow web sites stand out even more, users will become more selective. Many web sites are geared to handle their normal rates of web requests. They need more headroom to be able to deal with high peaks that occur when something attracts large numbers of people to their site.

Two well-known web servers that HP recommends are Apache and Zeus. The ubiquitous Apache Web Server is what users often start with on Linux, many applications come with an Apache server, and HP has included an Apache web server with HP Secure Linux.

However, to grow, whilst keeping operational costs low, requires more efficient web server software as well as high performance machines. This is where Zeus comes in. If you have a busy web site, or you're doing mass web-hosting, Zeus excels.

Zeus

- **Speed**
  - transactions/sec
- **Scalability**
  - simultaneous connections
  - headroom
  - number of virtual servers
- **Manageability**



HP WORLD 2002 Conference & Expo

1. **Security**: With SSL as standard, built-in security features to combat DDOS, and virus/worm attacks, ZWS is chosen for secure web solutions. ZWS can protect Microsoft IIS web server from Nimbda and CodeRed virii.
2. **Management:** The Administration GUI features are in line with HP's approach to simplification of overall management of web infrastructure, whether that's for hosting many web sites, or running a very busy web site.
3. **Clustering:** ZWS has clustering admin capabilities built-in as standard. No barriers to scale-up as web services are split across many servers.
4. **Efficiency:** The efficiency of the ZWS non-blocking IO state machine, and decoupled service processes gives its well-renowned speed and scalability.

HP conducted SSLPerf benchmarks with Zeus on Itanium 2 running HP-UX. The scaling of measurements with 1 and 2 cpu give an indication of the efficiency of the Zeus Web Server.

SSLPerf results:	1 CPU	2 CPU	scaling	(SSL transactions/sec.)
Zeus:	751	1446	92%	
Apache:	324	557	86%	

The numbers will be lower on IA32 Linux servers but the scaling is similar.

http://www.hp.com/products1/itanium/solutions/commercial/secure/zeus.html

Call to action

- **Understand the dangers**
- **Evolve the barriers**
- **Follow the advisories**
- **"Open" security measures**
- **Build trust**

HP WORLD 2002 Conference & Expo

Building trust - Call to action:

•Convince yourself: attacker threats to business assets are real.

•Don't confront the attacker with rhetoric – just quietly erect the barriers that make attack less worthwhile.

•Stay tuned to the advisories, stay ahead. This is the best way to "know the enemy".

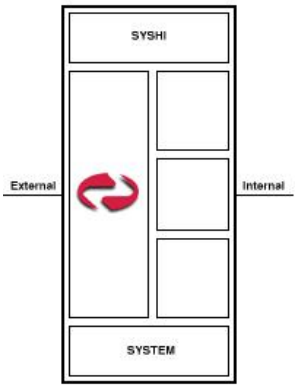
•Tell the customer what you can to reassure them about security investments you make, without giving your potential attacker useful information.

•Build trust with your customers and business partners.

Its likely there will always be exploits against individual applications running on any web server. HP Secure Linux allows you to contain applications so that if a break-in does occur, the attacker cannot easily damage other parts of your system.

Compartments

- Separate applications
- Separate file system
- Define allowed interaction
- Isolate vulnerabilities



HP WORLD 2002 Conference & Expo

HP Secure Linux: One central idea behind using HP Secure Linux for a web server and applications is compartmentalization. Using compartments to separate the web server from the other services, you can limit access to your system as a result of a vulnerability in one component.

Applications can be installed in the main file system, or in their own file tree within a compartment.

In the former case, compartment rules may still restrict what resources a process is allowed to access. So even though the application is installed in its normal root location, the process may still only be granted read access to that file system. In the latter case, the processes can be run in a chroot'd environment with no visibility of files outside the compartment.

We can configure Zeus to run as user:nobody, group:nobody. When you list the zeus processes you will see one zeus.web process running as root. It needs to do this in order to obtain ports controlled by root; e.g., port 80. Other spawned zeus.web processes run the web service, and they can run as nobody.

It is possible to run one part of the Zeus web server in one compartment, and another part in a different compartment. For example, a separate compartment for the administration server to be accessed from a dedicated admin LAN.

Steps to integration

1. Validate (SYSHI)
2. Create compartment
3. Install
4. Create Rules
5. Test

HP WORLD 2002 Conference & Expo

Validation – the easiest way to start is to validate that the application will run on HP Secure Linux in System High (SYSHI) compartment.

•Copy the files to be installed (use sftp if remote)

•Login with TLX_ADM and TLX_PRC capabilities; e.g. as tlinuxadm

•su to root, and switch to the SYSHI compartment

•Untar and install Zeus as normal; e.g. to /usr/local/zeus

As we are in System High, we don't need to define any rules to run. Zeus will run as normal. System High is a good starting place to test out that the application has the correct environment to run, before taking the next step to contain the application within a compartment.

•Test that it all works as expected

•Shut down the service and uninstall Zeus

Contain the application

- Create compartment
- Define rules

COMPARTMENT zeus -> HOST * PORT 53 METHOD UDP NETDEV any
HOST * PORT 53 -> COMPARTMENT zeus METHOD UDP NETDEV any
HOST * COMPARTMENT zeus PORT 80 METHOD TCP NETDEV any
HOST * COMPARTMENT zeus PORT 443 METHOD TCP NETDEV any
HOST * COMPARTMENT zeus PORT 9090 METHOD TCP NETDEV any

Create compartment – a single command creates the compartment; "tlcompadd zeus".

The Zeus Web Server needs to be able to resolve names, so it must have rules for accessing DNS via port 53. It also needs TCP access via port 80 (default HTTP location), port 443 (HTTPS), port 9090 (for Zeus Admin GUI interface). So the rules defining access to/from "zeus" location are simply:

COMPARTMENT zeus -> HOST * PORT 53 METHOD UDP NETDEV any
HOST * PORT 53 -> COMPARTMENT zeus METHOD UDP NETDEV any
HOST * COMPARTMENT zeus PORT 80 METHOD TCP NETDEV any
HOST * COMPARTMENT zeus PORT 443 METHOD TCP NETDEV any
HOST * COMPARTMENT zeus PORT 9090 METHOD TCP NETDEV any

Running the Web Server

- File system
  - Copy files required
- Run compartment
- Seal compartment

HP WORLD 2002 Conference & Expo

File system - The Zeus Web Server is very self-contained, and requires relatively few resources outside its own installed files. It was an easy decision, therefore to install the entire application within the file system contained within the compartment.

The steps we took were:

•Install ZWS as normal within the new “zeus” compartment; /compt/zeus/zeus.

•Remove any startup scripts from the /etc/rc* directories.

•Make the appropriate edits to startup files within the zeus compartment;

•Copy over the files that ZWS requires that are not installed by tlcompadd in the compartment.

•Start the compartment – this action starts the Zeus Web Server

•Seal the compartment (optional) prevents processes doing “su root” or any suid programs from running.

You still take the normal precaution to have the web server agent run as “nobody” rather than root, but even if the web server is somehow compromised, the attacker only has access to files and processes within the zeus compartment. Even with root access the attacker cannot access files and processes in other compartments; e.g., a database.

Applications

- Add FastCGI (or CGI)
- Add PHP
- Create compartment(s)
- Experiment

HP WORLD 2002 Conference & Expo

Installing FastCGI and PHP – Applications that form part of the backend of a web server can be separately compartmented. They often require more system resources, and so are frequently not installed within a separate compartment file system. If an attacker breaks into a compartment via, say, a PHP vulnerability, they will have access to the FastCGI and PHP compartment processes only. They will not have access to the web server, web server files, or database processes.

Apache uses an integrated mod_php approach to running PHP. Zeus uses FastCGI, and has been measured as 45% faster than Apache/mod_php.

See http://support.zeus.com/products/v3/php.html#perf for details.

•Install FastCGI

•Install PHP4

•Configure Zeus to use PHP via FastCGI

There are different options to consider when configuring this combination. One approach is to have FastCGI and PHP4 running in a single compartment. Create rules to access the FastCGI runner from the web server. Modify the startup and shutdown scripts within the compartment and remove any scripts in the /etc/rc* system directories. This gives the best performance.

MySQL

- Same approach
- Install in root file system
- Rules to enable access from PHP

MySQL – MySQL is a very popular database used by many web applications. PHP and MySQL are often used together as a combination with Zeus, or Apache. We investigated how to integrate Zeus with PHP and MySQL within HP Secure Linux.

We repeated the approach to installing MySQL; i.e., start with an installation within System High compartment.

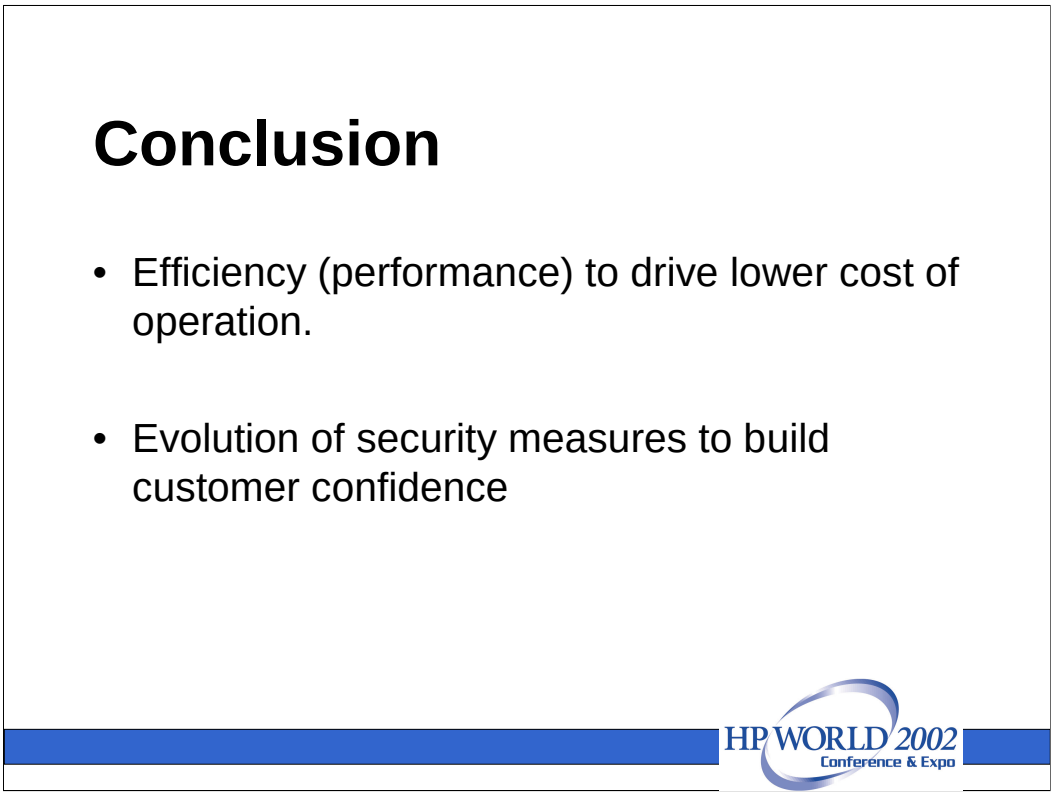
Familiarity

- Pilot the application
- Define the issues (for your circumstances)
- Security is knowledge

Experience (gaining familiarity with the OS environment) – We've seen that installing a single application is fairly straightforward. When you come to install a number of applications that need to work together as a unified system, its likely the possibilities will become more complex. Especially if this the solution is designed to be general purpose.

Our recommendation is to pilot a complex integration with the applications and data you are likely to use. It does take some time to get used to the security in HP Secure Linux. As the OS environment becomes more familiar, spend time trying different approaches to separating components. Weigh up the advantages of different approaches to your system. Choose and adopt the approach that suits you best. The approach you choose will take into account the threat you perceive from security advisories against the applications you use …

"Know the enemy and know yourself: One hundred challenges without danger;
Know not the enemy and yet know yourself: One triumph for one defeat;
Know not the enemy and know not yourself: Every challenge is certain peril."
Sun Tzu



Conclusion – A repeatable methodology for installing a new application in HP Secure Linux has been discussed. Installing an application within a compartment isolates the processes and resources. An attacker has limited access to the rest of the system if a vulnerability is exploited.

The approach for integrating several components to work together is more complex and requires a greater understanding of the system needs. We have discussed the needs for a secure web service solution with low cost of operation. HP Secure Linux with the Zeus Web Server and applications such as PHP and MySQL is one such combination that can be adapted or extended to meet these needs.

More complex integration requires some knowledge of potential hazards from exposure to vulnerability in any component. Security is constantly being challenged. Customer confidence in a web presence demands both responsiveness and security.

References:

Garfinkel, Spafford, Practical Unix & Internet Security, O'Reilly, 1991.

Zeus: http://www.zeus.com

PHP: http://www.php.net

FastCGI: http://www.fastcgi.com

MySQL: http://www.mysql.com

HP Secure Linux: http://www.hp.com/security/products/linux