Global Information Assurance Certification Paper

A confidential internal security audit of the *ftp.ok.com* upgrade.

EXECUTIVE SUMMARY

Open Kinomo's current process of providing ftp access is outgrown and must be replaced. Replacing the current ad hoc, largely unmanaged, distributed access points with a single server will allow more efficient centralized management at the risk of a single point of failure. This risk can, and should, be eliminated by adding a second ftp server and placing both under the load balancing and failover system Open Kimono uses for world wide web access. In the meantime, to counter this risk, additional steps need to be taken to assure availability of the new ftp server. Since this server will be accessible by the Internet community, additional steps need to be taken to assure that it is secure.

This report details the key aspects of building the new server to handle all customer ftp access.

The server, *ftp.ok.com*, will fit within the Open Kimono environment and follow the practices and procedures currently in place. It will be placed behind the firewall and accept only ftp traffic from the Internet.

Specific to the ftp server will be the special wu-ftp environment. No anonymous ftp access will be allowed. Clients will operate in a special chroot environment. This means that they will have access to a limited number of commands, and will not be able to see files or directories outside their specified area.

Management of the external data disks (/wuftp) will be performed outside the Information Infrastructure group.

Considerable reliance is placed on the overall security practices of Open Kimono. It is assumed that the internal network is secure, that communications, including logging information, is secure. Internal users and considered honest and care should be taken to avoid honest mistakes.

BACKGROUND

Open Kimono Inc (OK) provides specialized financial information to contract customers. The information provided is recognized as more timely and more in depth then what is available from commercial news sources, even those that specialize in financial information such as Dow Jones.

The information gathered by Open Kimono falls into two generalized categories; first regular reports that are provided at predetermined intervals, including the daily, weekly, monthly and quarterly reports, and, second, special in depth reports by company or industry as contracted individually by both regular and occassional clients.

The information is disseminated based on instructions from the customer. In keeping with national trends, most information today is disseminated electronically using Intranet technology. However many special reports are still printed and delivered to the customer by hand.

Although *www.ok.com* is the primary access point for clients, many customers rely or supplement that with ftp technology. Advantages are that large graphic reports can be easily downloaded and printed locally, customers with geographically dispersed offices can access identical reports, and electronic copies of copies can be disseminated within the client's own network. Many reports are not printed to the web. Each of these advantages is associated with unique concerns.

Currently there are seven OK servers providing ftp access, each generally used for specific types of reports and/or clients. Each of these servers also provides other functions. Expectations that ftp access will decrease have proved to be incorrect, all metrics relating to ftp access have grown.

In order to improve service all ftp service will be combined and provided through a dedicated ftp server, *ftp.ok.com*. Because *ftp.ok.com* will be a direct interface with clients, and accessible by the Internet, high availability and a tightened security stance are priorities.

REQUIREMENTS

The business requirements are:

- 24x7 availability from the public Internet.
- There are currently 307 client accounts and 57 internal accounts. Allow for 50% growth.
- Allow for up to 200 simultaneous connections.
- Allow 50GB for ftp data and archives. This grows unpredictably.
- Clients should have access only to their contracted data.
- Clients will only read (get) data. No clients upload data.
- Data will be placed and/or removed only by OK employees or internal processes.
- All accounts should be able to login and put/get data through automated processes.

- No anonymous access required.

RECOMMENDATION

Open Kimono extensively uses Sun Solaris servers. Although IBM's AI/X, Windows NT and Linux are also being used, the Sun Solaris platform will be used based on it's proven reliability, performance, plus already having a knowledgeable support staff. Solaris version 2.6 remains the standard for all OK Sun servers. There is no compelling reason for *ftp.ok.com* to vary from that standard.

Following is the best of three quotes for a recommended hardware/software configuration.

Server Hardware and price estimate (1)		
CPU	Sun Ultra 2 Model 2300 w/	$ 11,600
	2@ 300MHz 2MB UltraSparc II	
	1 GB RAM	
	2@ internal 9GB disks	
	Solaris Operating System license w/ CDROM	
I/O	2@ Wide Differential S-Bus SCSI cards	$ 1,500
Disks	2@ External Sun Multipacks w/4@ 18GB Disks	$ 5,500
	(8 disks total)	
S/W	Veritas Foundation Suite w/ Doc. & CDROM	$ 150
	Video -none-	
Support	Direct Assist 24x7	$ 900
	TOTAL	**$ 19,650**

Open Source Software Required	
rsync	Used to synchronize the boot and alt-boot disks
lsof	System administration utilities
top	System administration utilities

gzip	System administration utilities
gdf	System administration utilities
sudo	User permissions utility
ntp	Time syncronization
TCP-wrappers	System monitoring software
wu-ftp	ftp software

HARDWARE CONFIGURATION

Each of the two internal disks will be bootable. The system will boot off the primary disk; the second disk will be an alternate boot disk. The alternate disk will not be mounted at boot or during normal operations. The disks will be synced manually on a weekly basis. Details on the functions and configuration of the alternate boot disk follow. All system files, including application software and internal user home directories will be on the internal disk.

Each set of four disks in the external multipacks will be built into a single filesystem and the two filesystems mirrored using the Veritas software. The filesystems will be striped to increase throughput. All data and external users home directories will be on these external disks.

NETWORK CONFIGURATION

All Internet traffic to ok.com is routed through F5's Big IP load balancing and failover switch and then to redundant firewall hosts each running Checkpoint Firewall 1. Although at this time there is no load balancing function and no failover system, ftp traffic will follow this pattern. The firewall translates the external address (90.10.16.x) to the internal address (198.7.27.x). Currently ftp traffic is allowed to any host. This will be reconfigured to allow ftp traffic only to *ftp.ok.com* and deny all others. Additional availability and security related network concerns are beyond the scope of this report.

The current 100/mbs-switched network will handle anticipated ftp loads.

OPERATING SYSTEM CONFIGURATION

The standard server installation of End-User cluster plus documentation (man pages) and the current Recommended Patch Cluster will be sufficient for *ftp.ok.com*. NIS and NIS+ services can be removed. The Veritas software will need to be installed to configure the external disks.

Security related modifications:

The following services are normally in the boot process. None are required for the operation of the ftp server. Several of these create issues that make the server volnerable to attacks that have been puplished on the Internet. To help make *ftp.ok.com* a more reliable platform, they should be moved out of the boot schedule by placing a underscore (_) in front of the filename:

```
/etc/rc2.d/S30sysid.net              /etc/rc2.d/S71/sysid.sys
/etc/rc2.d/S72autoinstall            /etc/rc2.d/S60nfs.server
/etc/rc2.d/S73nfs.client       /etc/rc2.d/S73cachefs.deamon
/etc/rc2.d/S74autofs                 /etc/rc2.d/S80PRESERVE
/etc/rc2.d/S80lp                     /etc/rc2.d/S85power
/etc/rc2.d/S93cacheos.finish         /etc/rc2.d/S99dtlogin
```

The following script will assure that system daemons do not create world-writable files. (2)

```
echo 'umask 022' >/etc/init.d/umask.sh
chmod 744 /etc/init.d/umask.sh
for dir in /etc/rc?.d
do
ln -s ../init.d/umask.sh $dir/S00umask.sh
done
```

By adding the following networking parameters to the end of /etc/init.d/inetinit the system will have some protection against several common Denial of Service attacks. (3)(4)

```
ndd -set /dev/tcp tcp_conn_req_max_q0 10240
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip_send_redirects 1
ndd -set /dev/ip ip_ire_flush_interval 6000
ndd -set /dev/arp arp_cleanup_interval 60
ndd -set /dev/ip ip_forward_directed_broadcasts 0
ndd -set /dev/ip ip_forward_src_routed 0
ndd -set /dev/ip ip_forwarding 0
ndd -set /dev/ip ip_strict_dst_multihoming 1
```

Stop unneeded serial port access (5)

remove following line from /etc/inittab (5)

```
sc:234:respawn:/usr/lib/saf/sac -t 300
```

Remove unneeded crontabs (5)

```
cd /var/spool/cron/crontabs
rm adm lp sys
```

APPLICATION CONFIGURATION

Open Kimono maintains an administrative server (gorilla.ok.com) that is used to create CDROMs of current builds of open source software. The open source programs listed above should be transferred from *gorilla.ok.com* generated CD's to *ftp.ok.com*.

Configuration of TCP Wrappers

The purpose of the TCP Wrappers is to provide additional access protection. We want all external users to have ftp access only, and all internal users to have all access that is not otherwise filtered.

The addition of banners, legal notices concerning allowed access to the system, have proven to interfere with the automated log-on used both by clients to get information and internal processes that put information. Because of this and the difficulty in maintaining known work arounds, banners will not be configured. It is strongly recommended that banners be introduced if automated processes can be separated from manual logins, which generally accept the banners. TCP Wrappers should be configured to log to the remote logserver, *owl.ok.com*. Log rotation and monitoring is handled separately on *owl*.

To allow access the file /etc/hosts.allow needs to contain the following lines:

```
in.wu-ftp.d     :     ALL
ALL             :     ok.com
```

The File /etc/hosts.deny needs to contain the following:

```
ALL             :     ALL
```

Configuration of wu-ftp

No user application other than wu-ftp, which provides the ftp access should be configured on *ftp.ok.com*. The most current version (2.6.1 or later) of wu-ftp

should be downloaded from *ftp.wu-ftpd.org/pub/wu-ftp*, complied on *gorilla.ok.com* and transferred to *ftp.ok.com*.

No anonymous access is allowed on *ftp.ok.com*. The information is provided to paying customers only. Guest accounts can be created for specific reports and will be deleted immediately. All external (client) ftp accounts will be only in group ftpusers. ftp.ok.com will rely on UNIX filesystem permissions and especially group membership to control who can read and write information. Internal users, who will put and remove files will have regular accounts, as opposed to the chroot environment that external accounts are limited to.

Since the overhead for setting up multiple chroot homes is low, a minimum of four seperate chroot environments should be set up, one each for:
1) Each large, multiuser client (/wuftp/private).
2) Each type of recurring report that is accessed by several clients (/wuftp/report)
3) Unique reports for low volume clients (/wuftp/general)
4) Miscellaneous and guest accounts (/wuftp/special)

Within each chroot home a home subdirectory will contain the subdirectories for each account. The customers home directories and all files and directories below will be owned by the customer and the group ftpdata. Permissions will be such that the owners can read execute while the group has read write execute and no world access. (i.e. chmod 570 *)

Regular accounts will be created for OK users who will be responsible for removing obsolete data and placing current data. These accounts will belong to group ftpdata.

Configuring the Alternate boot disk.

The primary functions of the alternate boot device are to quickly recover from a crashed boot disk and to provide a quick back out method if software upgrades or patches adversely effect the system (6). Although only the root (/) filesystem is strictly required for an alternate boot disk, OK includes all system specific file systems in the alternate disk. This includes root (/), /usr, /var, /opt. Additionally home directories (/home) and swap (tmp) are included on the alternate boot disk.

The steps required to create the alternate boot disk are:

1) Partition the alternate boot disk exactly as the boot disk.
2) Make the alternate boot disk bootable with the following command:
installboot /usr/platform/`uname –I`/lib/fs/ufs/bootblk <special_device_name>
3) Create mountpoints with alt_ prefix (i.e. /usr & /alt_usr)
4) newfs the filesystems.

5) Add to /etc/vfstab with the mount at boot option set to no.
6) Mount the filesystems and copy the data from the boot device to the alt boot device.
7) Edit /etc/vfstab. Make sure each device's /etc/vfstab properly boots from and mounts its own filesystems.
8) Test the alternate boot device. From the OK prompt type 'boot disk1'
Note: The boot device is normally aliased to disk0 and the second internal disk to disk1. To find the system name for the device type 'ls –l /dev/dsk/cXtXdXs0' (replacing XXX with the path to the alternate device). This will show the where the link /dev/dsk/cXtXdXs0 points to. A PROM alias can be created for altboot to the hardware device file and from the OK prompt use the command 'boot altboot'

Synchronizing the alternate boot device is done with the rsync (7) program. Scripts need to be created that will
1) Create the alternate mount points
2) Mount the filesystems
3) Synchronize the data
4) Unmount the filesystems
5) Remove the mountpoints.

Care needs to be taken that the /etc/vfstab is not copied over. (Excluding files from synchronization is a rsync option). This synchronization should be run weekly and started either manually or through cron.

MAINTENANCE

General system maintenance of *ftp.ok.com* will be done by the Information Infrastructure Group within Open Kinomo in accordance with the company's best practices.

Logging of warning and above events to kern, deamon, auth and cron is done to the central log server owl.ok.com. Since wu-ftp logs messages to the user facility, messages of warning and above to the user facility should also be logged. Monitoring of *owl.ok.com* is done on a regular basis. Additionally logging of these events plus those to user and mail facilities are done locally to /var/adm/messages.

ftp.ok.com should be imeadiately put in the Open Kimono network backup schedule. Open Kimono has a central back up server (*ellie.ok.com*) utilizing Veritas Netbackup.

Account management is likely to be the most labor intense task faced by the system administers. Because of the special chroot environment it is

recommended that a primary and backup administrator be designated as the account management team to the sales and marketing department. They will co-ordinate creating and removing accounts, along with setting up special requirements.

Open Kimono has created a CD-ROM with a copy of Tripwire compiled for use with Solaris v2.6. A signatures of both the boot and the altboot disk need to be taken. These can be verified on the regular rotation of the secuirty audits.

VOLNERABILITES

Denial of service (DoS) attacts are the most serious threat. They are difficult to defend and can damage the reputation of Open Kimono to deliver timely information. Several known DoS attacks are defended in the steps outlined. Additional DoS protection is provided by the ok.com network environment.

There is no attempt here to encrypt data being transmitted. Although this information is the lifeblood of Open Kimono, and stealing it (even worse, changing it) could significantly damage Open Kimono, customers do not appear ready at this time to support encrypted transfers. Adding digital signatures is a recommended step that will allow customers to verify the source of the information.

REFERENCES:

(1) Quote #SN072700-03 dated July 27, 2000 by S. North of Solaris Communications Co.,

(2) Brad Powell, Dan Farmer, Matt Archibald. “The Titan Security Package”, http://www.fish.com/titan, from module add-mask.sh

(3) idib., from modules adjust-arp-timers.sh, disable-ip-holes.sh

(4) Jens Voeckler, “Solaris – Tuning Your TCP/IP Stack”, http://www.rvs.uni-hannover.de/people/voeckler/tune/EN/tune.html

(5) Hal Pomeranz, “Solaris Security Step by Step”
SANS Institute, 1999

(6) Jim McInstry. “Alternate Boot Devices”
Sys Admin Magazine, November 1998.

(7) Andrew Tridgell & Paul Mackerras, rsync
http://rysnc.samba.org