IBM OS/400 - AS/400 – Recognizing and Securing the System

Cmdr. Dave Pettinari
Pueblo County Sheriff's Office
davepet@cops.org

Information provided by:

John R. Lough
Account Exec, ACS
Colorado Springs
john.lough@brctsg.com
970.483.6584, 800.800.2725

Affiliated Computer Systems headquartered in Dallas, with an office in Colorado Springs. 35-40 Colorado counties are on this, Social Services, etc.

AS stands for Application System 400. Handle up to 300 comm lines coming in, up to 7000 client nodes, hard drive size up to 4300 gigabyte, lots of capacity, lots of room to hide stuff. Capable of C-2 security. RAM up to 40960 megabytes.

Black in color, usually, cabled into an ethernet hub. Very secure system.

Used by:

- Many businesses
- City and county governments
- Colorado state court system
- Department of Social Services
- School District 60

Great opportunity for fraudulent welfare records, wiping out convictions in court system, etc.

Administrator on site may not know how the system functions, nor do they have security knowledge.

Screen looks like UNIX, green and black, with command line at bottom. Lot of machines are dumb terminals without Windows, but capable of converting to a GUI screen, so you may see some of these.

Can log in under four or five different profiles at one time. Stealthy user could create a number of accounts that look like system accounts.

Menu driven or control language commands. GO (name a menu). Need Secofr privileges to change password, lock people out, etc.

WRKUSRPRF *ALL – gives you user profiles and allows you to work with them. Every keystroke made can be saved with logging. Need a programmer to look at it; most operators are not aware of how to do this.

Menu driven commands:

- GO setup

- GO assist
- GO sectools

If you have the right privileges, these commands will allow you to do just about anything in the system.

To disable users:

- Change user profile
- Change password to another password
- Change user status to *disabled
- Remember multiple profiles (dave, dave 1, mike, whatever)
- Multiple sessions possible

System-assigned password is same as user name, and many people keep this for a long time if they are not forced to change.

Preserve electronic evidence by backing up to tape. Most terminals do not have floppy or zip drives. Most servers have capability of backing up all data on PC hard drives. Can be read-only or shared with others. You can do a 2-gig backup tape for evidence, and another one to use on another AS/400 machine to do your search and analysis of information on that system.

Change User Profile – CHGUSRPRF
Need SECOFR privileges (security officer) in order to nuke someone else or change privileges.

This operating system is virtually virus proof, and harder to hack into than UNIX or other systems. Every file has security set up from zero to 90 level, and there are overall five levels of security.

Capable of being set up as an ISP server, ISDN lines, etc. Very expensive piece of equipment, so smaller ISPs may not buy. But someone with privileges on a system could easily set up a covert, pirate ISP.

Shut down the user
- Create a profile that looks like IBM internal user
- Or use sysadmin as sender
- Send a break message – interrupts
- Make it sound like system malfunction or maintenance
- Remember multiple sessions/profiles

Encourage user to sign off with message:
All users sign off immediately. Spool failure on SP8846 Library…

Windows Interface
- Standard operating procedures apply for forensic processing
- Get user away from computer
- File storage can be on either PC or AS/400
- File storage can be on either PC or AS/400
- In emergency, identify node and pull plug from the hub. Secures the AS/400 but doesn't secure the PC.
- Inquire about tape backups – data could be there

WE WILL NEED HELP FROM IBM OR OHER FORENSICS LABS TO
SAFELY EXAMINE AS/400 FILES.

AS 400s talk to each other. Be aware the suspect may have access to more than one system, and could have moved some evidentiary data over to that system.

IPL – same as "booting" in the AS/400 world.

Can go to a menu to do an automatic backup at that very time. Can also go to a menu to power the system down immediately.