"You mean I just can't run the OS out of the box?"

Milo Medin
Deputy Project Manager
NASA Science Internet Office
Moffett Field, CA 94035
medin@nsipo.nasa.gov

NSIUWG/CI '93
4/28/93
San Diego, CA

Milo Medin	NSIUWG/CI Conference '93	4/28/93

Host Security

Vendor Operating Systems issues

- Vendors need to keep adding new features, and are usually under a lot of pressure to get releases out the door
- Vendors keep trying to make system configuration easier
- Vendors don't usually configure systems with the Internet environment in mind
- Operating systems are growing increasingly dependent on the network for even minimal operation
- Vendors often view security considerations as a secondary issue - people rarely buy workstations because of security features

Milo Medin	NSIUWG/CI Conference ’93	4/28/93

Host Security

Default settings

- Password files often contain default system and user accounts that must be changed
- Yellow Pages (i.e. NIS) is usually configured in by default
- Several system files (passwd, hosts.equiv, etc...) are configured to use YP by default (the infamous “+” sign in files)
- Unneeded system daemons and services are often started up (rexd, etc...)
- Network software is often configured to allow unintended access by default (default DECNET account, tftp daemon, etc...)

Host Security

System software problems

- Configuration programs do the “wrong” thing (e.g. /etc/exports with filesystems exported to the world)
- NFS mount daemons tell anyone what filesystems are exported and who can mount them (i.e. showmount -e hostname)
- Filesystems have predictable generation numbers (fsirand can fix this)
- r-commands (e.g. rlogin, rsh, etc...) often can be spoofed by simple nameserver changes
- Plain old software bugs (in many proprietary systems, few people ever get to see the source code, and then expose latent bugs)

Milo Medin	NSIUWG/CI Conference ’93	4/28/93

Host Security

Summary

- Newer vendor OS releases generally have fewer problems and more security fixes (though BIG changes tend to introduce new bugs)
- Make a list of specific problems for operating systems you use, and patch them when you install a new system
- Keep an eye out for CERT announcements
- There is no substitute for a good systems administrator, as much of this knowledge is obtained through (often painful) experience