

Secure by Default

Scott Rotondo

Senior Staff Engineer

Solaris Security Technologies

What Is “Secure by Default” About?

- Eliminate services listening to the network
 - > Some services disabled, others local-only
 - > Exception: Secure Shell (ssh)
- Why disable network services?
 - > Any software can have bugs
 - > Network input transforms software bugs into convenient attack vector
 - > Unused services represent *unnecessary* risk
 - > Reduce the “attack surface” of the system
- By Default = before first boot

Other Approaches

- Minimization
 - > Avoid installing unused software
 - > Extra work to install later if needed
 - > Complicates patching of uninstalled components
- Hardening after installation
 - > Solaris Security Toolkit is one example
 - > Window of vulnerability before hardening
 - > Many systems are permanently connected to network

Built on Service Management Facility

- SMF services
 - > are referenced by name (FMRI)
 - > can be enabled or disabled
 - > store additional configuration in properties
- Profiles contain settings for multiple services
- Secure by Default delivers
 - > Additional SMF profiles
 - > `net services(1M)` command to apply profile and set service properties

Services Disabled

Service	FMRI
dtprintinfo	svc:/application/cde-printinfo
CDE subprocess control	svc:/network/cde-spc
DMI	svc:/application/management/dmi
SNMP	svc:/application/management/sma
Solstice Enterprise Agent	svc:/application/management/snmpdx
Seaport	svc:/application/management/seaport
X font server	svc:/application/x11/xfp
Internet print protocol	svc:/application/print/ipp-listener:default
SVM remote metaset	svc:/network/rpc/meta
SVM remote mediator	svc:/network/rpc/metamed
SVM remote multihost disk	svc:/network/rpc/metamh
SVM communication	svc:/network/rpc/mdcomm
rstatd	svc:/network/rpc/rstat:default
rusersd	svc:/network/rpc/rusers:default
telnetd	svc:/network/telnet:default
statd	svc:/network/nfs/status
lockd	svc:/network/nfs/nlockmgr
NFS client	svc:/network/nfs/client
NFS server	svc:/network/nfs/server
rquotad	svc:/network/nfs/rquota
NFS v4 callback daemon	svc:/network/nfs/cbd
NFS id mapping	svc:/network/nfs/mapid
ftpd	svc:/network/ftp:default
fingerd	svc:/network/finger:default
rlogind	svc:/network/login:rlogin
rshd	svc:/network/shell:default

Service Properties

Service	FMRI	Property	Values
rpcbind	svc:/network/rpc/bind	config/local_only	true , false
syslog	svc:/system/system-log	config/log_from_remote	true, false
sendmail	svc:/network/smtp:sendmail	config/local_only	true , false
smcwebserver	svc:/system/webconsole:console	options/tcp_listen	true, false
wbem	svc:/application/management/wbem	options/tcp_listen	true, false
X11	svc:/application/x11/x11-server	options/tcp_listen	true, false
CDE	svc:/application/graphical-login/cde-login	dtlogin/args	[null], -udpPort 0
ToolTalk	svc:/network/rpc/cde-ttdbserver:tcp	proto	tcp, ticotsord
calendar	svc:/network/rpc/cde-calendar-manager	proto	tcp, ticlts
BSD printing	svc:/application/print/rfc1179:default	bind_addr	[null], localhost

Default Configuration

- Solaris Nevada build 42
 - > New system installation: “limited” configuration
 - > New zone installation: “limited” configuration
 - > System or zone upgrade: No configuration change
- Solaris 10 update 3
 - > New system installation: Selected by install question
 - > Jumpstart keyword: `service_profile = [limited_net|open]`
 - > New zone installation: “open” configuration
 - > System or zone upgrade: No configuration change

Customization

- Run `net services` at any time to choose open or limited configuration
- Better approach: Start with limited configuration and enable what you need
- Examples:
 - > `svcadm enable telnet`
 - > `svccfg -s sendmail setprop config/local_only = false`
- Property settings (and command line above) are documented on each service man page

<http://www.opensolaris.org/os/community/security/projects/sbd>

Scott Rotondo

scott.rotondo@sun.com