Overview & Summary

University Computing Services (UCS) was contracted by the College of Engineering (COE) to assess the general state and security of their networked UNIX systems. The following report summarizes our findings regarding the COE server cluster.

Our report begins with an overview of the current computing environment in the College of Engineering. This provides both a context and basis for later discussion of the issues brought to light by the recently completed security investigation.

Next we identify and examine the specific vulnerabilities discovered, with attention to how they fit into the overall picture for COE and why they present a problem at all.

In the following section, we propose a means of categorizing and prioritizing threats with reference to the Ten Most Critical Internet Security Threats list published by SANS.

We then move to a general discussion of backups, administrative practices, and other related security policy questions.

Our report concludes with a prioritized summary list of the major areas of concern for COE and our recommended solutions. This table of Action Items may be used for reference as an executive summary of the more detailed contents of this report. An appendix of reference web sites is also provided.

We also want to note here that security is, by its very nature, an ongoing process. The fixes, patches, and solutions proposed here are not one-time panaceas, but the first steps that must be taken in a long series.

Key Features of the Department

There are approximately 60 faculty and staff in the College of Engineering, all of whom are potential customers. Our current customers include 20 professors / lab coordinators and their associated graduate students (usually two-five per lab). Hardware resources include approximately 50 UNIX clients in labs and on desktops as well as four centralized servers and their peripherals.

Current Server Configuration

Here we discuss the current configuration of the College's servers. In order to be able to judiciously improve what is being offered, we must first understand what arrangement of services already exist.

The College of Engineering servers are a heterogeneous mix of hardware platforms and Operating Systems (OS's). Even where the vendor is the same, the OS's have not been maintained in the same fashion (for example, one machine is running Solaris 2.4 while its neighbor is running Solaris 2.5.1). This kind of inconsistency makes security much more difficult: trying to keep analogous configurations in synch, adapting to the quirks of an additional OS, etc.
(See Action Item #3)

All server Operating Systems are far behind the current available revisions, both in the OS itself and patch sets. When vendor OS's are left unpatched, the vendor often will not support the system should problems arise. Unpatched systems are also left vulnerable to a wide range of well-known attacks. *(See Action Item #4)*

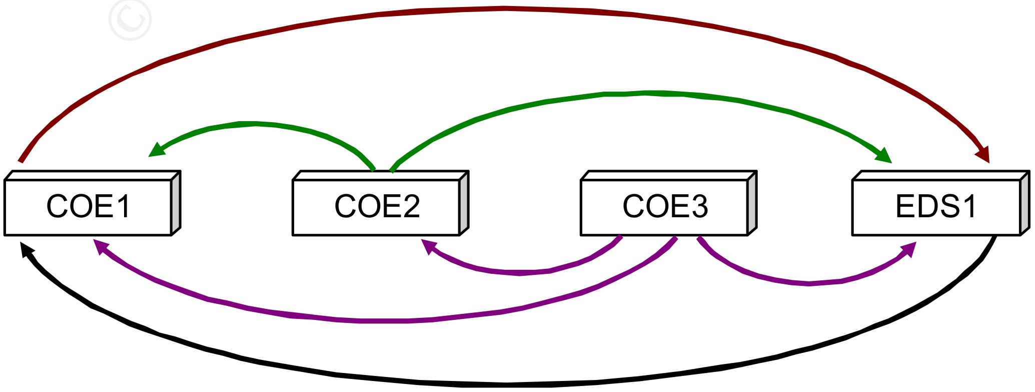
Each machine provides multiple services. We find it an especially dubious practice to provide NFS disk service and mail services on a machine that also hosts multi-user logins. There is less chance of a malicious user gaining access to critical services if users are barred from logging into that server. *(See Action Item #6)*

The College of Engineering Servers

COE1	**COE2**	**COE3**	**EDS1**
SGI Crimson	*Sun SparcServer 1000*	*Sun Ultra 2*	*SGI Challenge S*
IRIX 5.3	Solaris 2.4	Solaris 2.5.1	IRIX 5.3
• Multi-User login • License Server • Mail Services: ○ IMAP ○ POP ○ SMTP	• Multi-User Login	• Multi-User Login • License Server	• Dedicated Server *(No General User Login)*
• NFS Services: ○ scratch disks ○ /usr/local: SGIs ○ /usr/engr: SGIs ○ /var/mail	• NFS Service: ○ scratch disks ○ /usr/local to Suns ○ /usr/engr to Suns	• NFS Service: ○ scratch disks ○ /usr/local: Suns ○ /engr: Suns	• NFS Service: ○ home directories ○ scratch disks
• Tape Backups • Print Server • YP Master	• Tape Backups • YP Slave Server	• YP Slave Server	• Tape Backups
• Mounts: ○ eds1: home dirs ○ coe1: /itl	• Mounts: ○ eds1: home dirs ○ coe1: /var/mail	• Mounts: ○ eds1: home dirs ○ eds1: scratch ○ coe1: scratch ○ coe1: /var/mail ○ coe2: scratch ○ coe2: /usr/engr	• Mounts: ○ coe1: /usr/local

The most egregious flaw in the current COE server configurations is the cyclic dependencies in services and boot order. Currently no machine can fully boot without the active operation of the others. *(See the following diagram and Action Item #5)*

Boot-time Dependency Loops



Operating system vulnerabilities

In this section, we consider all the holes and problems that our vendor OS's are known to have. OS vulnerabilities are critical to correct because they can potentially allow any attacker to exploit well-known holes such as buffer overflows and race conditions – leading directly to root access. Once root is gained on a machine, the entire network can be considered compromised

There are a veritable plethora of Operating System security vulnerabilities on each machine in the COE server farm. Since the machines are running at old revisions and largely un-patched, such weaknesses are to be expected. *(See Action Item #4)*

Once the patches listed below are applied to a machine, it is theoretically "safe" from vendor OS-related exploits. The following three tables show all currently available vendor OS and security patches:

IRIX 5.3: Current SGI advisory / patch list *(SGI Crimson and Challenge S)*

SGI Advisory #	Subject/ Issue	SGI Patch #	Other Org #
19950201	sendmail	332>407>526	CERT 95:05
19951001	sendmail/syslog	825	CERT CA-95:13
19951101	telnetd	1020	CERT CA-95:14
19960101	object server	1096	
19960102	oampkg	na	
19960203	sendmail	1146	CERT CA-96.04
19960501	gui perms tool	1324	
19960801	gui tools	1518	
19960802	expreserve	na	CERT CA-96.19
19960901	SYN DoS	na	CERT CA-96.21
19961001	desktop sysmon	1110	
19961101	systour/OutOfBox	na	
19961102	license manager	patchLic5.3	
19961103	sendmail	na	CERT CA-96.24
19961201	searchbook	1596	
19961202	SYN/Ping DoS	1529	CERT CA-96.21&26, SGI19961202
19961203	netprint	1685	
19970101	csetup	1751	CERT CA-97.03
19970102	xfs	1409	
19970301	fsdump	na	
19970401	gmemusage	na	
19970501	webdist,handler	2315	CERT CA-97.12,AUSCERT AA-97.14
19970502	xlock	2090	CERT CA-97.13,AUSCERT AA-97.24
19970504	rld	2064	
19970505	df	2224	AUSCERT AA-97.19,CERT CA-97.21
19970506	pset	2176	AUSCERT AA-97.20, CERT CA-97.21
19970507	eject	2228	AUSCERT AA-97.21,CERT CA-97.21
19970508	login LOCKOUT	2216	AUSCERT AA-97.12, CERT CA-97.15
19970508	login/scheme	2216	AUSCERT AA-97.22, CERT CA-97.21
19970509	ordist	2212	AUSCERT AA-97.23, CERT CA-97.21
19970701	talkd	2132	CERT CA-7.04, AUSCERT AA-97.01
19970801	ftpd	2292	AUSCERT AA-97.03, CERT CA-97.16
19970901	nls	2286 or 2183	CERT CA-97.10
19971101	libXt	2155	CERT CA-97.11
19971102	at	2225	CERT CA-97.18
19971103	syserr/perms	2238 & 2273	
19971201	statd	1391	AUSCERT AA-97.29, CERT CA-97.26
19980301	dmedia_eoe	2563	AUSCERT AA-96.11,AA-96.20,AA-97.05
19980402	lp	2166	AUSCERT AA-96.12
19980404	suidperl/sperl	not avail	CERT CA-97.17, AUSCERT AA-97.13
19980405	suid_exec	not avail	AUSCERT AA-96.17
19980406	LicenseManager	1678	
19980601	OSF/DCE & DFS	not avail	CERT VB-97.12
19980602	mediad	3191 & 3189	
19980603	BIND DNS named	3268	CERT CA-98.05
19980604	mail/sendmail	3347	CERT CA-96.20
19980605	Mail/mailx	3347	
19980801	qpopper	not avail	CERT CA-98.08
19980802	imapd	not avail	CERT CA-98.09
19981002	xterm	3142	CERT VB-98.04
19981003	Xaw X library	3162	CERT VB-98.04
19981004	routed	2770	
19981101	rpc.ttdbserverd	3510	NAI-29, CERT CA-98.11
19990301	X fonts	3236 or 3237	
20000301	fam		NAI-0016

Solaris 2.4: Current Sun patch list *(Sun SparcServer 1000)*

```
Sun          OS/        Subject/
Patch #      Subsystem  Issue
________________________________________________________________________________
 103670-07   CDE 1.0.2: dtcm sdtcm_convert rpc.cmsd patch
 103671-08   CDE 1.0.1: dtcm sdtcm_convert rpc.cmsd patch
 102479-13   SunOS 5.4: libresolv, in.named, named-xfer, nslookup & nste
 101902-09   SunOS 5.4: add_drv, drvconfig, pcfs, fdformat & fd fixes
 101907-16   SunOS 5.4: usr/sbin/vold patch
 101945-63   SunOS 5.4: Kernel update
 101959-21   SunOS 5.4: lp patch
 101973-37   SunOS 5.4: libnsl, nistbladm & ypbind fixes
 101977-06   SunOS 5.4: lockd patch
 102042-05   SunOS 5.4: usr/bin/mail jumbo patch
 102044-01   SunOS 5.4: bug in mouse code makes "break root" attack poss
 102049-05   SunOS 5.4: linker fixes
 102066-22   SunOS 5.4: /usr/lib/sendmail patch
 102070-06   SunOS 5.4: usr/sbin/rpcbind patch
 102165-04   SunOS 5.4: nss_dns.so.1 fixes
 102218-04   SunOS 5.4: libbsm fixes
 102277-03   SunOS 5.4: nss_nisplus.so.1 fixes
 102656-01   SunOS 5.4: /dev/qec should protect against being opened dir
 102664-01   SunOS 5.4: data fault in scanc() due to bad "cp" argument
 102685-02   SunOS 5.4: /usr/lib/nfs/mountd patch
 102693-12   SunOS 5.4: /usr/bin/at and /usr/sbin/cron patch
 102704-02   SunOS 5.4: jumbo patch for NIS commands
 102711-02   SunOS 5.4: usr/bin/ps and usr/ucb/ps patch
 102741-01   SunOS 5.4: libm can hit SEGV in multi-threaded mode
 102756-01   SunOS 5.4: expreserve still has security problem
 102769-07   SunOS 5.4: statd fixes
 102773-02   SunOS 5.4: in.tftpd patch
 102788-05   SunOS 5.4: Patch for sccs
 102922-05   SunOS 5.4: inetd fixes
 102960-01   SunOS 5.4: vipw has security problem
 103070-02   SunOS 5.4: patch usr/bin/tip
 103263-03   SunOS 5.4: ufsdump, ufsrestore and wall patch
 103270-01   SunOS 5.4: nissetup default permissions not secure enough
 103706-02   SunOS 5.4: rpc.nisd_resolv rebuild for BIND 4.9.3
 103813-03   SunOS 5.4: /usr/bin/rdist patch
 104617-01   SunOS 5.4: /usr/lib/newsyslog patch
 104701-01   SunOS 5.4: in.talkd security problem fix
 104798-02   SunOS 5.4: eeprom patch
 104973-01   SunOS 5.4: chkey and newkey patch
 105099-01   SunOS 5.4: usr/sbin/sysdef patch
 105254-01   SunOS 5.4: usr/bin/rlogin patch
 106042-01   SunOS 5.4: in.rexecd does not prevent access to expired acc
 106451-01   SunOS 5.4: /usr/sbin/ping fix
 101878-18   OpenWindows 3.4: Xview Patch
 101879-02   OpenWindows 3.4: XView Binary Compatibility Patch
 102030-12   OpenWindows 3.4: Calendar Manager patch
 102057-42   OpenWindows 3.4: Server (Xsun) Patch
 102292-04   OpenWindows 3.4: filemgr (ff.core) fixes
 102386-09   OpenWindows 3.4: OLIT Patch
 105075-01   OpenWindows 3.4: libXt patch
 105244-01   OpenWindows 3.4: libXt Binary Compatibility Patch
 102226-31   Motif 1.2.3: libXm RunTime Kit Patch
 103290-08   SPARCstorage Array 2.0: SSA Jumbo patch for Solaris 2.4 11/
 105678-02   SunOS 5.4: /usr/sbin/auditreduce patch
 106704-01   SunOS 5.4: /usr/sbin/in.uucpd patch
 106912-01   SunOS 5.4: /usr/bin/apropos patch
 106990-01   SunOS 5.4: uux has buffer overflow problems
 106671-02   OpenWindows 3.4: libce suid/sgid security fix
 106672-02   OpenWindows 3.4: libdeskset patch
 106646-03   SNC 3.2: rpc.pcnfsd has security problem, also hangs and du
 101880-16   OpenWindows 3.4: Mailtool Patch
 108490-01   SunOS 5.4: Snoop may be exploited to gain root access
 102734-05   OpenWindows 3.4: ToolTalk 1.1.2: fix core dumps, leaks, ODS
 108636-01   CDE 1.0.1/1.0.2: ToolTalk patch
 108495-01   SunOS 5.4: ASET sets the gid bit on /tmp,/var/tmp during me
 104950-02   SunOS 5.4: usr/bin/uustat patch
 108769-02   SunOS 5.4: telnet environment has extra NULL field between
 109446-01   SunOS 5.4: patch /usr/vmsys/bin/chkperm
```

Solaris 2.5.1: Current Sun patch list *(Sun Ultra 2)*

```
    Sun         OS/ Subject/
    Patch #     Subsystem  Issue
    ______________________________________________________________________________

104578-03  SunOS 5.5.1: pkginstall patch
103670-07  CDE 1.0.2: dtcm sdtcm_convert rpc.cmsd patch
103630-15  SunOS 5.5.1: ip ifconfig arp udp icmp patch
103663-15  SunOS 5.5.1: libresolv, in.named, named-xfer, nslookup & ns
103558-15  SunOS 5.5.1: admintool/launcher fixes + swmtool fixes & y20
103582-24  SunOS 5.5.1: /kernel/drv/tcp and /usr/bin/netstat patch
103594-19  SunOS 5.5.1: sendmail fixes
103597-04  SunOS 5.5.1: /kernel/strmod/sockmod patch
103603-12  SunOS 5.5.1: ftp, in.ftpd, in.rexecd and in.rshd patch
103622-15  SunOS 5.5.1: /kernel/drv/sd driver patch
103640-33  SunOS 5.5.1: kernel, nisopaccess, & libthread patch
103627-13  SunOS 5.5.1: Linker patch
103680-03  SunOS 5.5.1: nscd/nscd_nischeck/nss_files.so.1 patch
103686-02  SunOS 5.5.1: rpc.nisd_resolv patch
103690-13  SunOS 5.5.1: cron/crontab/at/atq/atrm patch
103696-05  SunOS 5.5.1: /sbin/su, /usr/bin/su and /sbin/sulogin patch
103699-02  SunOS 5.5.1: /usr/sbin/ping patch
103743-01  SunOS 5.5.1: XFN source modifications for BIND 4.9.3
103801-07  SunOS 5.5.1: Patch for make, sccs, as
103817-04  SunOS 5.5.1: /usr/bin/rdist patch
103866-05  SunOS 5.5.1: BCP (binary compatibility) patch
103934-17  SunOS 5.5.1: /kernel/drv/isp patch
103959-12  SunOS 5.5.1: lp patch
104010-01  SunOS 5.5.1: VolMgt Patch
104212-13  SunOS 5.5.1: /kernel/drv/hme patch
104220-03  SunOS 5.5.1: /usr/lib/nfs/mountd patch
104246-08  SunOS 5.5.1: /kernel/drv/fas patch
104266-02  SunOS 5.5.1: inetd patch
104283-04  SunOS 5.5.1: /kernel/fs/procfs patch
104331-07  SunOS 5.5.1: /usr/sbin/rpcbind patch
104490-06  SunOS 5.5.1: ufsdump and ufsrestore patch
104334-01  SunOS 5.5.1: lockd patch
104516-03  SunOS 5.5.1: aspppd patch
104560-05  SunOS 5.5.1: /kernel/fs/hsfs patch
104605-09  SunOS 5.5.1: ecpp driver patch
104613-01  SunOS 5.5.1: /usr/lib/newsyslog patch
104650-03  SunOS 5.5.1: /usr/bin/rlogin patch
104654-05  SunOS 5.5.1: automount/automountd patch
104166-04  SunOS 5.5.1: /usr/lib/nfs/statd patch
104692-01  SunOS 5.5.1: usr/sbin/in.talkd patch
104708-19  SunOS 5.5.1: ssd, pln, soc, ssaadm and ssafirmware patch
104735-02  SunOS 5.5.1: platform/sun4m/kernel/drv/sx patch
104736-04  SunOS 5.5.1: /usr/bin/csh patch
104776-02  SunOS 5.5.1: libvolmgt patch
104795-02  SunOS 5.5.1: eeprom patch
104841-05  SunOS 5.5.1: /usr/sbin/vold patch
104893-02  SunOS 5.5.1: /kernel/sys/c2audit patch
104935-01  SunOS 5.5.1: usr/sbin/in.rlogind patch
103738-14  SunOS 5.5.1: /usr/sbin/syslogd patch
104956-04  SunOS 5.5.1: usr/sbin/in.rarpd patch
104958-01  SunOS 5.5.1: usr/sbin/in.rdisc patch
104960-02  SunOS 5.5.1: usr/sbin/snoop patch
104968-02  SunOS 5.5.1: chkey and newkey patch
105004-11  SunOS 5.5.1: pci_pci, ebus, pci and rootnex driver patch
105050-01  SunOS 5.5.1: usr/bin/ps and usr/ucb/ps patch
105092-01  SunOS 5.5.1: usr/sbin/sysdef patch
105299-02  SunOS 5.5.1: kernel/misc/nfssrv patch
105784-05  SunOS 5.5.1: libbsm patch
106382-01  SunOS 5.5.1: /usr/sbin/rmmount patch
105310-13  SunOS 5.5.1: Patch for socal, sf driver, and luxadm
105324-04  SunOS 5.5.1: ses driver patch
105344-01  SunOS 5.5.1: usr/bin/gcore patch
105352-01  SunOS 5.5.1: kernel/exec/elfexec patch
103981-18  SunOS 5.5.1: glm driver patch
104595-09  SunOS 5.5.1: prtdiag patch
106563-04  SunOS 5.5.1: PAM Patch
104628-05  SunOS 5.5.1: driver_aliases, driver_classes and name_to_maj
105789-08  VIS/XIL 2.5.1: Graphics Patch
105790-23  Creator 2.5.1: FFB Graphics Patch
103879-05  OpenWindows 3.5.1: KCMS tools have security vulnerability
103566-53  OpenWindows 3.5.1: Xsun patch
103900-01  OpenWindows 3.5.1: XView Binary Compatibility Patch
103901-13  OpenWindows 3.5.1: Xview Patch
104338-03  OpenWindows 3.5.1: libXt patch
104533-05  OpenWindows 3.5.1: OLIT Patch
104976-06  OpenWindows 3.5.1: Calendar Manager patch
105251-01  OpenWindows 3.5.1: libXt Binary Compatibility Patch
106224-01  OpenWindows 3.5.1: filemgr (ff.core) fixes
106663-01  OpenWindows 3.5.1: libdeskset patch
106662-01  OpenWindows 3.5.1: libce suid/sgid security fix
103461-34  Motif 1.2.3: Runtime library patch
107756-01  SunOS 5.5.1: /usr/bin/pax patch
104873-05  SunOS 5.5.1: /usr/bin/uustat and other uucp fixes
105077-06  SunOS 5.5.1: /kernel/fs/fifofs patch
106689-01  SunOS 5.5.1: /usr/sbin/in.uucpd patch
106905-01  SunOS 5.5.1: apropos/catman/man/whatis patch
104093-08  OpenWindows 3.5.1: mailtool patch
106411-06  OpenWindows 3.5.1: xdm patch
106646-03  SNC 3.2: rpc.pcnfsd has security problem, also hangs and du
108658-02  SunOS 5.5.1: Patch for sadmind
104489-11  OpenWindows 3.5.1: ToolTalk patch
106529-07  SunOS 5.5.1: Shared library patch for C++
108497-01  SunOS 5.5.1: ASET sets gid on /tmp,/var/tmp when med/high s
108470-01  SunOS 5.5.1: Possible denial of service bug
109275-01  SunOS 5.5.1: security: /bin/mail has buffer overflow
109392-01  SunOS 5.5.1: /usr/vmsys/bin/chkperm patch
108802-01  SunOS 5.5.1: tip has buffer overrun with security implicati
109774-01  SunOS 5.5.1: Require correction to timezone data for Austra
```

Configuration Vulnerabilities

Here we consider the various threats that derive not from the OS itself, but from the configuration of various programs and services that are run on the machine. We first examine the consensus list initiated by the SANS Institute - one of the first documents of its kind, identifying the most common configuration mistakes and mishaps. Such a list is a valuable tool for organizing threat vectors and prioritizing their remedy. With this tool, then, we identify which COE servers may be vulnerable and what to do about it. Then we turn to other, less well-known problems that must still be corrected.

I. The Ten Most Critical Internet Security Threats – SANS Consensus List

> *"The majority of successful attacks on computer systems via the Internet can be traced to exploitation of one of a small number of security flaws. … A few software vulnerabilities account for the majority of successful attacks because attackers are opportunistic – taking the easiest and most convenient route. They exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, by scanning the Internet for vulnerable systems."*
>
> *- See http://www.sans.org/topten.htm*

1. BIND weaknesses *(See Action Item #8)*
   - COE1 is currently running an old version of BIND; this service should be turned off.
   - EDS1 is currently running an old version of BIND; this service should be turned off.

2. Vulnerable CGI programs *(See Action Item #14)*
   - COE1 is currently running a web server; this service should be migrated to a dedicated server, CGI's should be audited and denied to users.

3. Remote Procedure Call (RPC) weaknesses *(See Action Item #9)*
   - COE1 is currently serving NFS; this service should be consolidated to a dedicated server, other rpc services turned off.
   - COE2 is currently serving NFS; patches should be applied, other rpc services turned off.
   - COE3 is currently serving NFS; this service should be consolidated to a dedicated server, other rpc services turned off.
   - EDS1 is currently serving NFS; patches should be applied, other rpc services not needed for NFS and NIS turned off.

4. RDS security hole in the Microsoft Internet Information Server (IIS)
   - *None of the machines is running MS IIS*

5. Sendmail buffer overflow weaknesses *(See Action Item #8)*
   - COE1 is currently the department mailhost; this service should be migrated to a dedicated server, configurations updated for a client.
   - COE2 is currently mis-configured and running sendmail; this service should be turned off, configurations updated for a client.
   - EDS1 should be modified to be the department mailhost; upgraded to the most recent sendmail version, configurations updated for a server.

6. Sadmind and mountd *(See Action Item #14)*
   - COE1 is currently running mountd; newest version & patches should be applied.
   - COE2 is currently running sadmind and mountd. Sadmind should be turned off. For mountd: newest version & patches should be applied.
   - COE3 is currently running sadmind and mountd. Sadmind should be turned off. For mountd: newest version & patches should be applied.
   - EDS1 is currently running mountd. Newest version & patches should be applied.

7. Global file sharing and inappropriate information sharing … *(See Action Item #14)*
   - COE1 is currently serving NFS; this service should be consolidated to a dedicated server.
   - COE2 is currently serving NFS; exports should be updated to export by IP, not be global.
   - COE3 is currently serving NFS; this service should be consolidated to a dedicated server.
   - EDS1 is currently serving NFS; exports should be updated to export by IP, not be global.

8. User IDs, especially root/administrator with no passwords or weak passwords. *(See Action Item #15)*
   - All blank password fields have been changed to "*LK*" and null passwords have been forbidden in /etc/default/login. Password validators (like passwd+) should be run at password change-time. Password cracking should be run by administrators (with approval!) to look for weak passwords.

9. IMAP and POP buffer overflow vulnerabilities or incorrect configuration. *(See Action Item #8)*
   - COE1 is currently running IMAP and POP; these services should be migrated to the dedicated mail server, upgraded to the latest stable versions, and re-configured.

10. Default SNMP community strings set to 'public' and 'private.'
    - *SNMP is not running on any server.*

II. Other Configuration Vulnerabilities

Running non-dedicated servers means that there are more potential holes to be exploited, more services that can be compromised if even one on the machine develops a problem. Also a single point of failure is created for a broad spectrum of services, making them more susceptible to a Denial of Service attack. *(See Action Item #6)*

Risks From Installed Third-Party Software

Misconfigurations, or worse, substitution of a Trojan program, can seriously compromise the security of the following programs and the system they reside on. COE heavily uses all of these programs, and should continue to derive great benefit from their proper use *(See Action Item #10)*:

- tcp_wrappers
- sudo
- wu_ftpd
- sendmail

Vendor simulation software needed by research faculty is typically proprietary, and thus subject to unexaminable and potential harmful bugs. *(See Action Item #4)*

Administrative practices

The following is a list of the undesirable system administrative practices that we have catalogued as part of the servers' history. With some attention, these can be wholly corrected:

- General neglect *(See Action Item #10)*
- Machines with local accounts that don't necessarily match main server username/uids *(See Action Item #13)*
- No centralization of configurations *(See Action Item #11)*
- No documentation *(See Action Item #12)*
- Local, undocumented, non-backed-up file storage *(See Action Item #7)*
- Poor password hygiene *(See Action Item #15)*
- Use of /.rhosts *(See Action Item #14)*
- Excess services (finger, chargen, echo, daytime, etc) running on main servers through inetd *(See Action Item #14)*

Backup Policies, Disaster Preparedness, etc

Backups are a critical aspect of security at any site. Good backups allow for data recovery in the event of a disaster, accidental deletion, or malicious corruption. Unverified backups are, of course, still unknown quantities – we can't know that the file image on tape is a good one until we examine it.

The College of Engineering currently has three 8mm tape devices in use. Backups are managed by the Amanda software developed at UMD College Park. Each drive has its own rotating set of 28 tapes, meaning that every month the tapes are overwritten (in sequence). There are no archivals of any type.

Unfortunately, there is no fail-over capacity in the current configuration: each tape drive is a different brand or revision and the versions of Amanda are disparate (though not wholly incompatible). If one drive should fail, it will at the least be difficult to get a clean data restore. *(See Action Item #7)*

With regard to general disasters, the College has no stockpile of hardware and no service contracts. Since the vast majority of COE's machines are out of warranty, this means that there is little hope of quick turnaround time in the event of catastrophic failure. *(See Action Item #7)*

Other Issues / Vulnerabilities

Physical Security - The servers sit in a good physical location: a locked room with a human monitor on duty for 2/3 of the day. When the monitor is not physically present, the doors to the room are locked and alarmed. The room is well situated with regard to HVAC concerns: there are redundant chillers, multiple power conditioners, and UPS power. Our only recommendation is to increase the capacity and duration of the UPS's available. *(See Action Item #7)*

Network Security – COE is currently part of a switched network. This prevents casual wire-sniffing and related password "loss"

Action Items: *A Prioritized List of Major Areas of Concern & Recommended Solutions*

1. ***Root passwords***

Discussion: The College of Engineering systems have lain fallow for nearly a year – there has been no systems administrator assigned to the department. The previous admins did not change the root passwords upon their departure, so not only is root unchanged for far too long, but ex-employees of the department also know it.

Solution:

- Change the root passwords immediately, distribute on a need-to-know basis
- Use sudo and restrict access to what is most strictly needed by non-admins (if root access must be shared at all)

2. Increasingly undependable hardware

Discussion: There is a great deal of legacy hardware employed in the COE server cluster. As a result, most of the servers have inadequate, undependable components. During the evaluation phase alone, there were numerous server crashes due to SCSI bus errors, backup failures due to bad drives and media. From a security standpoint, this is clearly unacceptable: part of security is assuring access to the systems.

Solution: Replace what is deteriorating:
Approximately 24 Gb of disk space
SCSI cabling of various connector types
Augment core server hardware:
New multi-user login machine
New tape drive *(see below)*

3. Out of date Operating Systems

Discussion: It is imperative that all server Operating Systems be upgraded to current revisions. Since none of the UNIX versions under discussion here are free, there will likely be some kind of cost associated with this upgrade.

Solution: Contact individual vendors to inquire about upgrade paths and pricing.

4. Out of date patches

Discussion: It is imperative that all Recommended and Security patch sets from respective vendors.

Solution: Download free Recommended and Security patch sets from the web (this covers IRIX and Solaris).
Contact third-party software vendors to verify product functionality at new OS/patch levels, acquire any necessary patches for product.

5. Cyclic dependencies in server configurations

Discussion: This mis-configuration creates an enormous race condition whenever any one of the servers needs to be rebooted, all the others either crash, busy-wait, or likewise need to be rebooted. It is critical to correct this problem.

Solution: Revamp services configuration so that there are no dependency loops.

6. *Poorly distributed services: multiple offerings from one under-powered server*

Discussion: This problem is related to the cyclic dependencies discussed above. Services appeared to have been initially distributed to whatever machine had the lowest "load" at the time when the service needed to be installed. This applies equally to internal services (such as NFS service) as well as externally available services (such as web, ftp, etc). A service living on a on-dedicated servers can also fall victim to an exploit on a completely unrelated service.

Solution: Upgrade, securely configure, and relocate services onto dedicated machines.

7. Inadequate backup and recovery capabilities

Discussion: The College currently has a backup scheme in place: three tape drives running week-night dumps under *Amanda*. Along with the proposed disk and service redistribution, we would also recommend consolidating all tape backups to a dedicated, hardened machine. The failing tape drives should also be replaced with newer, warranted technology. Currently, recovery capabilities are limited by the undependability of the tape backup media; tapes have "gone bad" or simply never taken a clean backup. This could also be addressed through some strategic purchases.

Solution: Purchase either an AIT or DLT tape drive (and media).
Validate backup integrity on a regular basis.
Purchase additional UPS capacity

8. *Known vulnerabilities from out of date software (Services, Applications)*

Solution: Upgrade and securely configure affected software.

9. Use of insecure network protocols

Solution: Migrate to ssh and other encrypted, authenticated protocols.

10. Un-updated service configurations

Discussion: According to the previous administrators of the site who we were able to contact, many software and service configurations had been left unexamined for over a year. For much of this time, COE had been without a UNIX systems administrator, so while the lapse is unfortunate, it is not unexpected.

Solutions: Update free software that has fallen behind revision
Remove network-based root access
Configure tcp_wrappers
Remove extraneous network services

11. Inconsistent system configurations

Discussion: Inconsistency creates a difficult task for the security-aware admin: trying to keep analogous configurations in synch while adapting to the quirks of an additional OS. As the number of systems grows, it becomes increasingly difficult to keep track of the state of each without some sort of helping tool.

Solution: Migrate to a centralize configuration management scheme (using cfengine/CVS/RCS).

12. *Lack of documentation*

Discussion: Even during the evaluation period, we encountered numerous undocumented configuration interdependencies. One of the worst stumbling blocks to hit during an upgrade is the brutal destruction of a beautiful system by an ugly hidden dependency.

Solution: Create on-going documentation for the College’s security policy, software and server configurations

13. Lack of account management

Discussion: Although COE has experienced the typical turnover associated with a university environment (students graduating, etc), there has been no routine purging of unused user accounts. Stagnant accounts are one major target for intruders; intruders know that the legitimate owner is unlikely to notice and report the illegitimate activity and that to system administrators the activity will appear to be within normal tolerances

Solution: We recommend that all unrecognized, unused accounts be purged. Users with multiple accounts on the system should be consolidated into one (for accountability). Enforce use of a consistent username, uid, and password (possibly through kerberization).

14. ***Unexpected / unauthorized services being offered***

Discussion: When machines are offering “bizarre” services that were neither approved nor intentionally run by the admins, there are a number of possibilities for what is occurring:

1. The services are turned on by default and were never shut off.
2. A non-malicious user has set up the service
3. A malicious user has set up the service.

In all cases, the admins should investigate, and either run the service officially or shut it down.

Solution: We recommend a course of routine site audits to identify such services

15 Periodic system auditing

Discussion: Since security is, by its very nature, an ongoing process, we must pay attention to it! The purpose here is to assess the continued integrity of the system

Solutions:

- Scan (using `find)` for `setuid, setgid`, and world-writable files
- Use COPS for internal auditing
- Perform SATAN, Nessus and nmap scans and compare to archived results
- Run Crack to assess user password integrity

Further References

A small compendium of references is provided here, should the reader desire to research the vulnerabilities enumerated above.

AntiOnline: General Computer Security, Hackers, & Hacking
http://www.antionline.com

Red Hat Linux: patches and information
http://www.redhat.com/support/errata

SANS Institute
Home Page: http://www.sans.org
GIAC: http://www.sans.org/giac.htm
Top Ten Threats: http://www.sans.org/topten.htm

SGI site: patches and information
http://www.sgi.com/support/patch_intro.html

Sun site: patches and information
http://sunsolve.sun.com/pubpatch

X-Force: broad spectrum threats & vulnerability information
http://xforce.iss.net