UNI SOLUTIONS ®
UNISOLUTIONS ASSOCIATES

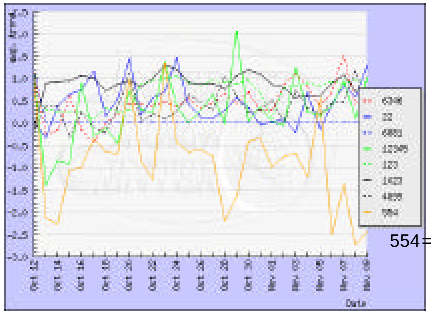
Extracting Security Value from Chargeback Data

Haral Tsitsivas
UniSolutions Associates
http://www.unisol.com
haral@unisol.com

Increasing Costs of Security Threats and Vulnerabilities

- Vendor vulnerabilities are on the rise
- Exploits of vendor vulnerabilities are released in an ever increasing rate
- Computer users are faced with a multitude of threats
- Consumers are at increased risk of identify theft and financial loss (ChoicePoint)

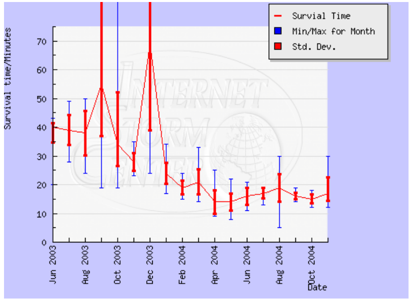
Historical Trend of Ports Scanned



554=rtsp

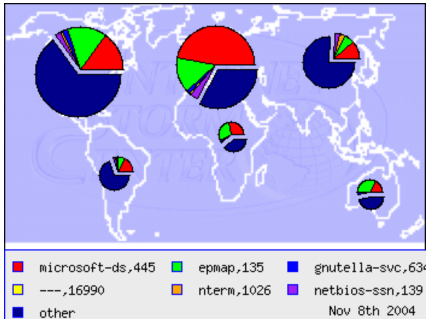
Source: SANS – http://www.sans.org

Unprotected Host Survival Time Graph



Source: SANS – http://www.sans.org

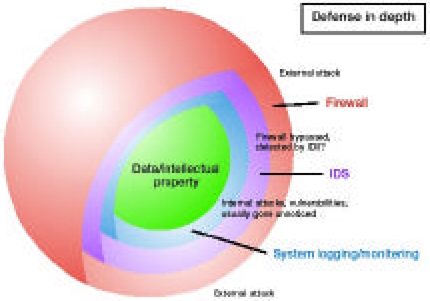
Threat World Map



Source: SANS – http://www.sans.org

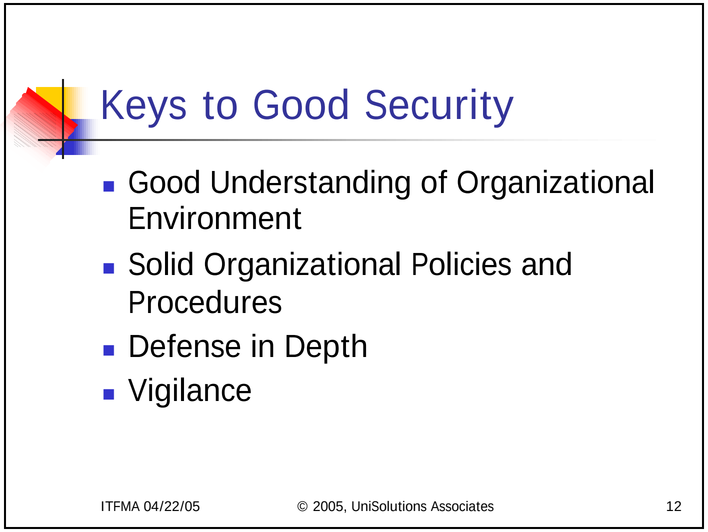
When Can Things Go Wrong? Anytime! Even in Public...

Defense In Depth


Defense in depth
External attack
Firewall
Firewall bypassed, detected by IDS?
Data/intellectual property
IDS
Internal attacks, vulnerabilities, usually goes unnoticed
System logging/monitoring
External attack

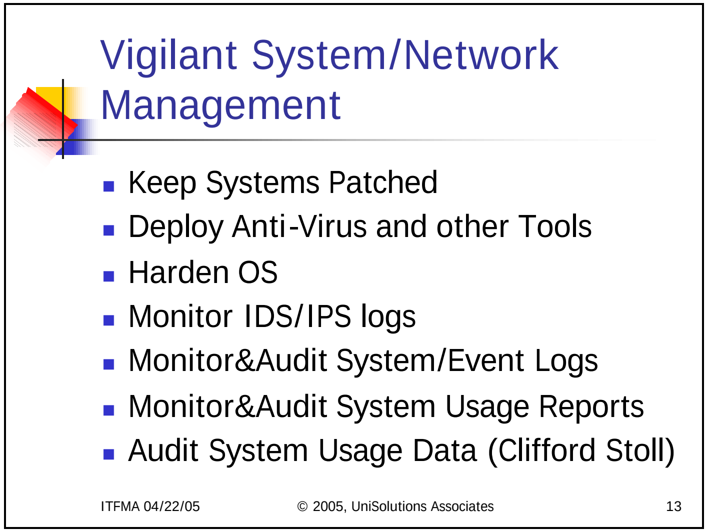
DID - Technologies and Vulnerabilities Addressed

IDS/IPS	Detect/prevent attacks on vulnerabilities
Firewalls	Block networks from attacks
Security Policy	Sets guidelines to prevent security breach
Patch Mgmt	Fixes vulnerabilities
Anti-Virus	Detects known attacks to known vulnerabilities
Event/Log Analysis	Monitors system/network state for attacks



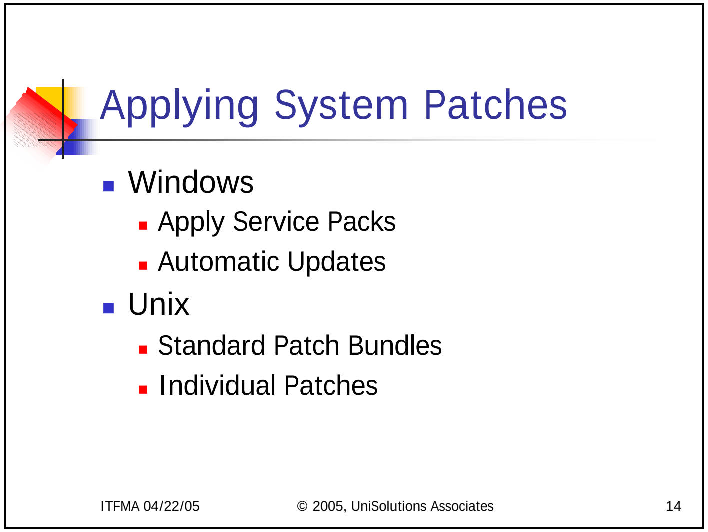
Keys to Good Security

- Good Understanding of Organizational Environment
- Solid Organizational Policies and Procedures
- Defense in Depth
- Vigilance



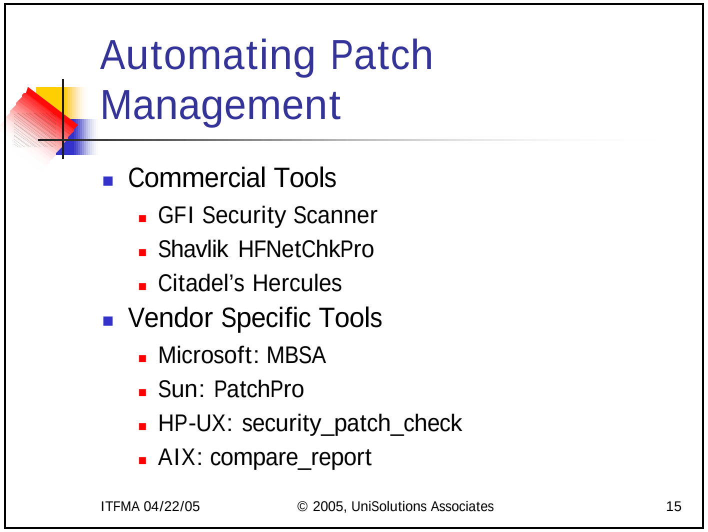
Vigilant System/Network Management

- Keep Systems Patched
- Deploy Anti-Virus and other Tools
- Harden OS
- Monitor IDS/IPS logs
- Monitor&Audit System/Event Logs
- Monitor&Audit System Usage Reports
- Audit System Usage Data (Clifford Stoll)



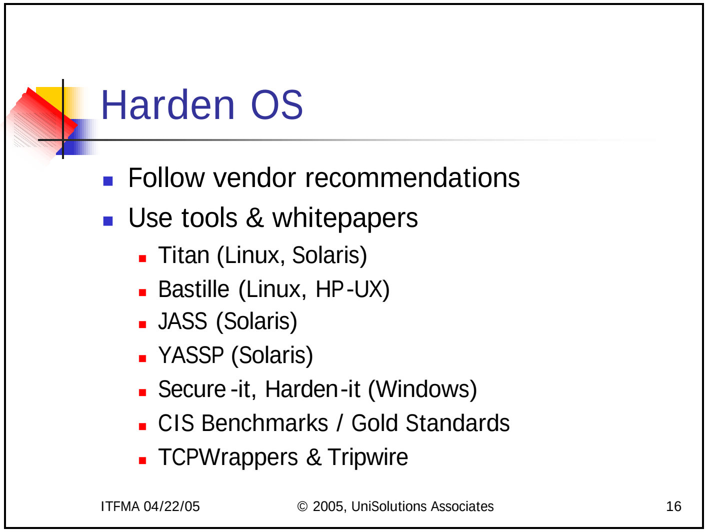
Applying System Patches

- Windows
  - Apply Service Packs
  - Automatic Updates
- Unix
  - Standard Patch Bundles
  - Individual Patches



Automating Patch Management

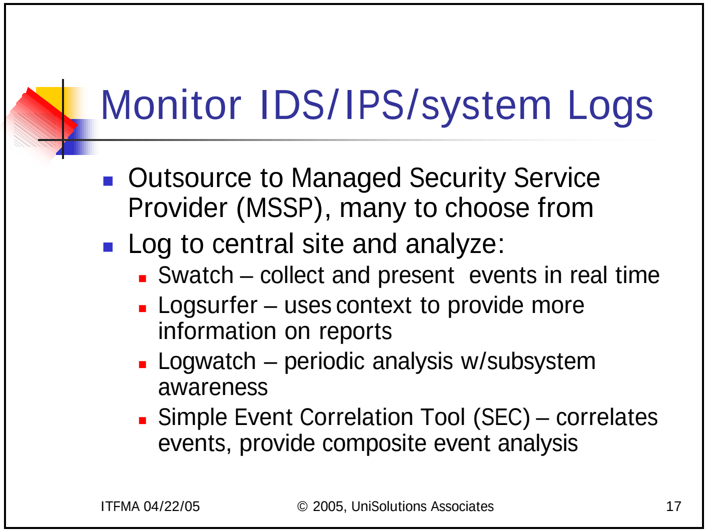
- Commercial Tools
  - GFI Security Scanner
  - Shavlik HFNetChkPro
  - Citadel's Hercules
- Vendor Specific Tools
  - Microsoft: MBSA
  - Sun: PatchPro
  - HP-UX: security_patch_check
  - AIX: compare_report



Harden OS

- Follow vendor recommendations
- Use tools & whitepapers
  - Titan (Linux, Solaris)
  - Bastille (Linux, HP-UX)
  - JASS (Solaris)
  - YASSP (Solaris)
  - Secure-it, Harden-it (Windows)
  - CIS Benchmarks / Gold Standards
  - TCPWrappers & Tripwire

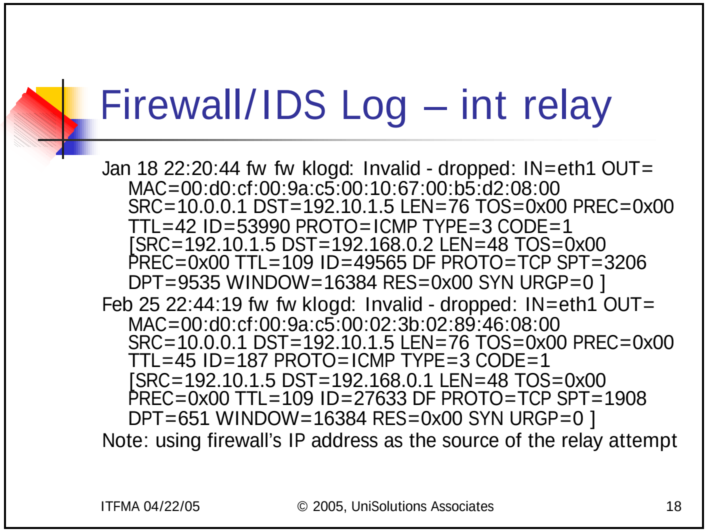
ITFMA 04/22/05 © 2005, UniSolutions Associates 16



Monitor IDS/IPS/system Logs

- Outsource to Managed Security Service Provider (MSSP), many to choose from
- Log to central site and analyze:
  - Swatch – collect and present events in real time
  - Logsurfer – uses context to provide more information on reports
  - Logwatch – periodic analysis w/subsystem awareness
  - Simple Event Correlation Tool (SEC) – correlates events, provide composite event analysis

ITFMA 04/22/05 © 2005, UniSolutions Associates 17

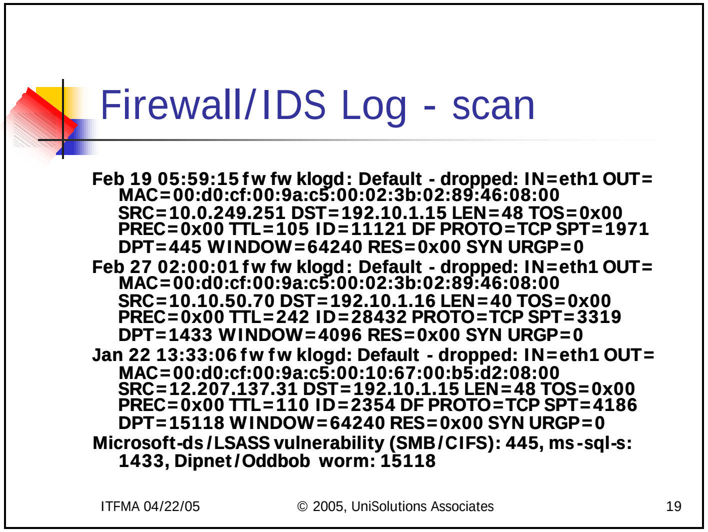


Firewall/IDS Log – int relay

```
Jan 18 22:20:44 fw fw klogd: Invalid - dropped: IN=eth1 OUT=
    MAC=00:d0:cf:00:9a:c5:00:10:67:00:b5:d2:08:00
    SRC=10.0.0.1 DST=192.10.1.5 LEN=76 TOS=0x00 PREC=0x00
    TTL=42 ID=53990 PROTO=ICMP TYPE=3 CODE=1
    [SRC=192.10.1.5 DST=192.168.0.2 LEN=48 TOS=0x00
    PREC=0x00 TTL=109 ID=49565 DF PROTO=TCP SPT=3206
    DPT=9535 WINDOW=16384 RES=0x00 SYN URGP=0 ]
Feb 25 22:44:19 fw fw klogd: Invalid - dropped: IN=eth1 OUT=
    MAC=00:d0:cf:00:9a:c5:00:02:3b:02:89:46:08:00
    SRC=10.0.0.1 DST=192.10.1.5 LEN=76 TOS=0x00 PREC=0x00
    TTL=45 ID=187 PROTO=ICMP TYPE=3 CODE=1
    [SRC=192.10.1.5 DST=192.168.0.1 LEN=48 TOS=0x00
    PREC=0x00 TTL=109 ID=27633 DF PROTO=TCP SPT=1908
    DPT=651 WINDOW=16384 RES=0x00 SYN URGP=0 ]
```

Note: using firewall's IP address as the source of the relay attempt

ITFMA 04/22/05 © 2005, UniSolutions Associates 18



Firewall/IDS Log - scan

```
Feb 19 05:59:15 fw fw klogd: Default - dropped: IN=eth1 OUT=
    MAC=00:d0:cf:00:9a:c5:00:02:3b:02:89:46:08:00
    SRC=10.0.249.251 DST=192.10.1.15 LEN=48 TOS=0x00
    PREC=0x00 TTL=105 ID=11121 DF PROTO=TCP SPT=1971
    DPT=445 WINDOW=64240 RES=0x00 SYN URGP=0
Feb 27 02:00:01 fw fw klogd: Default - dropped: IN=eth1 OUT=
    MAC=00:d0:cf:00:9a:c5:00:02:3b:02:89:46:08:00
    SRC=10.10.50.70 DST=192.10.1.16 LEN=40 TOS=0x00
    PREC=0x00 TTL=242 ID=28432 PROTO=TCP SPT=3319
    DPT=1433 WINDOW=4096 RES=0x00 SYN URGP=0
Jan 22 13:33:06 fw fw klogd: Default - dropped: IN=eth1 OUT=
    MAC=00:d0:cf:00:9a:c5:00:10:67:00:b5:d2:08:00
    SRC=12.207.137.31 DST=192.10.1.15 LEN=48 TOS=0x00
    PREC=0x00 TTL=110 ID=2354 DF PROTO=TCP SPT=4186
    DPT=15118 WINDOW=64240 RES=0x00 SYN URGP=0
```

Microsoft-ds/LSASS vulnerability (SMB/CIFS): 445, ms-sql-s: 1433, Dipnet/Oddbob worm: 15118

ITFMA 04/22/05 © 2005, UniSolutions Associates 19

Firewall/IDS Log - spoof

```
Jan 19 07:58:15 fw fw klogd: Spoof - dropped: IN=eth1 OUT=
    MAC=00:d0:cf:00:9a:c5:00:10:67:00:b5:d2:08:00
    SRC=192.168.9.10 DST=192.10.1.5 LEN=40 TOS=0x00
    PREC=0x00 TTL=230 ID=0 DF PROTO=TCP SPT=14662
    DPT=2740 WINDOW=0 RES=0x00 RST URGP=0
Jan 20 02:39:28 fw fw klogd: Spoof - dropped: IN=eth1 OUT=
    MAC=00:d0:cf:00:9a:c5:00:10:67:00:b5:d2:08:00
    SRC=192.168.9.10 DST=192.10.1.5 LEN=40 TOS=0x00
    PREC=0x00 TTL=230 ID=0 DF PROTO=TCP SPT=4662
    DPT=1230 WINDOW=0 RES=0x00 RST URGP=0
Feb 05 08:44:15 fw fw klogd: Spoof - dropped: IN=eth1 OUT=
    MAC=00:d0:cf:00:9a:c5:00:02:3b:02:89:46:08:00
    SRC=192.168.9.100 DST=192.10.1.5 LEN=121 TOS=0x00
    PREC=0x00 TTL=107 ID=59821 DF PROTO=TCP SPT=4662
    DPT=1235 WINDOW=65444 RES=0x00 ACK PSH URGP=0
Alarm: 2740, p2p/edonkey: 4662, periscope: 1230
```

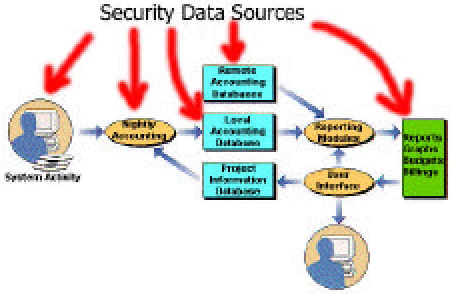
Benefits of Log Review

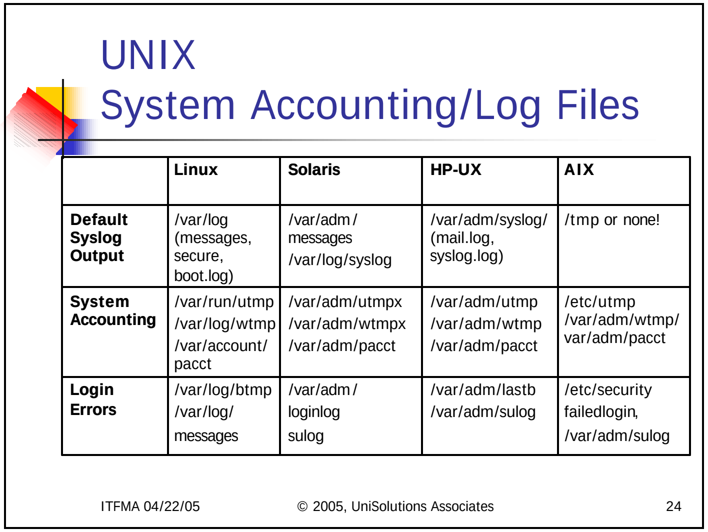
- Confirm Smooth Operation, Proper System/Device Configuration
- Verify SLA
- System/Applications failures are logged and can be fixed!
- Collect evidence in case of security breach that can be used to prosecute!

Benefits of Chargeback

- Capacity Planning
- Project Management
- Benchmarks
- Fiscal and Regulatory Reporting
- Clear Communication in SLAs
- Another source of security data!

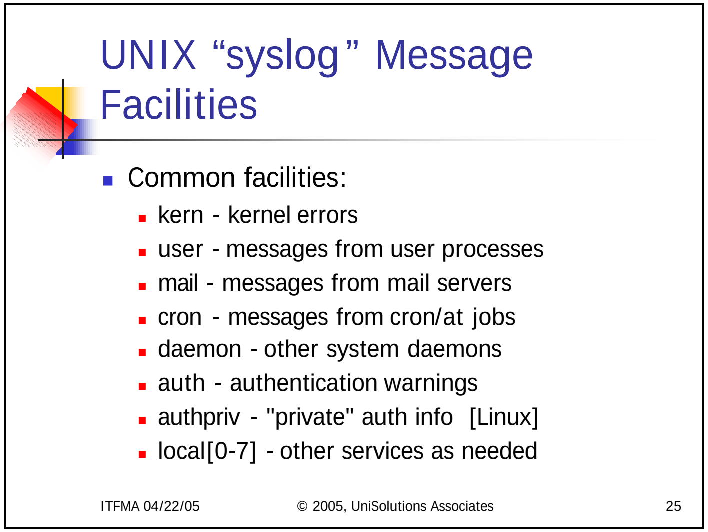
Chargeback Data Flow and Points of Interest…


Security Data Sources
Remote Accounting Databases
System Activity
Nightly Accounting
Local Accounting Database
Reporting Modules
Reports Graphs Budgets Billings
Project Information Database
User Interface



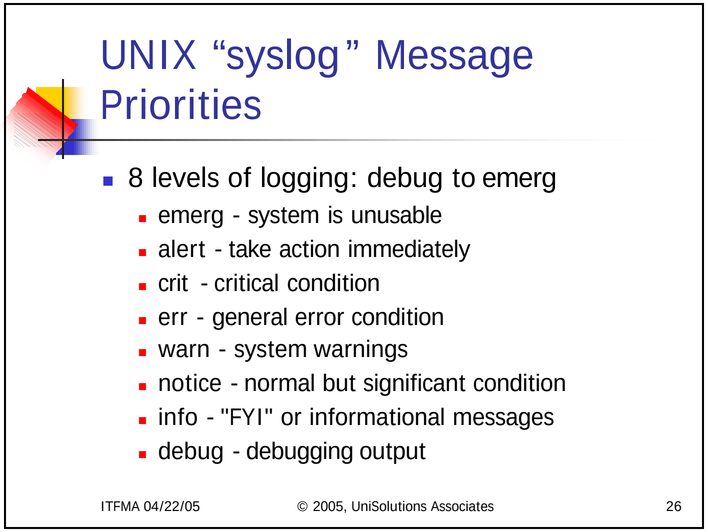
UNIX System Accounting/Log Files

	Linux	Solaris	HP-UX	AIX
Default Syslog Output	/var/log (messages, secure, boot.log)	/var/adm/ messages /var/log/syslog	/var/adm/syslog/ (mail.log, syslog.log)	/tmp or none!
System Accounting	/var/run/utmp /var/log/wtmp /var/account/ pacct	/var/adm/utmpx /var/adm/wtmpx /var/adm/pacct	/var/adm/utmp /var/adm/wtmp /var/adm/pacct	/etc/utmp /var/adm/wtmp/ var/adm/pacct
Login Errors	/var/log/btmp /var/log/ messages	/var/adm/ loginlog sulog	/var/adm/lastb /var/adm/sulog	/etc/security failedlogin, /var/adm/sulog



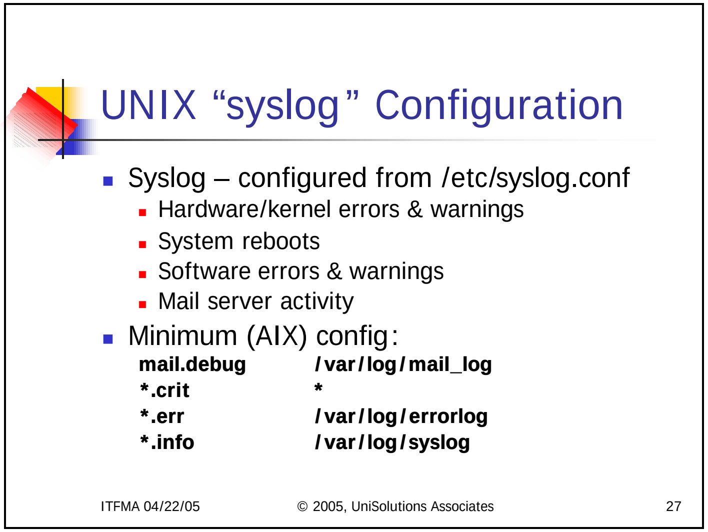
UNIX “syslog” Message Facilities

- Common facilities:
  - kern - kernel errors
  - user - messages from user processes
  - mail - messages from mail servers
  - cron - messages from cron/at jobs
  - daemon - other system daemons
  - auth - authentication warnings
  - authpriv - "private" auth info [Linux]
  - local[0-7] - other services as needed



UNIX “syslog” Message Priorities

- 8 levels of logging: debug to emerg
  - emerg - system is unusable
  - alert - take action immediately
  - crit - critical condition
  - err - general error condition
  - warn - system warnings
  - notice - normal but significant condition
  - info - "FYI" or informational messages
  - debug - debugging output



UNIX “syslog” Configuration

- Syslog – configured from /etc/syslog.conf
  - Hardware/kernel errors & warnings
  - System reboots
  - Software errors & warnings
  - Mail server activity
- Minimum (AIX) config:

```
mail.debug      /var/log/mail_log
*.crit          *
*.err           /var/log/errorlog
*.info          /var/log/syslog
```

Syslog Event Sample

```
Jan  9 14:30:16 unisol xntpd[309]: [ID 126520 daemon.info]
    system event 'event_sync_chg' (0x03) status 'leap_none,
    sync_ntp , 15 events, event_peer/strat_chg' (0x6f4)
Jan  9 14:31:30 unisol sendmail[9333]: [ID 801593 mail.notice]
    j09MVLW09333: ruleset=check_rcpt,
    arg1=<moreno@unisol.com>,
    relay=pcp0010981600pcs.hyatsv01.md.comcast.net
    [68.54.94.75], reject=550 5.7.1 <moreno@unisol.com>... Mail
    from 68.54.94.75 refused by blackhole site dnsbl.sorbs.net
Apr  4 20:49:39 unisol shutdown: [ID 600729 auth.crit] reboot by
    root
Apr  4 20:49:41 unisol xntpd[27132]: [ID 866926 daemon.notice]
    xntpd exiting on signal 15
```

Syslog Security Issues

- Can be altered:
  - When system is compromised
  - Altered and/or truncated by rootkits
- Solution: log to a remote system or a dedicated syslog server
  - Can log to both local and remote system
  - Filter port 514 at firewall

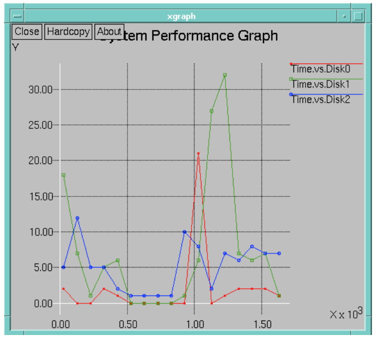
UNIX System Accounting/Performance Data

- System resource usage data:
  - CPU and memory utilization
  - paging
  - Disk and file I/O
  - TTY activity
  - System calls
  - semaphore activity
- Detect intruders
  - Check for gaps in accounting data
  - Usage spike (DoS – ip spoof, smurf, …)

UNIX Performance Data

- Top
- Vmstat (Solaris)
- Sadc/sa1/sa2 – collect data
- Sar – report on collected or real-time data
- Sag – Graphical (tek term emulation in xterm) reports of sar/sadc data
- Data can be exported to text files or spreadsheets
  - JobAcct ™ generates X/Motif graphs

Graphing System Performance Data – JobAcct sample



Sample “top” Output

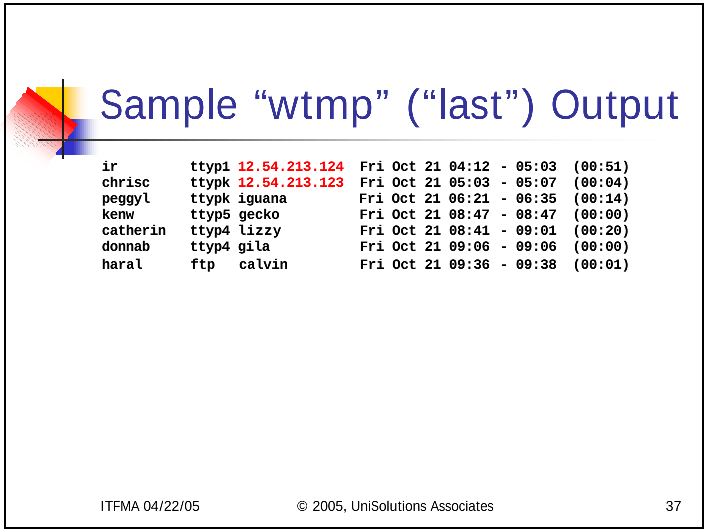
```
load averages:  0.32,  0.14,  0.11                                  22:39:38
132 processes: 127 sleeping, 2 running, 1 zombie, 1 stopped, 1 on cpu
CPU states:  0.0% idle,  1.6% user, 24.5% kernel, 73.9% iowait,  0.0% swap
Memory: 1024M real, 49M free, 1123M swap in use, 2735M swap free

   PID USERNAME THR PRI NICE  SIZE   RES STATE    TIME    CPU COMMAND
   987 craig      6  40    0   15M 3032K sleep  393:57  4.66% sunpcbinary
 22622 haral      1  60    0 1008K  824K sleep    0:07  4.26% du
 22645 haral      1  60    0 1008K  824K sleep    0:02  3.57% du
   661 root       1  59    0  191M   67M sleep   29.1H  1.20% Xsun
 22650 root       1  58    0 2248K 1328K cpu      0:00  0.25% top
   708 oracle     1  48    0    0K    0K sleep  118:05  0.07% oracle
   700 oracle    13  59    0    0K    0K sleep   12:18  0.03% oracle
  9482 craig     10  49    0  162M  125M run    255.3H  0.02% mozilla-bin
  4582 root       1  58    0 4128K 2776K sleep    0:20  0.02% smbd
   243 root       1  58    0 6928K 5880K sleep   12:20  0.02% in.named
   620 root      12  58    0 4272K 3584K sleep   19:48  0.02% mibiisa
   232 daemon     6  58    0 2712K 1464K sleep    0:02  0.01% statd
 22924 bob        7  58    0  270M   95M sleep   59:24  0.01% mozilla-bin
  1371 haral      1  59    0 7592K 4080K sleep    2:07  0.01% dtterm
   221 root       1  58    0 2736K 1368K sleep    0:37  0.01% inetd
```

Sample “vmstat” Output

```
#  vmstat 5 15
 procs     memory            page            disk          faults      cpu
 r b w   swap  free  re  mf pi  po fr de sr f0 s0 s1 s6   in   sy   cs us sy id
 0 0 0 3124696 143928 6  27 40 12 12  0  0  0  8  2  0  401    1  516 16  1 83
 0 0 0 2801488 18896  3  56 432 0  0  0  0  0 103 0  0  760 4053  756  3 10 88
 0 0 0 2801424 16808  1  17 843 8  8  0  0  0 175 0  0 1069 8940 1008  4 19 76
 0 0 0 2801424 24328  1  28 928 8  8  0  0  0 177 0  0 1075 9088 1020  5 16 78
 0 0 0 2801424 37408  1  22 1081 0 0  0  0  0 168 0  0 1075 8256 1008  5 16 79
 0 1 0 2801120 37584  0  51 956 0  0  0  0  0 166 0  0 1111 5163  967  2 11 87
 0 3 0 2800704 37432  3  43 288 0  0  0  0  0 130 0  0  956 2580  724  2  4 93
 0 2 0 2801208 38720  0  16 507 0  0  0  0  0 120 0  0 1178 5459 1012  2  8 90
 0 2 0 2801200 39520  1  22 507 0  0  0  0  0 126 0  0 1197 4689 1047  3  7 90
 0 1 0 2801200 39256  0  28 598 0  0  0  0  0 115 0  0 1168 4515 1028  3  7 90
 0 2 0 2801200 39232  0  17 620 0  0  0  0  0 125 0  0 1215 5059 1043  2  8 90
 0 1 0 2801200 39272  0  28 568 0  0  0  0  0 128 0  0 1198 4614 1011  3 11 86
 0 3 0 2801200 39624  0  22 180 0  0  0  0  0 195 0  0 1045 2382  581  2  4 94
 0 1 0 2801320 41696  0  23 667 0  0  0  0  0 170 0  0 1137 7228 1079  4 12 84
 0 1 0 2801352 44624  0  28 705 0  0  0  0  0 160 0  0 1030 7658 1003  6 16 79
```

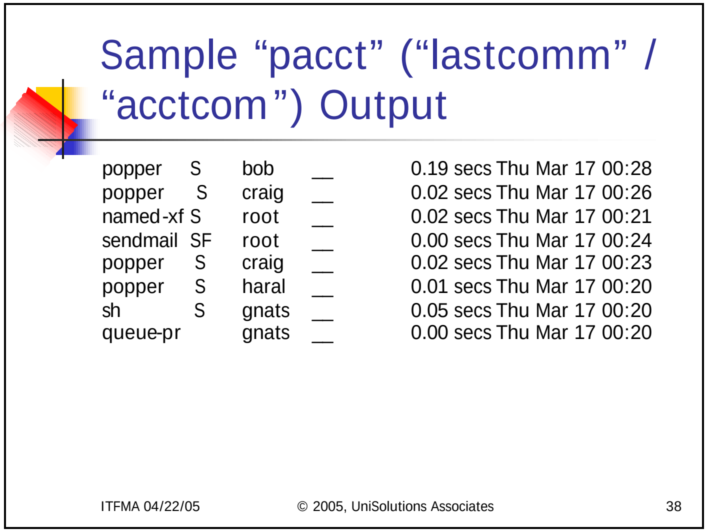
UNIX Login & Process Accounting Files

- utmp – current logins
- wtmp – login history
- pacct – process history
- sulog – su history
- loginlog – failed login attempts



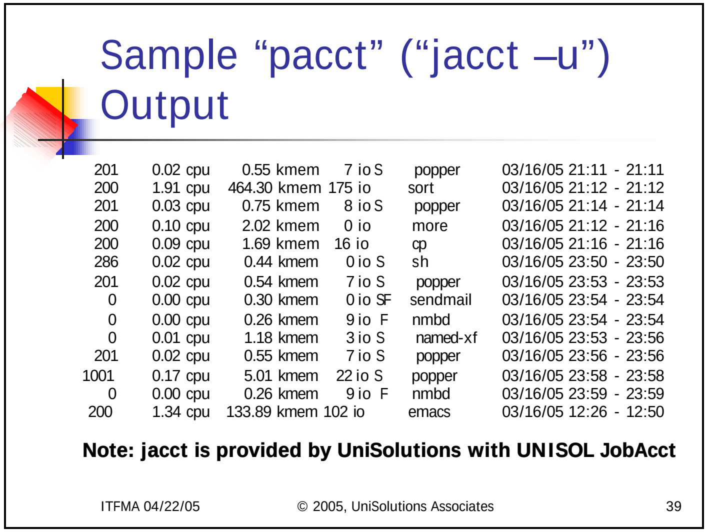
Sample “wtmp” (“last”) Output

```
ir        ttyp1 12.54.213.124  Fri Oct 21 04:12 - 05:03  (00:51)
chrisc    ttypk 12.54.213.123  Fri Oct 21 05:03 - 05:07  (00:04)
peggyl    ttypk iguana         Fri Oct 21 06:21 - 06:35  (00:14)
kenw      ttyp5 gecko          Fri Oct 21 08:47 - 08:47  (00:00)
catherin  ttyp4 lizzy          Fri Oct 21 08:41 - 09:01  (00:20)
donnab    ttyp4 gila           Fri Oct 21 09:06 - 09:06  (00:00)
haral     ftp   calvin         Fri Oct 21 09:36 - 09:38  (00:01)
```



Sample “pacct” (“lastcomm” / “acctcom”) Output

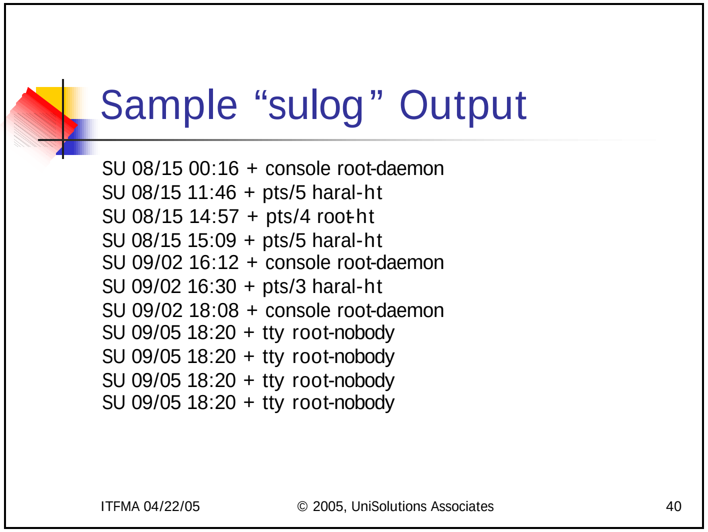
```
popper     S    bob     __     0.19 secs Thu Mar 17 00:28
popper     S    craig   __     0.02 secs Thu Mar 17 00:26
named-xf   S    root    __     0.02 secs Thu Mar 17 00:21
sendmail   SF   root    __     0.00 secs Thu Mar 17 00:24
popper     S    craig   __     0.02 secs Thu Mar 17 00:23
popper     S    haral   __     0.01 secs Thu Mar 17 00:20
sh         S    gnats   __     0.05 secs Thu Mar 17 00:20
queue-pr        gnats   __     0.00 secs Thu Mar 17 00:20
```



Sample “pacct” (“jacct –u”) Output

```
 201   0.02 cpu    0.55 kmem    7 io S   popper    03/16/05 21:11 - 21:11
 200   1.91 cpu  464.30 kmem  175 io     sort      03/16/05 21:12 - 21:12
 201   0.03 cpu    0.75 kmem    8 io S   popper    03/16/05 21:14 - 21:14
 200   0.10 cpu    2.02 kmem    0 io     more      03/16/05 21:12 - 21:16
 200   0.09 cpu    1.69 kmem   16 io     cp        03/16/05 21:16 - 21:16
 286   0.02 cpu    0.44 kmem    0 io S   sh        03/16/05 23:50 - 23:50
 201   0.02 cpu    0.54 kmem    7 io S   popper    03/16/05 23:53 - 23:53
   0   0.00 cpu    0.30 kmem    0 io SF  sendmail  03/16/05 23:54 - 23:54
   0   0.00 cpu    0.26 kmem    9 io  F  nmbd      03/16/05 23:54 - 23:54
   0   0.01 cpu    1.18 kmem    3 io S   named-xf  03/16/05 23:53 - 23:56
 201   0.02 cpu    0.55 kmem    7 io S   popper    03/16/05 23:56 - 23:56
1001   0.17 cpu    5.01 kmem   22 io S   popper    03/16/05 23:58 - 23:58
   0   0.00 cpu    0.26 kmem    9 io  F  nmbd      03/16/05 23:59 - 23:59
 200   1.34 cpu  133.89 kmem  102 io     emacs     03/16/05 12:26 - 12:50
```

Note: jacct is provided by UniSolutions with UNISOL JobAcct



Sample “sulog” Output

```
SU 08/15 00:16 + console root-daemon
SU 08/15 11:46 + pts/5 haral-ht
SU 08/15 14:57 + pts/4 root-ht
SU 08/15 15:09 + pts/5 haral-ht
SU 09/02 16:12 + console root-daemon
SU 09/02 16:30 + pts/3 haral-ht
SU 09/02 18:08 + console root-daemon
SU 09/05 18:20 + tty root-nobody
SU 09/05 18:20 + tty root-nobody
SU 09/05 18:20 + tty root-nobody
SU 09/05 18:20 + tty root-nobody
```

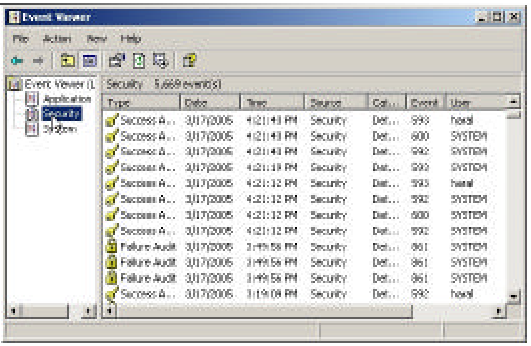
Kernel Level Auditing

- Most UNIX systems allow "kernel-level" auditing ("C2" level or above)
- Every system call can be logged:
  - Great level of detail
  - Generates a lot of data
  - Potential system performance impact
  - No good tools for analyzing audit trail
  - Must be enabled manually
- Configuration required...

Windows Event Log

- Application Error Records
- Security Audit Records
- System Error Records
- DNS Error Records (DNS)
- Directory Service Error Records (DC)
- File Replication Service Error Records (DC)

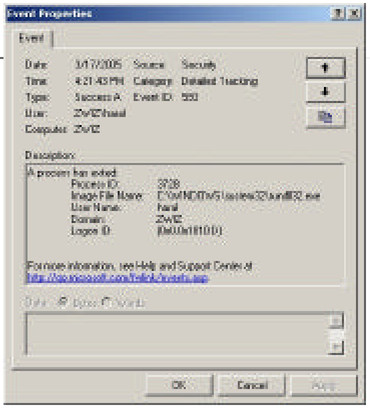
Security Event Log Screen



Security 5,669 event(s)

Type	Date	Time	Source	Cat...	Event	User
Success A...	3/17/2005	4:21:43 PM	Security	Det...	593	hand
Success A...	3/17/2005	4:21:43 PM	Security	Det...	600	SYSTEM
Success A...	3/17/2005	4:21:43 PM	Security	Det...	592	SYSTEM
Success A...	3/17/2005	4:21:19 PM	Security	Det...	592	SYSTEM
Success A...	3/17/2005	4:21:12 PM	Security	Det...	593	hand
Success A...	3/17/2005	4:21:12 PM	Security	Det...	592	SYSTEM
Success A...	3/17/2005	4:21:12 PM	Security	Det...	600	SYSTEM
Success A...	3/17/2005	4:21:12 PM	Security	Det...	592	SYSTEM
Failure Audit	3/17/2005	3:49:56 PM	Security	Det...	861	SYSTEM
Failure Audit	3/17/2005	3:49:56 PM	Security	Det...	861	SYSTEM
Failure Audit	3/17/2005	3:49:56 PM	Security	Det...	861	SYSTEM
Success A...	3/17/2005	3:19:08 PM	Security	Det...	592	hand

Detailed Event Screen



Date: 3/17/2005 Source: Security
Time: 4:21:43 PM Category: Detailed Tracking
Type: Success A Event ID: 593
User: ZWIZ\hand
Computer: ZWIZ

Description:

A process has exited:
Process ID: 3728
Image File Name: C:\WINDOWS\system32\rundll32.exe
User Name: hand
Domain: ZWIZ
Logon ID: (0x0,0x181D1)

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

View Event Log (with process activity) with "dumpel"

```
1/12/2005     10:44:23 PM  8    5    593  Security   NT
    AUTHORITY\NETWORK SERVICE    ZWIZ   2840
    C:\WINDOWS\system32\wbem\wmiprvse.exe NETWORK SERVICE
    NT AUTHORITY (0x0,0x3E4)
1/12/2005     10:48:05 PM  8    5    593  Security   NT
    AUTHORITY\SYSTEM          ZWIZ   2420
    C:\WINDOWS\system32\wuauclt.exe ZWIZ$ MAVENT (0x0,0x3E7)
1/12/2005     10:52:38 PM  8    5    592  Security   ZWIZ\haral
    ZWIZ  1164 C:\Program Files\Real\RealPlayer\rphelperapp.exe 1896
    haral ZWIZ (0x0,0x1F298)
1/12/2005     10:52:38 PM  8    5    861  Security   ZWIZ\haral
    ZWIZ   RealPlayer C:\Program Files\Real\RealPlayer\realplay.exe
    1896 haral ZWIZ No No IPv4 UDP 1097 Yes No
1/12/2005     10:52:38 PM  8    5    593  Security   ZWIZ\haral
    ZWIZ  1164 C:\Program Files\Real\RealPlayer\rphelperapp.exe haral
    ZWIZ (0x0,0x1F298)
```

Note: dumpel is available on the Windows 2000 Resource Toolkit

Summarize Process Activity from System Event Log

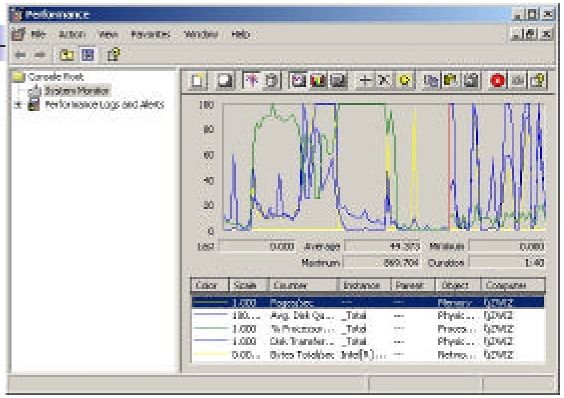
- "jacct –l" output

```
haral     log.exe        2176400896 0x0,0x6a3d 03/09/98 14:40 -
    03/09/98 14:40
haral     more.com       2188125152 0x0,0x6a3d 03/09/98 14:40 -
    03/09/98 14:40
haral     cmd.exe        2176731072 0x0,0x6a3d 03/09/98 14:40 -
    03/09/98 14:40
haral     CAT.EXE        2176400896 0x0,0x6a3d 03/09/98 14:43 -
    03/09/98 14:43
haral     CL.EXE         2169915200 0x0,0x6a3d 03/09/98 14:47 -
    03/09/98 14:47
haral     VCSPAWN.EXE  2163179008 0x0,0x6a3d 03/09/98 14:47 -
    03/09/98 14:47
```

Performance and Process Activity (Windows)

- Task Manager
- perfmon – Platform SDK or AdminTools
- Pstat - Platform SDK
- Pulist – Microsoft 2000 Support Tools
- Pslist/cpumon/diskmon - sysinternals
- Psl – JobAcct

Windows Performance Monitor



Last 0.000 Average 49.373 Minimum 0.000
Maximum 869.704 Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
	1.000	Pages/sec	---	---	Memory	\\ZWIZ
	100...	Avg. Disk Qu...	_Total	---	Physic...	\\ZWIZ
	1.000	% Processor...	_Total	---	Proces...	\\ZWIZ
	1.000	Disk Transfer...	_Total	---	Physic...	\\ZWIZ
	0.00...	Bytes Total/sec	Intel(R)...	---	Netwo...	\\ZWIZ

Process Activity summary with “jacct –p” Output (“pslistsvc”)

```
 PID  User      Command       AuthID        CPU Time WPeak WSet  IORead IOWrite  IOOther
      Start Time   ETime
2160 haral     avgw.exe      0x181dd,0x0     0.1001  4112   4072        60       11       680  03/16
      00:32-00:32
1500 haral     userinit.exe  0x181dd,0x0     0.2704  2848   2848         2        1       421  03/16
      00:43-00:45
1332 haral     avgw.exe      0x181dd,0x0 1257.6885  47524 5344   1859054     981    279 361
               03/16 02:59-03:55
3908 haral     realsched.exe  0x181dd,0x0    0.4006  2660    288        11        3       856  03/15
      08:43-08:44
 460 haral     userinit.exe  0x181dd,0x0     0.0701   2848  2848         2        1       421
               03/16 08:44-08:45
2176 SYSTEM  wuauclt.exe  0x3e7,0x0         0.2804   6264  6256       264       34      2118
               03/16 08:43-08:49
 492 haral     notepad.exe   0x181dd,0x0     0.3104  3564 3560          1        1       439
               03/16 10:51-10:52
3616 haral     pwquickstart.exe 0x181dd,0x0 0.5608 11636 10592      218       50      1050
               03/16 11:16-11:17
3072 haral     pwquickstart.exe 0x181dd,0x0 0.6910 11400 10424      219       49      1646
               03/16 11:58-11:58
3088 haral     pwconsole.exe 0x181dd,0x0 12.1174 21732 16100        271      292      2771
               03/16 11:16-12:03
 772 haral     grabber2k.exe 0x181dd,0x0   9.3034  16964 13380      246      347      4867 03/16
      12:15-13:04
3112 haral     pwconsole.exe 0x181dd,0x0 34.0590  24188 18880       283      451      5445
```

Command Usage Summary by User

- Command summary by user (cmdstats)

```
haral
        awk        4      0.03cpu        0Mmem      7 io
        cat        4      0.03cpu        0Mmem     11 io
        chmod      1      0.01cpu        0Mmem      3 io
        cp         3      0.22cpu        0Mmem     61 io
        cpio       4     73.72cpu        1Mmem   7162 io
        crontab    1      0.02cpu        0Mmem      8 io
        deroff     1      0.00cpu        0Mmem      4 io
        df         2      0.01cpu        0Mmem      7 io
        diff       1      0.02cpu        0Mmem      4 io
        emacs      5      5.21cpu        0Mmem    562 io
        expr       3      0.02cpu        0Mmem      4 io
        file       2      0.02cpu        0Mmem      8 io
        grep       7      4.29cpu        0Mmem    295 io
        gzip       8      0.16cpu        0Mmem     28 io
```

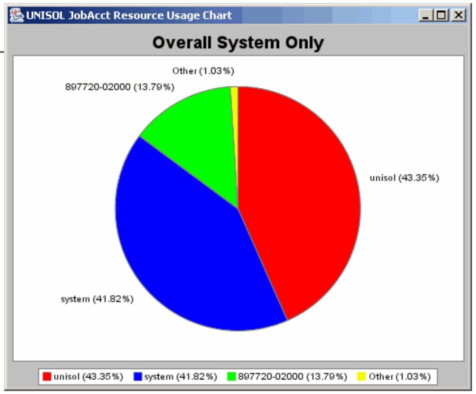
User-Level Chargeback Report

```
User      UID     Group        GID    Project
haral     1002    staff        513    unisol

# of Commands: 91      Logins: 3
Disk Blocks (1K): 124510 = $124.51
------------Connect Time (hrs)-----------
    Prime      Non-Prime             Reduced
     7.89           3.04                9.50
   $15.78          $4.56               $9.50
---------------CPU Time (mins)-----------
    Prime      Non-Prime             Reduced
    42.84           2.81                0.33
    $0.17          $0.01               $0.00
---------Total K-Core Minutes------------
    Prime      Non-Prime             Reduced
 58176.73        1530.02              593.42
    $0.52          $0.01               $0.00
…
      Total Amount: $156.25
```

Top-Level Chargeback Report

```
Resource Charge-Back Report         Page   1      Charge-Back Summary

    SYSTEM:    gecko                SITENAME: UniSolutions Associates
    Printed on 02/7/04              Period ending 02/7/04 (Weekly)

Project Accts Connect    CPU   Disk DskI/O    CORE   Pages %Total

netdev      2   4.97%  1.47%  0.00%  0.59%  0.41%  8.58%  3.32%
staff      14  15.08% 46.47% 44.36% 84.81% 52.55%  0.00%  29.70%
Test        6  61.34% 18.13% 24.75%  4.99% 13.16% 52.82%  37.80%
xdev        4  18.61% 33.93% 30.89%  9.61% 33.88% 38.61%  29.18%

TOTAL      26    100%   100%   100%   100%   100%   100%   100%
```

Top-Level Chargeback Pie Chart



Monitor System Usage Reports

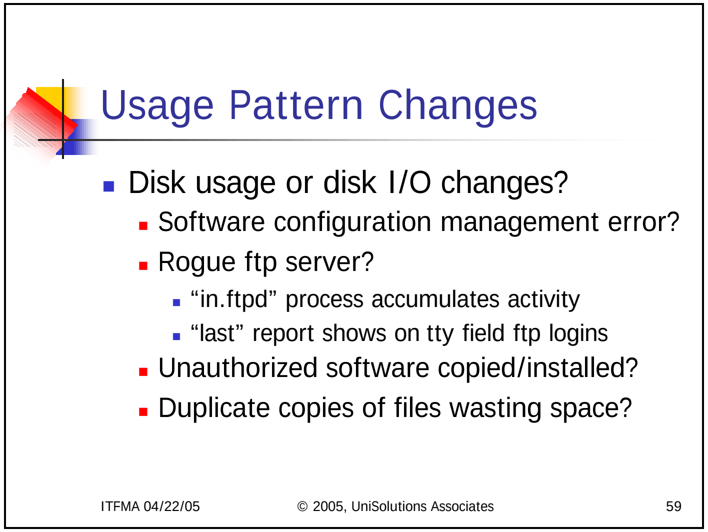
- Review Chargeback Reports
  - Understand system usage
  - Plan system upgrades
  - Observe change in usage patterns?
  - Notice new activity on inactive account?
  - Suspect excessive usage?
- Follow-up

Monitor System Usage

- Departments should review own usage
  - Users know project activity
  - Can point out unusual usage patterns
  - Side-benefits
    - Education can reduce resource usage
    - Postpone costly system upgrades
  - Get Upper management buy-in

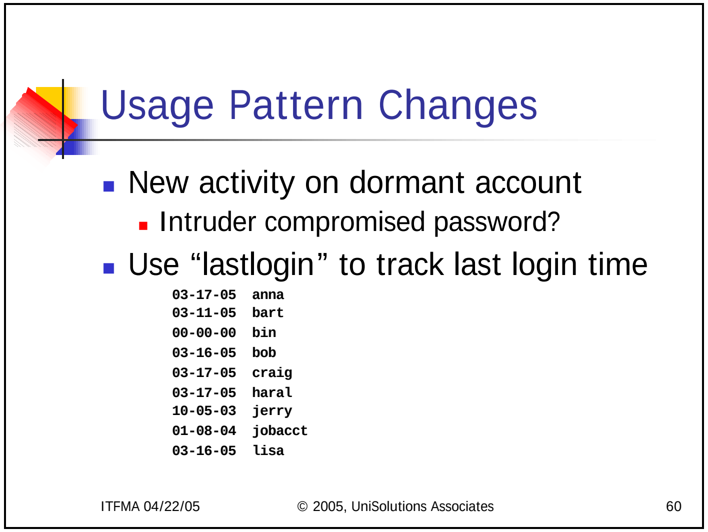
Usage Pattern Changes

- Cpu usage increase or change?
  - Malicious software may have been introduced into the system
  - User may be running password cracker
  - User may be scanning for vulnerabilities
  - Unauthorized/buggy software may be wasting cpu time, affecting other users
  - Incorrect system/software/device configuration



Usage Pattern Changes

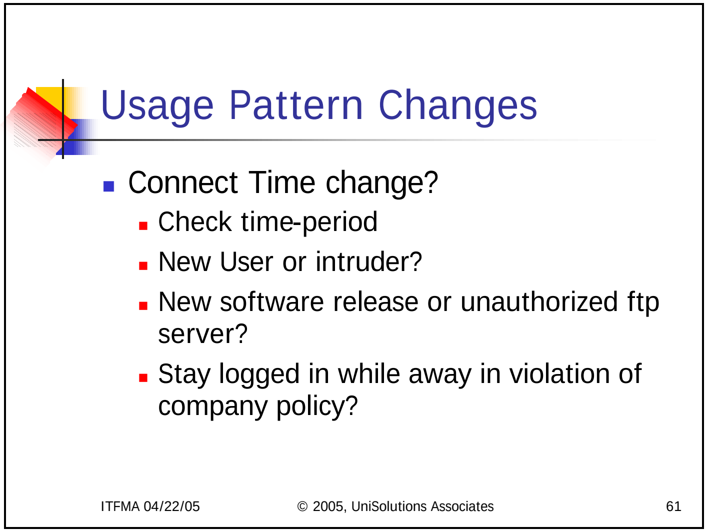
- Disk usage or disk I/O changes?
  - Software configuration management error?
  - Rogue ftp server?
    - “in.ftpd” process accumulates activity
    - “last” report shows on tty field ftp logins
  - Unauthorized software copied/installed?
  - Duplicate copies of files wasting space?



Usage Pattern Changes

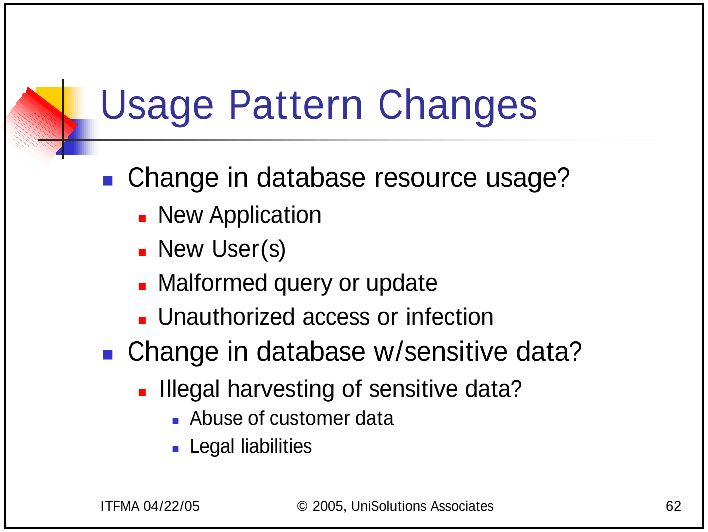
- New activity on dormant account
  - Intruder compromised password?
- Use “lastlogin” to track last login time

```
03-17-05  anna
03-11-05  bart
00-00-00  bin
03-16-05  bob
03-17-05  craig
03-17-05  haral
10-05-03  jerry
01-08-04  jobacct
03-16-05  lisa
```



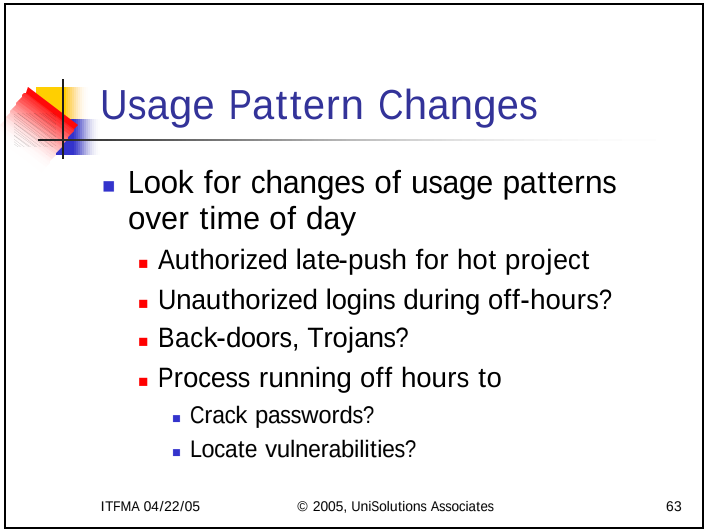
Usage Pattern Changes

- Connect Time change?
  - Check time-period
  - New User or intruder?
  - New software release or unauthorized ftp server?
  - Stay logged in while away in violation of company policy?



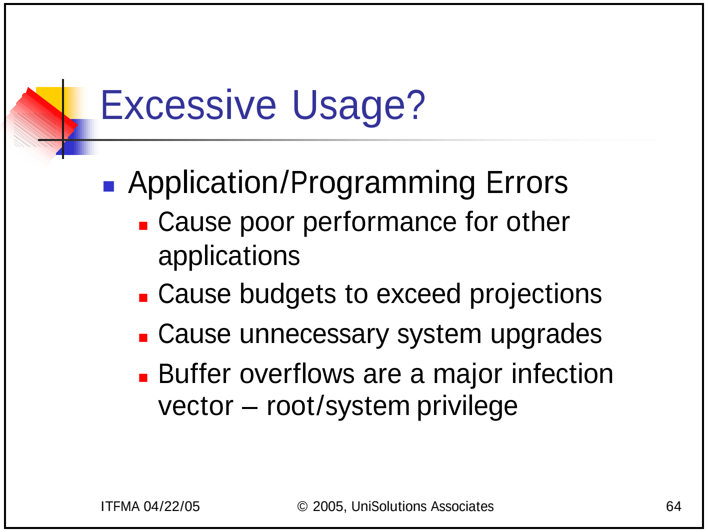
Usage Pattern Changes

- Change in database resource usage?
  - New Application
  - New User(s)
  - Malformed query or update
  - Unauthorized access or infection
- Change in database w/sensitive data?
  - Illegal harvesting of sensitive data?
    - Abuse of customer data
    - Legal liabilities



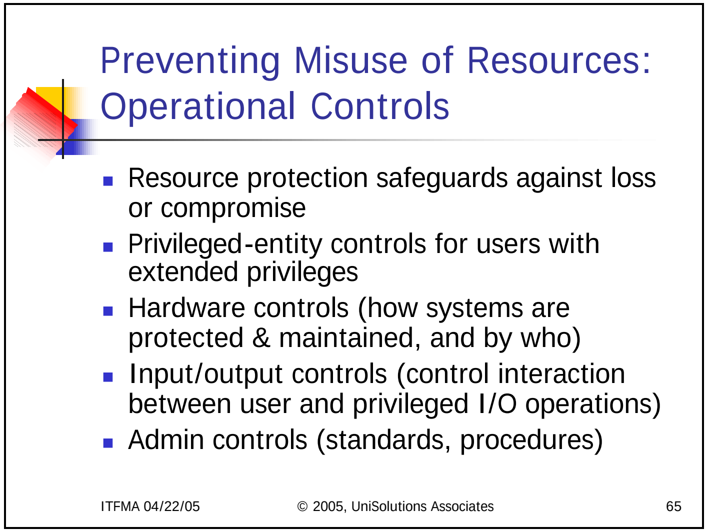
Usage Pattern Changes

- Look for changes of usage patterns over time of day
  - Authorized late-push for hot project
  - Unauthorized logins during off-hours?
  - Back-doors, Trojans?
  - Process running off hours to
    - Crack passwords?
    - Locate vulnerabilities?



Excessive Usage?

- Application/Programming Errors
  - Cause poor performance for other applications
  - Cause budgets to exceed projections
  - Cause unnecessary system upgrades
  - Buffer overflows are a major infection vector – root/system privilege

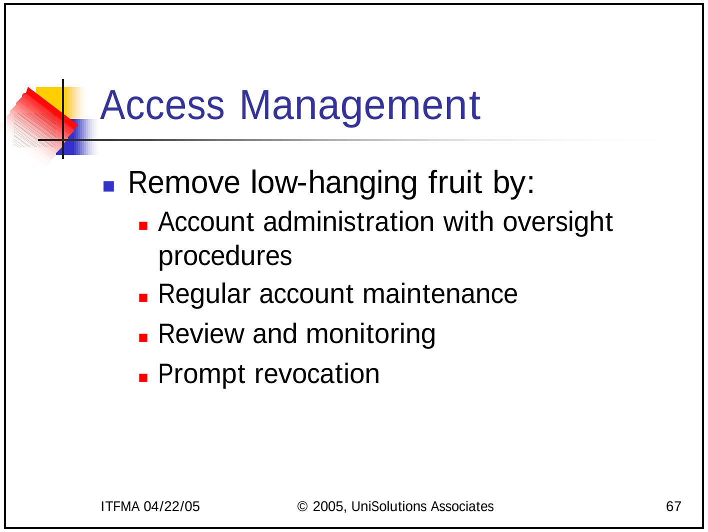


Preventing Misuse of Resources: Operational Controls

- Resource protection safeguards against loss or compromise
- Privileged-entity controls for users with extended privileges
- Hardware controls (how systems are protected & maintained, and by who)
- Input/output controls (control interaction between user and privileged I/O operations)
- Admin controls (standards, procedures)

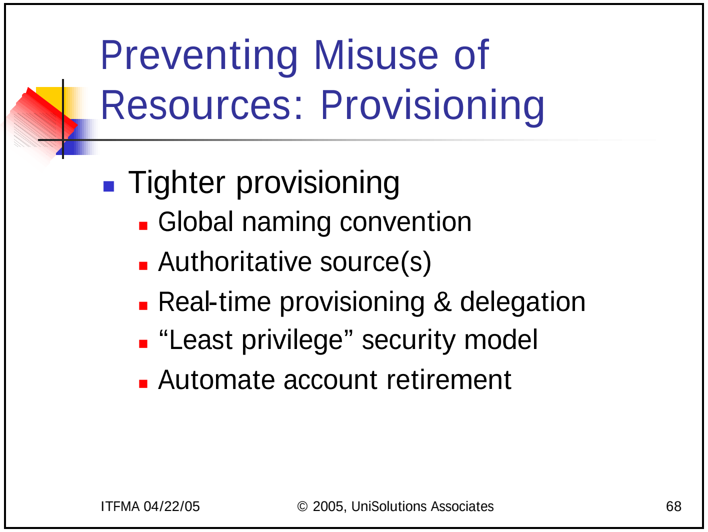
Preventing Misuse of Resources: Control Types

- Directive controls (administrative)
- Preventive controls (technical)
- Detective controls (validate preventive & detective controls)
- Corrective controls (procedures & instructions)
- Recovery controls (can organizations recover?)



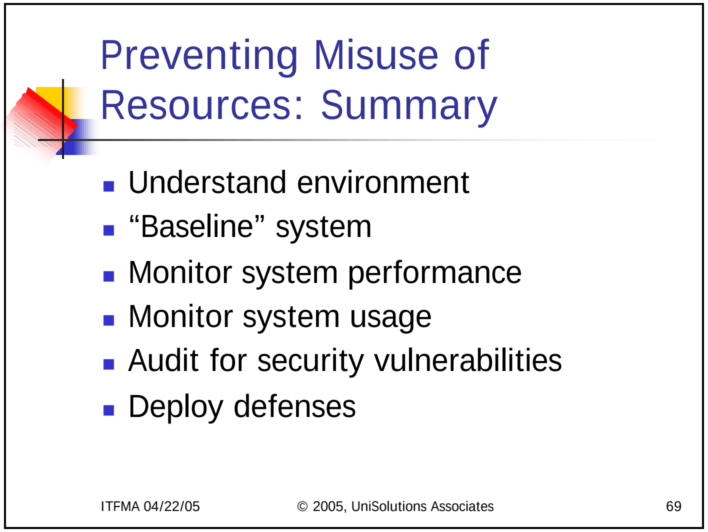
Access Management

- Remove low-hanging fruit by:
  - Account administration with oversight procedures
  - Regular account maintenance
  - Review and monitoring
  - Prompt revocation



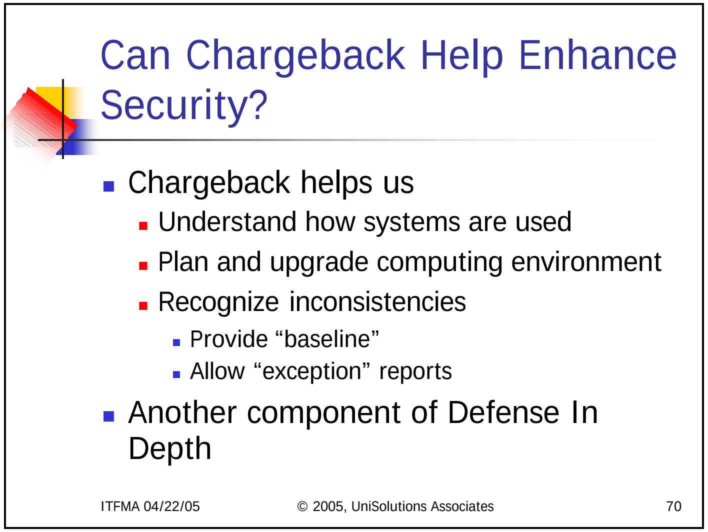
Preventing Misuse of Resources: Provisioning

- Tighter provisioning
  - Global naming convention
  - Authoritative source(s)
  - Real-time provisioning & delegation
  - “Least privilege” security model
  - Automate account retirement



Preventing Misuse of Resources: Summary

- Understand environment
- “Baseline” system
- Monitor system performance
- Monitor system usage
- Audit for security vulnerabilities
- Deploy defenses



Can Chargeback Help Enhance Security?

- Chargeback helps us
  - Understand how systems are used
  - Plan and upgrade computing environment
  - Recognize inconsistencies
    - Provide “baseline”
    - Allow “exception” reports
- Another component of Defense In Depth