VAB: Visual Audit Browsing

James A. Hoagland, Christopher Wee, Karl Levitt
Computer Security Laboratory
University of California, Davis
hoagland@cs.ucdavis.edu

NSA supported under the University Research Program
Audit WorkBench project (DOD-MDA904-92-C-5148)

<URL:http://seclab.cs.ucdavis.edu/awb/>

Visual Audit Browsing Applications

- ❏ Computer security incident investigation
- ❏ Investigative system administration tasks
- ❏ Program execution analysis
- ❏ Program signature analysis
- ❏ Other audit log analysis tasks

Users include:

- ❏ security investigators
- ❏ system administrators
- ❏ security tool developers

BSM Audit Log

```
file,Thu Oct 21 16:23:39 1993, + 970501 msec,
header,107,execve(2):,Thu Oct 21 16:23:43 1993, + 160000 msec
path,/,/usr/export/home/heberlei,/usr/export/home/heberlei/loadmodule
process,heberlei,heberlei,heberlei,staff,330
return,No such file or directory,-1
trailer,107
header,53,vfork(2): process creation,Thu Oct 21 16:23:43 1993, + 170000 msec
argument,0,330,child PID
process,heberlei,heberlei,heberlei,staff,319
return,Error 0,330
trailer,53
header,120,execve(2):,Thu Oct 21 16:23:43 1993, + 170000 msec
path,/,/usr/export/home/heberlei,/usr/openwin/bin/./loadmodule
attribute,104755,root,staff,1822,55365,56424
process,heberlei,root,heberlei,staff,330
return,Error 0,0
trailer,120
header,104,open(2): read,Thu Oct 21 16:23:43 1993, + 170000 msec
path,/,/usr/export/home/heberlei,/usr/lib/ld.so
attribute,100555,root,staff,1822,101476,25280
process,heberlei,root,heberlei,staff,330
return,Error 0,3
trailer,104
...
hheader,35,exit(2): process termination,Thu Oct 21 16:23:49 1993, + 100000 msec
process,heberlei,root,root,daemon,334
return,Error 0,0
trailer,35
header,141,stat(2):,Thu Oct 21 16:23:49 1993, + 610000 msec
path,/,/usr/export/home/heberlei/.wastebasket,/usr/export/home/heberlei/.wastebasket
attribute,42755,heberlei,staff,1822,59984,4414
process,heberlei,heberlei,heberlei,staff,174
return,Error 0,0
trailer,141
file,Thu Oct 21 16:23:51 1993, + 447661 msec,
```

Figure 1. Excerpt from BSM audit log

■
University of California, Davis
seclab@cs.ucdavis.edu

Visual Audit Browsing Toolkit

VAB Toolkit is four prototype tools to assist analysis of BSM audit logs

Frame Generator*

- ❏ Produces graphs of the audit log
  - nodes represent processes, files, and other objects
  - edges represent events and present associations

Movie Maker

- ❏ Produces animated sequences of audit graphs in Postscript format
- ❏ Graphs are like those in Frame Generator
- ❏ New nodes edges appear as the sequence goes along, corresponding to later events
- ❏ Inactive nodes and edges can disappear or fade away

* The output of some of these tools do not present well on transparencies; examples of the output of these tools are available on the WWW at <URL:http://seclab.cs.ucdavis.edu/awb/>.

■
University of California, Davis
seclab@cs.ucdavis.edu

Visual Audit Browsing Toolkit [2]

Hypertext Generator

- Produces HyperText Markup Language (HTML) format files corresponding to what is recorded in audit log
- Files produced correspond to:
  - audit uid with processes
  - files
  - time-ordered summary of audit log
  - index of files produced

Focussed Audit Browser

- Presents a graph of part of the audit log corresponding to a specified “focus” object
- Graph is similar to the ones from Frame Generator
- User interface is a HTML form that allows focus specification

University of California, Davis
seclab@cs.ucdavis.edu

Conclusions

Benefits of these tools

- Multiple associations are presented simultaneously
  - Method of looking directly at textual log only indicates time-wise connections directly
- Graphs present overview of log
- Replay captures the temporal dimension of audit log
- Hypertext allows rapid browsing of audit logs
- WWW permits distributed browsing and annotation
  - Coordinated analysis by SSOs at different sites
  - Security and privacy an issue

Challenges faced by these tools

- Frame Generator and Movie Maker don’t scale well with the size of the log
- CPU use for tools is proportional to size of log
- Relative time of occurrence of events in audit log is not always accurate, hindering accurate movies

University of California, Davis
seclab@cs.ucdavis.edu

Future Work

Incorporate additional information into visualization

❏ Sources such as:

- system policy
- attack database
- program, user, and attacker profiles
- multiple audit sources including application ones
- IDS output
- security analysis tool output, i.e., from Tripwire and SATAN

❏ To do this, aggregation and integration techniques needs to be studied

Enhance toolkit

❏ Add the use of color and other media to visualizations

❏ Expand Frame Generator with different “views” of the audit log

❏ Allow non-BSM audit sources

❏ Adjust reported order of events to be more accurate

■
University of California, Davis
seclab@cs.ucdavis.edu