Audit BoFs

Steve Grubb
Red Hat

What's happened over the last year?

Filesystem auditing in upstream kernel
New IO protocol to allow new things to be expressed
Audit by selinux subject/object
Audit event dispatcher
SE Linux troubleshooter
Many new message types
New keywords for time in search utilities
Labels provided in every message

What's new (cont.)

Filter keys added to syscalls
New event exclusion filter in kernel
autrace has threat model option
execute a script as an action to auditd (rotate,space,err)
ausearch/aureport take stdin
ausearch can output unprocessed events (for piping)

Current Work

Auparse
new event dispatcher
immutable configuration

Near term work

Audit directory tree
new rule operators for bit mapped syscall function
audit a process and its children
Closer mapping of file system auditing with language in NISPOM/DCID 6/3

Near term work (cont.)

Remote logging
Compression
GUI based tools
Pushing into more trusted apps
Change setting of loginuid to syscall

Future Direction

Look into IDS/IPS
Add more security relevant events like segfaults
Integrate with security config scanner
Integration with crypto events
Remote logging protocols like IMDEF/XDAS

Discussion

?