Linux Kernel Security

A general overview to MAC

"If you tell the truth, you don’t have to remember anything.", Mark Twain

Alexandre Dulaunoy <adulau@conostix.com>, <adulau@foo.be>

Agenda

- Unix Security and current issues with DAC
- Mandatory Access Control
- Overview of existing Free Software implementation
- LIDS
- SELinux
- RSBAC
- Others
- Implementation
- Bibliography

Current Operating System security

- DAC is enough ? (discretionary access control)
- Decisions are only based on user identity and ownership
- Each user has complete discretion over his objects
- Only two major categories of users : user and superuser
- Some services must run as superuser
- No protection against malicious software
- If superuser is compromised...

Mandatory Access Control

- MAC versus DAC
  - DAC : user (or group of users) can decide on their objects
  - MAC : user (or group of users) can't decide on their objects
  - (example : SECRET classification)
- Separation Policies
  - Enforcing Legal restrictions on data
  - Establishing well-defined user roles
  - Restrictions to classified/compartmented data
- Containment Policies
  - Minimizing damage from viruses to other malicious code
  - (example : http server/mod_ssl worm)
- Integrity Policies
  - Protecting applications from modification
- Invocation Policies
  - Guaranteeing that data is processed as required
  - (example : freeswan encryption policies)

LIDS (http://www.lids.org/)

- Linux kernel patch for adding :
  - File protection
  - Process protection
  - Kernel Sealing (i/o mem, modules,...)
  - Misc
- Examples :
- lidsadm -A -s /usr/local/apache/bin/httpd -o CAP_NET_BIND -j GRANT
- lidsadm -A -o /etc/shadow -j DENY
- lidsadm -A -s /bin/login -o /etc/shadow -j READ

SELinux (http://www.nsa.gov/selinux/)

- Combines type enforcement (own process domain) & role-based access control
- Using the flask architecture (Object Manager <---AVC---> Security Server)
- Interface well defined
- More complex to implement
- Will be in 2.5 via LSM (Linux Security Module)
  - Type Enforcement with insmod :
  - allow sysadm_t insmod_exec_t:file x_file_perms;
  - allow sysadm_t insmod_t:process transition;
  - allow insmod_t insmod_exec_t:process {entrypoint execute};
  - allow insmod_t sysadm_t fd:inherit_fd_perms;
  - allow insmod_t self:capability sys_module;

RSBAC (http://www.rsbac.de/)

- RSBAC is a control framework
- Generalized Framework for Access Control (GFAC)
- You can combine model from MAC, RC (Role), ACL...
- You can write your own model

- Shell tools (rsbac_*) and dialog tools

- Similarity with SELinux and opposition (f.example : extended API calls)

- Future versus LSM ? Integration ?

Others

Medusa DS9

- Medusa provides a user-space authorization server called Constable. Before performing any tasks, the kernel asks permission from the Constable. Speedy communication between Constable and the kernel is achieved with a special device file /dev/medusa. Medusa includes a kernel patch and the Constable daemon.

- Paradox of user-space / kernel-space

Others

LOMAC

- LOMAC implements MAC integrity protection based on the Low Water-Mark model using Linux loadable kernel modules. Its a bit different from the other security products, as there is no configuration required, nor are there any kernel patches or modifications to existing files. LOMAC divides the system into two conceptual levels of integrity, high and low. Access control is based on integrity level and not on user identity. System binaries, configuration files, and kernel servers are placed in the high level, and user-interacting daemons are relegated to low levels.

Conclusion

- Test, test, test...
  - UML (User Mode Linux)
  - syscalltrak to debug
- GNU/Linux critics around the lack of MAC ?
  - LIDS, SELinux, RSBAC -> Usable in 2.4
  - LSM -> Kernel 2.5
- MAC is a usable solution for critical GNU/Linux server
-

Bibliography

- LSM (Linux Security Module) http://lsm.immunix.org/
- SELinux http://www.nsa.gov/selinux/
- LIDS http://www.lids.org/
- RSBAC http://www.rsbac.de/
- Medusa http://medusa.terminus.sk/
- Lomac http://freshmeat.net/projects/lomac
- Linux ACL http://acl.bestbits.at/
- Syscalltrak http://syscalltrak.sf.net/