CERIAS

the center for education and research in information assurance and security

Analyzing Protection Quality of Security-Enhanced Operating Systems

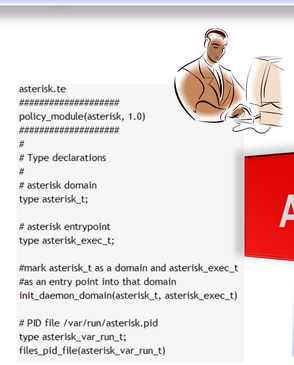
Hong Chen Ninghui Li Ziqing Mao

Motivation

- Host compromise is a serious problem
- Operating system security enhancement
  - DAC + MAC

SELinux redhat. AppArmor suse User Account Control IE Protected Mode

High-Level Security Properties



```
asterisk.te
#####################
policy_module(asterisk, 1.0)
#####################
#
# Type declarations
#
# asterisk domain
type asterisk_t;

# asterisk entrypoint
type asterisk_exec_t;

#mark asterisk_t as a domain and asterisk_exec_t
#as an entry point into that domain
init_daemon_domain(asterisk_t, asterisk_exec_t)

# PID file /var/run/asterisk.pid
type asterisk_var_run_t;
files_pid_file(asterisk_var_run_t)
```

A Wide Gap!

- What attacks are prevented?
- How to penetrate?
- Use another distribution?

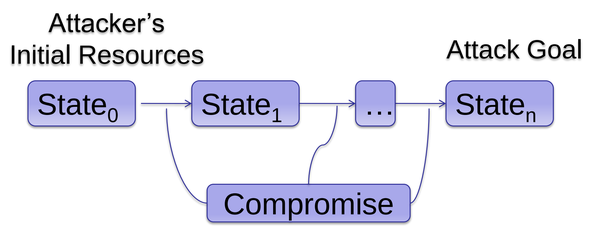
Low-Level Security Policy Rules

Vulnerability **S**urface **An**alyzer (**VulSAN**)

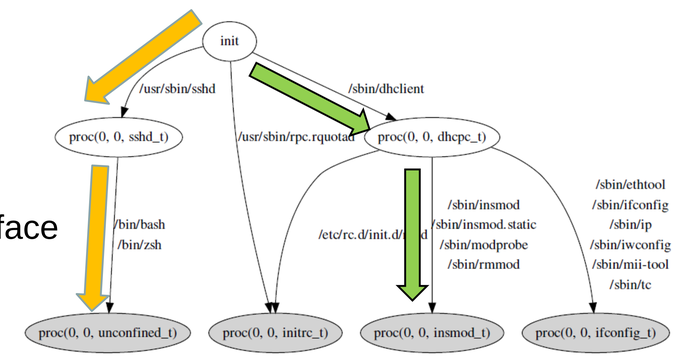
➢Analyze and compare the quality of protection offered by MAC policies in Linux

Solution

- Attack Scenario = Attack's Initial Resource + Attack Goal
  - Network access, local account, …
  - Load kernel module, plant Trojan Horse, …
- State Transition
  - SELinux: *proc(uid, gid, domain)*
  - AppArmor: *proc(uid, gid, profile)*



- Host Attack Graph
  - Attack paths
  - Vulnerability surface



- Logic Programming
  - System facts
  - System rules

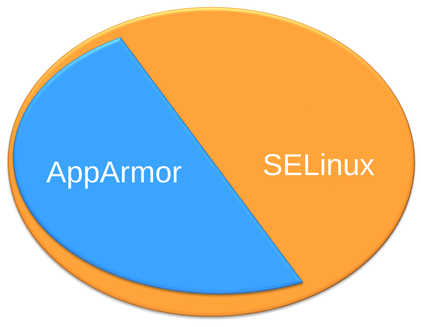
```
se_can_execute_type(Domain, Type, NewDomain) :-
se_typetrans(old_dom(Domain), new_dom(NewDomain), type(Type)),
!,
se_domain_privilege(domain(Domain), type(Type), class(file), op(execute)),
se_domain_privilege(domain(Domain), type(NewDomain), class(process), op(transition)),
se_domain_privilege(domain(NewDomain), type(Type), class(file), op(entrypoint)).

se_can_execute_type(Domain, Type, NewDomain) :-
se_domain_privilege(domain(Domain), type(Type), class(file), op(execute)),
se_domain_privilege(domain(Domain), type(Type), class(file), op(execute_no_trans)),
NewDomain = Domain.
```

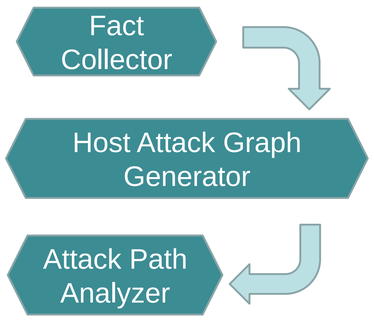
Results

- Evaluation (SELinux / AppArmor)
  - Ubuntu Server Edition 8.04
  - SUSE Linux Server Edition 10
  - Fedora 8
- Show tightening opportunities

Vulnerability Surface: SELinux vs. AppArmor
Ubuntu Server Edition 8.04



- Unique attack paths of SELinux
  - Privileged programs run under unconfined_t: nmbd, smbd, vsftpd, portmap, and rpc.statd
  - Confinement not as tight as AppArmor: cupsd and dhclient
  - Setuid confinement: ping, passwd
- Conclusion – with data
  - In this configuration, AppArmor provides better protection



Full paper appeared in the *16th Network and Distributed System Security Symposium (NDSS)* 2009

PURDUE UNIVERSITY CERIAS® Discovery Park e-Enterprise Center