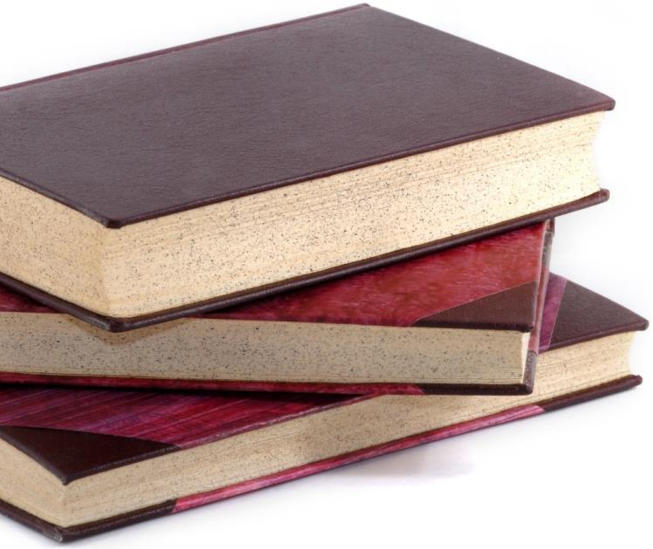
MPSIT

Lecture 8



8

Security

06 decembrie 2016

Outline

- Security in Linux
- SELinux
- Grsecurity
- Yocto Project security
- Meta-security
- Meta-selinux

Recap: real-time

- GPOS vs RTOS: Linux was enhances for real-time scenarios support also
- PREEMT_RT: Linux real-time solution
- Yocto Project –rt kernel: PREEMPT_RT supported by Yocto Project
- Linux real-time apps: real-time operating system has special real-time application requirements
- Benchmarking: Evaluation scenarios for a RTOS context
- Meta-realtime: Yocto Project real-time activities related layer initiative

Outline

- Security in Linux
- SELinux
- Grsecurity
- Yocto Project security
- Meta-security
- Meta-selinux

Security in Linux

- Important part of the entire Linux ecosystem
- Behind security names as James Morris appear
- Represented by a number of security features and programs
- Security required at every levels
- Linux security subsystem – kernel security: http://kernsec.org/wiki/index.php/Main_Page

Security status

- We still design IT infrastructures like we designed cars in the 60s. What does that mean?
  - More Hz, RAM, cores
  - Larger, faster disks
  - Faster, lower-latency networks
  - One click deployment
  - Containers, for everyone to deploy
- The status began to change a bit though

2016 IT engineer

- Designs components to run safely
- Nothing leaks, explodes or jabs you in the face
- Nothing catches on fire under most conditions
- Harmful traffic is kept well away from users
- Components fail safely by saving state and dumping core before crashing

How about human errors?

- IT company responses:
  - Protecting users against their own mistakes is expensive
  - Adding safety features sacrifices usability
  - Problem much better solved by user education
  - Customers are just not asking for it so why bother
- This might take some time after changing
- More IT security positions or collaborate with security specialized companies appeared
- Security is regaining the interest inside companies

Linux security subsystem

- Provides security enhancements and verification to the Linux kernel
- Maintains a certain level of trust
- Current focus on upstreaming grsec/pax features
- Responsible for:
  - Testing of critical subsystems for various vulnerabilities
  - Development of tools required for Linux kernel security assistance
  - Guidance and maintenance
  - Security improvements to various projects or build systems

Security as a Linux objective

- Lack of security was for a long time the source of problems
- It constituted an external factor for most companies
- Requested by clients due to latest industry trends
- Became an even bigger problem due to lack of actual overall knowledge around employees
- Driven by Linux Foundation
- Kill classes of bugs vs individual bugs

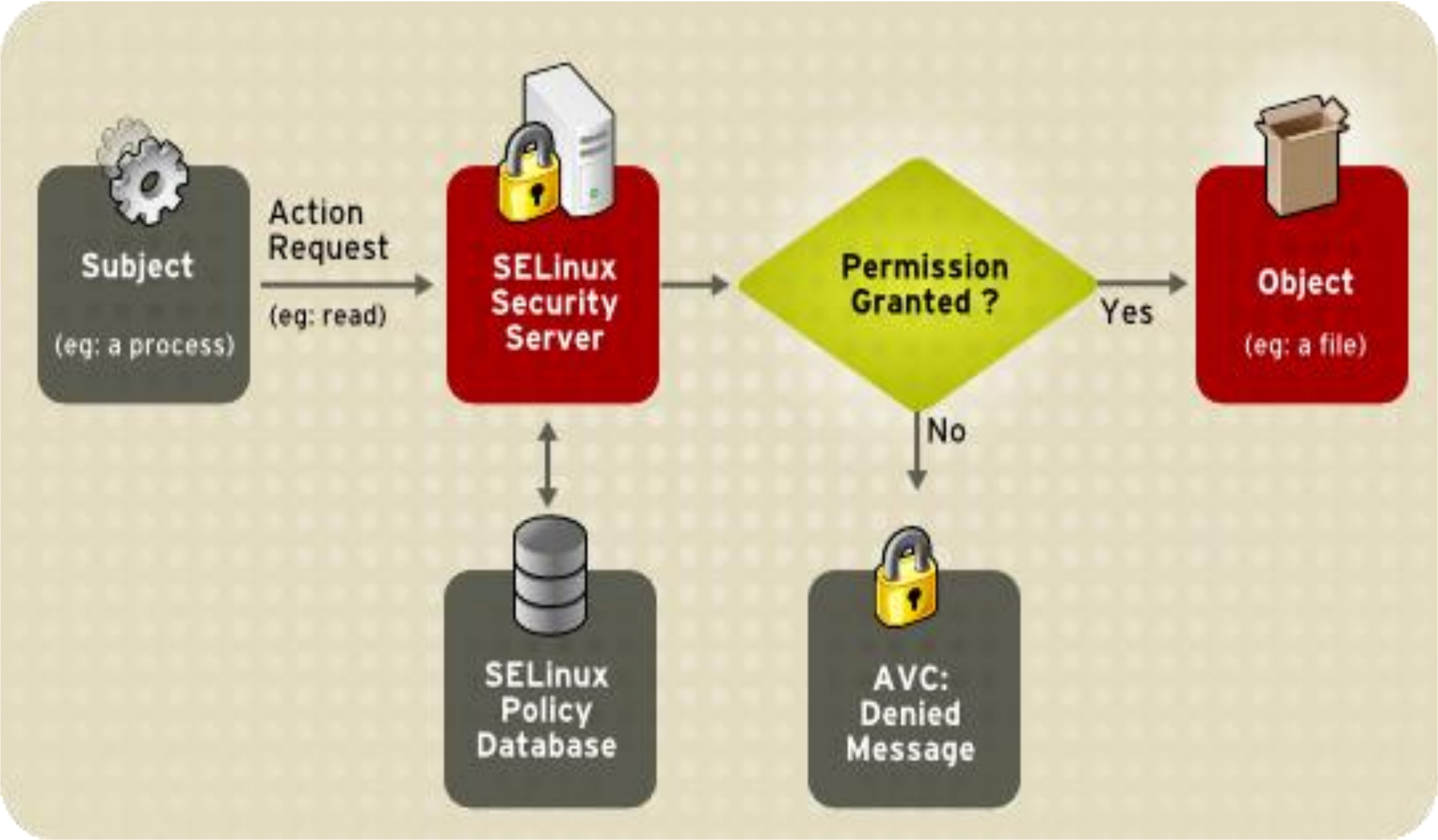
Outline

- Security in Linux
- SELinux
- Grsecurity
- Yocto Project security
- Meta-security
- Meta-selinux

SELinux

- Security enhancement for the Linux kernel
- Developed by NSA
- Policy based architecture
- Part of LSM (Linux Security Modules)
- Aims at military-level security
- Shipped with a large number of Linux distributions

Policy based system



SELinux basic concepts

- Users: different from the one available in the UNIX context because it does not change during a user session
- Roles: a user has one or more roles and are defined based on policies
- Types: primary method to take authorization decisions
- Context: an attribute that determines whether access should be allowed between an object and a process
- Object Classes: represents the category of objects
- Rules: security mechanisms of SELinux, usually states if a type is allowed to perform various actions

Configure SELinux

- Available on most Linux distributions
- sudo apt-get install selinux
- Two available options:
  - Enforcing: most useful one in production
  - Permissive: here policies are not enforced, but denials are logged and used later in the debugging process
- Reboot the system for the changes to take place
- More info here: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/SELinux_Guide/index.html

Outline

- Security in Linux
- SELinux
- Grsecurity
- Yocto Project security
- Meta-security
- Meta-selinux

Grsecurity

- Suite of GPL patches based
- Development started in 2001
- Initially ported a number of security enhancing patches from Openwall Project
- Released for kernel 2.4.1
- Never part of kernel but things started to change lately

Grsecurity benefits

- Configuration-free operations
- Protection against a large variety of address space change bugs
- Includes comprehensive ACL and a number of auditing systems which meet lots of demands
- Able to interact with multiple operating systems and processor architectures

Role-based Access Control

- Formalized in 1992 by David Ferraiolo and Rick Kuhn
- Alternative to DAC and MAC
- Offers least-privilege system
- Only minimum required privileges are offered in order to achieve a task
- Due to this chroot() system call is hardened to prevent privilege escalation

Memory corruption defenses

- Automatic response to brute force exploits
- Hardened BPF JIT against spray attacks
- Hardened userland memory permission
- Random padding between thread stacks
- Prevent direct userland access by kernel
- Industry-leading ASLR
- Bound check on kernel copies to/from userland

Filesystem hardening

- Chroot hardening
- Eliminate side-channel attacks against admin terminals
- Prevent users from tricking Apache into accessing other users files
- Hide processes of other users from the unprivileged users
- Provide Trusted Path Execution

Miscellaneous Protections

- Prevent ptrace-based process snooping
- Prevent dumping unreadable binaries
- Prevent attackers from auto-loading vulnerable kernel modules
- Deny access to overly-permissive IPC objects
- Enforce consistent multithreaded privileges

RBAC security

- Intuitive design
- Automatic full system policy learning
- Automated policy analysis
- Human-readable policies and logs
- Stackable with LSM
- Unconventional features

GCC plugins security

- Prevent integer overflows in size arguments
- Prevent leaking of stack data from previous syscalls
- Add entropy at early boot and runtime
- Randomize kernel structure layout
- Make read-only sensitive kernel structures
- Ensure all kernel function pointers point into the kernel

Grsecurity source code fetching

- wget https://www.kernel.org/pub/linux/kernel/v3.x/linux-3.14.19.tar.gz
- wget https://www.kernel.org/pub/linux/kernel/v3.x/linux-3.14.19.tar.sign
- wget http://grsecurity.net/stable/gradm-3.1-201502222102.tar.gz
- wget http://grsecurity.net/stable/gradm-3.1-201502222102.tar.gz.sig
- wget http://grsecurity.net/stable/grsecurity-3.1-3.14.36-201503182218.patch
- wget http://grsecurity.net/stable/grsecurity-3.1-3.14.36-201503182218.patch.sig

Grsecurity checksum verification

- wget http://grsecurity.net/spender-gpg-key.asc
- sudo gpg --import spender-gpg-key.asc
- sudo gpg --verify gradm-3.1-201502222102.tar.gz.sig
- sudo gpg --verify grsecurity-3.1-3.14.35-201503092203.patch.sig
- gzip -d linux-3.14.19.tar.gz
- sudo gpg --verify linux-3.14.19.tar.sign
- sudo gpg --keyserver hkp://keys.gnupg.net --recv-keys 6092693E
- sudo gpg --verify linux-3.14.19.tar.sign

Grsecurity configuration

- tar xf linux-3.14.19.tar
- cd linux-3.14.19/
- patch -p1 < ../grsecurity-3.1-3.14.35-201503092203.patch
- Skip include/linux/compiler-gcc5.h since it might be missing from your Linux distribution available support
- sudo apt-get install libncurses5-dev
- make menuconfig

Outline

- Security in Linux
- SELinux
- Grsecurity
- Yocto Project security
- Meta-security
- Meta-selinux

Yocto Project security discussion

- Is done inside a specialized mailing list: yocto-security@yoctoproject.org
- Quite a new subject in Yocto Project
- Activity includes identifying the latest and most dangerous security threats(CVEs) and fixing them
- Mostly based on Poky
- More info here: https://wiki.yoctoproject.org/wiki/Security

Outline

- Security in Linux
- SELinux
- Grsecurity
- Yocto Project security
- Meta-security
- Meta-selinux

Meta-security

- Yocto layer which includes tools for securing, hardening and protecting embedded devices
- Maintained by Saul Wold and Armin Kuster
- Can be used together with meta-selinux or other security related layers if needed
- Extending its support is recommended

Supported packages

- Bastille
- Redhat-security
- Pax-utils
- Buck-security
- Libseccomp
- Ckecksecurity
- TOMOYO
- Nikto
- Nmap
- Clamav
- Isic
- Samhain
- Suricata
- Tripwire

TOMOYO

- Appeared in March 2003 and was sponsored by NTT Data Corporation Japan until March 2012
- Another LSM for MAC implementation
- Has an automatic policy configuration mechanism
- After enabling it acts as a watchdog that does not permit processes to use more resources then they declared initially
- Parallel developments also available for this project
    - TOMOYO Linux 1.x: the original source code version
    - TOMOYO Linux 2.x: the mainline source code version
    - AKARI: a TOMOYO 1.x forked version

Redhat-security

- Collection of scripts:
  - find-chroot.sh: scans the whole system for ELF files which call chroot and also include a call to chdir
  - rpm-chksec.sh: it takes a rpm file and checks its content for their compiling flags.
  - find-nodrop-groups.sh: scans the whole system for those programs which change UID or GID without calling setgroups and initgroups calls.
  - find-hidden-exec.sh: scans the system for hidden executables and reports the results back to the user for investigation.
  - selinux-check-devices.sh: checks all the available devices if they are correctly labelled
- They can be simply invoked inside terminal for execution

Pax-utils

- A number of scripts:
  - scanelf: is used for finding pre-information about the ELF structure of the binary.
  - dumpelf: an user-space utility used for dumping the internal ELF structure in the equivalent C structures (debugging or reference purposes).
  - pspax: used for scanning /proc and list various available ELF types and corresponding PaX flags, attributes and filenames.
- Used mostly for ELF files consistency scannings

Other packages(1)

- Samhain: system integrity monitoring and reporting tool
- Tripwire: similar to samhain
- Bastille: hardening tool used for environment securing
- Nmap: network mapper for system administration, network discoveries and security auditing
- Suricata: high-performance IDS/IPS and Security Monitoring engine for the network

Other packages(2)

- ISIC: a suite of utilities for IP Stack Integrity Checking
- Nikto: scanner used for detecting dangerous CGI or web server related files
- Libseccomp: library for abstracting the seccomp kernel syscall filtering mechanism
- Checksecurity: setuid changes detection framework
- ClamAV: UNIX command line anti-virus
- Buck-security: similar to redhat-security

Outline

- Security in Linux
- SELinux
- Grsecurity
- Yocto Project security
- Meta-security
- Meta-selinux

Meta-selinux

- Different from meta-security
- Maintained by: Joe MacDonald, Philip Tricca and Mark Hatle
- Only enables support for one tool (SELinux)
- Also adds support for SELinux possible extensions
- The extensions can also be used for self-contained purposes

SELinux extensions

- Audit: kernel auditing tool, used a number of utilities and libraries for data searching and recording
- Libcap-ng: libcap alternative with simplified POSIX capabilities, analyses and prints application`s capabilities
- Setools: policy analysis tool, includes a number of libraries, graphical tools and command line options
- Swig: Simplified Wrapper and Interface Generator, used for fast prototyping and testing
- Ustr: micro string API for C language, has low overhead

The End