Using SElinux

Is it insane, too much trouble or the only smart thing to do?

Jari Turkia (j-redacted@omniata.com)
Senior Software Engineer

It’s insane!

1. Edit `/etc/default/grub`
2. Add `selinux=0` into `GRUB_CMDLINE_LINUX`
3. Run:
   ```
   grub2-mkconfig --output=/boot/grub2/grub.cfg
   ```
4. Reboot
5. It’s gone:
   ```
   [ ! -e /sys/fs/selinux ] && echo "SElinux deactivated"
   ```

It’s too much trouble

- Too complicated!
- Nobody needs this!

1. Edit `/etc/default/grub`:
2. Add `selinux=0` into `GRUB_CMDLINE_LINUX`
3. ...

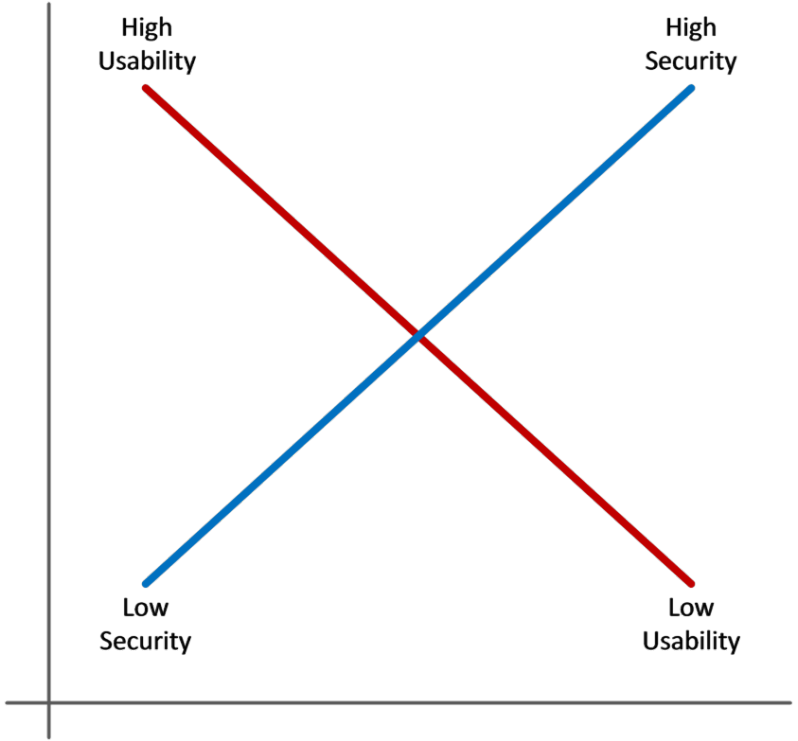

Figure 1: Security and usability tend to be inversely related

SElinux 1

- Security-Enhanced Linux (SELinux) is a Linux kernel security module that provides the mechanism for supporting access control security policies
  - Wikipedia
- SELinux is a mandatory access control system which enables a more fine-grained mechanism where the security administrator defines what a user can do
  - Gentoo wiki

SElinux 2

- Originally created by NSA

- Open source
- index : kernel/git/stable/linux-stable.git https://git.kernel.org/cgit/linux/kernel/git/stable/linux-stable.git/tree/security/selinux?id=refs/tags/v3.16.1

Motivation 1 - Attacks

- Enterprises Are Experiencing a Wide Variety of Web Application Attacks
  - The Enterprise Strategy Group, 2013
- 27%: Application authentication
  25%: Attacks on sensitive information
  25%: Configuration management
  25%: Application authorization
  21%: Session management
  18%: Parameter manipulation
  16%: Auditing/logging
  16%: Exception management
  16%: Input validation

Motivation 2 - NATO CCD COE

- NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)
  - Baltic Cyber Shield 2010
- Jussi Jaakonaho
  - Microsoft Security Bulletin MS03-010 - Important
  - Microsoft thanks jussi jaakonaho for reporting this issue to us and working with us to protect customers.

Motivation 3 - Baltic Cyber Shield

- Task: Protect a “nuclear power plant”
- Attacker: 72 hours of time to investigate and prepare
- Defender: <3 hours of time to prepare
- "Are you sure? This skill level isn't even remotely fair."
  - Doom, on Nightmare
- Result: Defenders win

Motivation 4

- Q: How is that possible!!?
- Number of security upgrades installed: 0
- Take the only thing the attacker wants out of play
- Interactive command shell:
  - By using existing exploit
  - By introducing new piece of software into the system

Demo 1

Backdoor

SElinux explained

- There is a context (aka. domain)
  - in filesystem: files, directories
  - in process space: processes
- Note: context can also be *unconfined*
- Other resources: sockets, ports, etc.
- True power of SElinux:
  policy dictates what can be accessed from given process context

Example: Apache policy

1. Transitions:
    1. `kernel_t` executes a file in the context of `execute init_exec_t`, resulting a process in `init_t`
    2. `init_t` executes a file in the context of `initrc_exec_t`, resulting a process in `initrc_t`
    3. `initrc_t` executes a file in the context of `httpd_exec_t`, resulting a process in `httpd_t`

Demo 2

Backdoor /w default Apache context

Beefing up Apache policy

- Stop using `httpd_exec_t` and create an own policy
- Ready-made tools and examples exist
- Introducing `backdoor_exec_t`

Demo 3

Backdoor /w a more restricted context

Wrap up

- Prepare for your website to be exploited!
- Make the attacker’s life miserable
  - Prevent writing new executable content
  - Think execution permissions
- SElinux can help you with that

Thank you!

Questions?

Helsinki Security Meetup August 20, 2014

Jari Turkia (j-redacted@omniata.com)
Senior Software Engineer