HitachiSoft

2006 SELinux Symposium

Progress of SELinux Policy Editor

Hitachi Software Engineering
The George Washington University
Yuichi Nakamura
ynakam@gwu.edu

Introduction: What is SELinux Policy Editor

HitachiSoft

- The goal: easy SELinux
  - make SELinux as easy as other secure OS(such as AppArmor, LIDS), but can be more secure
- Currently distributed/maintained at
  - http://seedit.sourceforge.net/
  - Talked at last SELinux Symposium
- Composed of simplified policy and its tools
  - Simplified Policy hides detail of SELinux, and s implified policy tools make it much easier
- The most significant is simplified policy

Background: Symplified policy

HitachiSoft

- A policy described by Simplified Policy Description Language(SPDL)
  - Path-name based
  - Reduces number of permissions
    - remove/integrate permission
  - Can describe entire SELinux policy
  - SELinux policy is generated from SPDL
- Example:

SPDL

```
domain httpd_t;
allow /var/www r,s;
```

Types are generated from path name, allows are outputted

Generated Policy

```
type httpd_t, domain;
type var_www_t,file_type;
allow httpd_t var_www_t:file { getattr read ioctl lock };
allow httpd_t var_www_t:lnk_file { getattr read ioctl lock};
.... allow for file related object classes....
```

What's going on now

HitachiSoft

- The version on last symposium
  - worked at only Fedora Core2
  - developed based on old SELinux(as of 2002)

- Need update
  - Security
  - Implementation

Process of security improvement

HitachiSoft

- 1. Review all permissions of new SELinux
  - Wrote document of SELinux permissions(as of Nov 2005)
    - http://seedit.sourceforge.net/doc/access_vectors/
- 2. Reduce number of permission by permission removal
  - Almost done
- 3. Re-design of permission integration
  - File/device permissions
  - Network permissions(not yet)
  - Others(not yet)

Consideration of permission removal

- Permission removal=allow the permission all domains
- All permissions in SELinux(not including user space permissions)
  - 708 permissions!(object class x access vector permissions)
- Criteria:
  - Unused
    - such as file:swapon
  - Related to control DAC and POSIX capability
    - such as capablity:dac_override
      - Because SELinux can cover DAC and POSIX capability
  - Overlapping
    - Example: process:ptrace, capabiliby:sys_ptrace
      - -> remove capability:sys_ptrace
      - sys_ptrace can be controled finer-grained by process:ptrace

Removed 128 permissions (18%)

List is available: http://seedit.sourceforge.net/doc/permission_integrate/

Consideration of file permission

HitachiSoft

- Only 4 permissions in old version
  - s(Stat): Permissions for “ls”
  - r(Read): read file
  - w(Write): write and create,delete files
    - -> allowing too much
  - x(eXecute): execute files

- Optional new +5 permissions
  - “w” is separated
    - o(Overwrite)
    - a(Append)
    - c(Create)
    - e(Erace)
    - t(seTattr)
  - This is cooperation with Okayama University

Device files

HitachiSoft

- Old version
  - All object classes related to file are treated as same

    Ex: domain smbd_t

    allow /var/samba r,w; -> smbd_t is allowed to read and create device under /var/samba
- New version
  - allows for chr_file/blk_file are not generated by default
  - Access to chr_file/blk_file are allowed only directory by allowdev

    Ex: domain smbd_t

    allow /var/samba r,w;

    allowdev -root /dev
  - -> smbd_t can not access devices under /var/samba
  - -> smbd_t can access devices under /dev if it is allowed by “allow /dev/xxxx...”

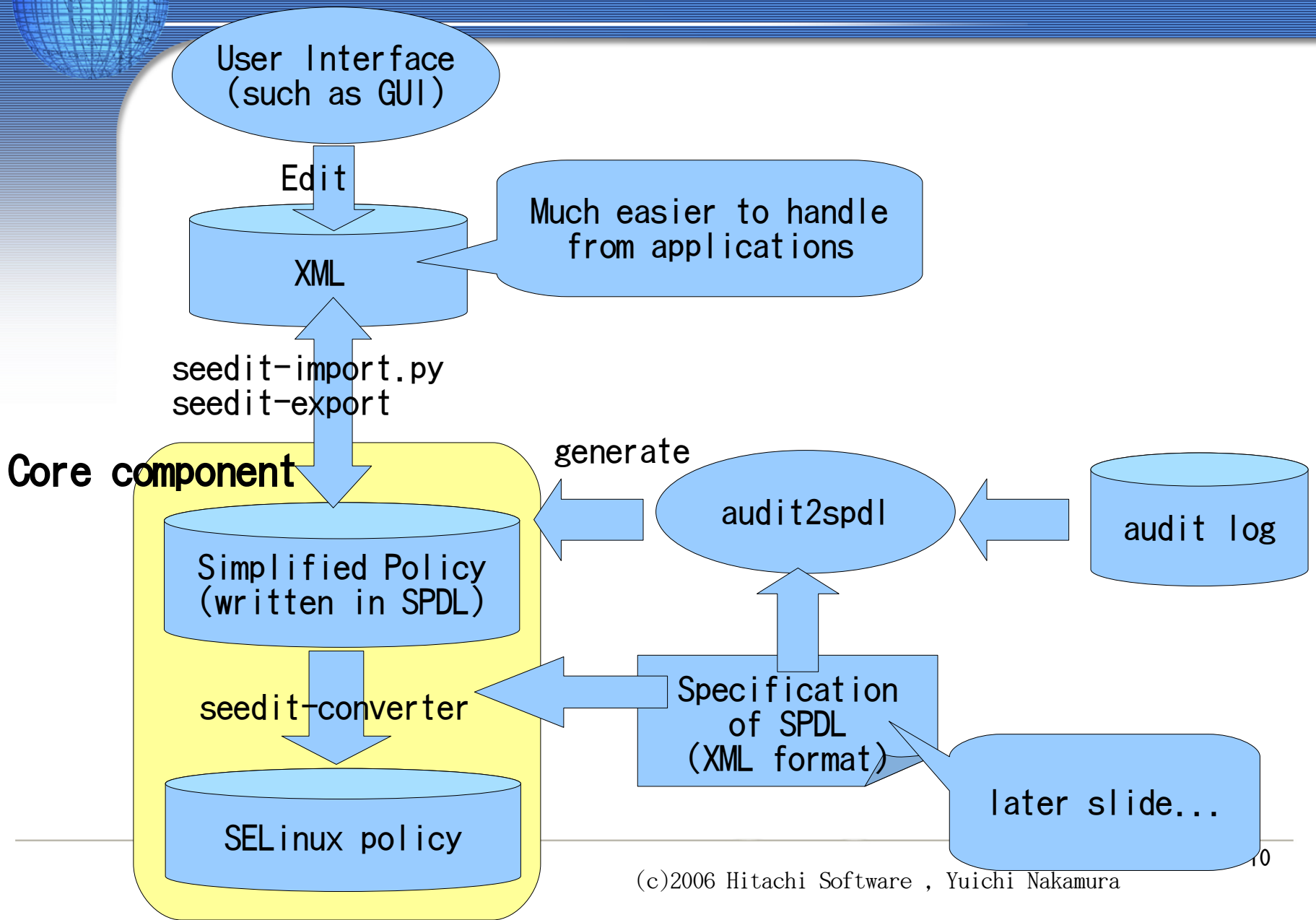
Implementation

HitachiSoft

- Update for latest distros
  - Now works at Fedora Core4, TurboLinux10Server, Asianux2.0
  - -> Released as version 1.2
- New architecture
  - XML support
  - Policy Generation from log(audit2spdl)
  - Will appear as version 1.3.3
- New GUI

New architecture

HitachiSoft



Specification of SPDL

HitachiSoft

Specification of SPDL (XML format)

Integration of permissions are described
(Ex: “r” grants file:read,file:lock etc

- Generation latex document of permission integration
- Macro generation used SPDL->SELinux poilcy conversion
- Used in “audit2spdl” tool
  - audit2spdl
    - convert audit log into SPDL
    - ex:
      - log of “deny avc=read class=file type=” var_www_t”
      - -> generate “allow /var/www r;”
    - Used in translation from SELinux permission to SPDL permission

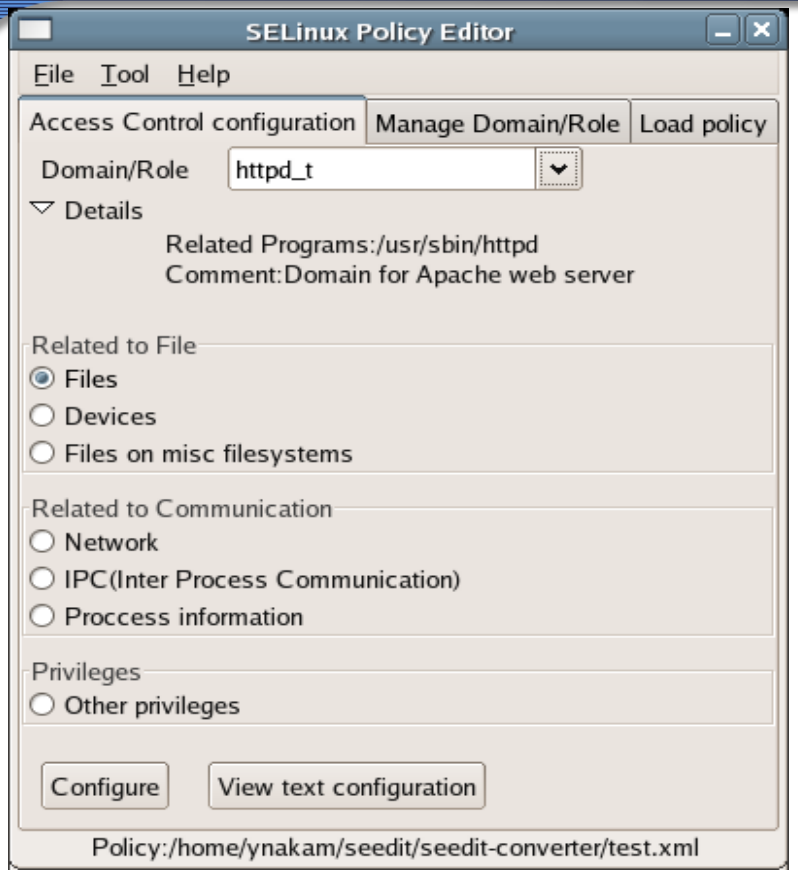
New GUI

HitachiSoft

- Started to develop GUI from scratch.
  - Old GUI(Webmin+perl)can not be maintained(bad coding)
- X window based GUI
  - Using python, Gtk+(pygtk)
  - i18n aware(gettext)
  - logic is separated for reuse
    - for web-based GUI,console based commands, in future:-)
    - Edit XML simplified policy

GUI screen shot

HitachiSoft



- In progress..
  - Much more comfortable to implement than Webmin based(pygtk, python, XML is great!)
  - hopefully will appear around this summer?

Summary

HitachiSoft

- Updated SELinux Policy Editor
  - security
  - new architecuture
- Plan:
  - Release version “2.0” around summer
    - with new GUI
- Other interesting things..
  - More XML
    - To manage many machines
      - XML tree that contains every policy template?
  - Appendable simplified policy
    - It would be easier now by policy module infractructure

Visit http://seedit.sourceforge.net/

Version 1.3.3(or later) will support new features
-> will be announced to NSA's ml

Acknowledgement

HitachiSoft

- Dr. Jonathan Stanton@ The George Washington University
  - Advisor, provided research lab
- Dr. Toshihiro Tabata, Mr. Takuto Yamaguchi @ Okayama University
  - Research about file permissions