Apparmor—Linux内核中的强制访问控制系统

AppArmor

因为最近在研究OJ（oline judge）后台的安全模块的实现，所以一直在研究Linux下沙箱的东西，同时发现了Apparmor可以提供访问控制。

AppArmor(Application Armor)是Linux内核的一个安全模块，AppArmor允许系统管理员将每个程序与一个安全配置文件关联，从而限制程序的功能。简单的说，AppArmor是与SELinux类似的一个访问控制系统，通过它你可以指定程序可以读、写或运行哪些文件，是否可以打开网络端口等。作为对传统Unix的自主访问控制模块的补充，AppArmor提供了强制访问控制机制，它已经被整合到2.6版本的Linux内核中。

目前Ubuntu已自带了Apparmor， 可以在手册中获得相应的资料。文章是从很多英文资料中整理总结出来的，可能会有不准确的地方，请各位见谅。

一、与程序绑定的访问控制

Apparmor提供的访问控制是与程序绑定的：

> AppArmor's unique security model is to bind access control attributes to programs rather than to users.

假设有一个可执行文件的路径为/home/lei/demoexe，如果要用Apparmor对其进行访问控制的话，就要新建一个配置文件（后面我再讲怎么写这个配置文件），文件名为home.lei.demoexe，并把这个配置文件放到Apparmor专门放置配置文件的目录下（/etc/apparmor.d）。所以每一个可执行文件都是与一个配置文件绑定的，因此如果修改demoexe的文件名的话，配置文件将失效。

二、两种工作模式

Apparmor有两种工作模式：enforcement、complain/learning

Enforcement – 在这种模式下，配置文件里列出的限制条件都会得到执行，并且对于违反这些限制条件的程序会进行日志记录。

Complain–在这种模式下，配置文件里的限制条件不会得到执行，Apparmor只是对程序的行为进行记录。例如程序可以写一个在配置文件里注明只读的文件，但Apparmor不会对程序的行为进行限制，只是进行记录。

那既然complain不能限制程序，为什么还需要这种模式呢，因为——如果某个程序的行为不符合其配置文件的限制，可以将其行为记录到系统日志，并且可以根据程序的行为，将日志转换成配置文件。

当然我们可以随时对配置文件进行修改，选择自己需要的模式。

三、访问控制与资源限制等

Apparmor可以对程序进行多方面的限制，这里我只介绍自己用到的。

（1）文件系统的访问控制

Apparmor可以对某一个文件，或者某一个目录下的文件进行访问控制，包括以下几种访问模式：

r	Read mode
w	Write mode (mutually exclusive to a)
a	Append mode (mutually exclusive to w)
k	File locking mode
l	Link mode
linkfile-> *target*	Link pair rule (cannot be combined with other access modes)

可读、可写、可扩展、可链接等（还有可执行x在表中没有列出）……

在配置文件中的写法：

如/tmpr, (表示可对/tmp目录下的文件进行读取)

注意一点，没在配置文件中列出的文件，程序是不能访问的，这有点像白名单。

（2）资源限制

Apparmor可以提供类似系统调用setrlimit一样的方式来限制程序可以使用的资源。要限制资源，可在配置文件中这样写：

```
set rlimit [resource] <= [value],
```

其resource代表某一种资源，value代表某一个值，

要对程序可以使用的虚拟内存做限制时，可以这样写：

set rlimit as<=1M,（可以使用的虚拟内存最大为1M）

注意：Apparmor可以对程序要使用多种资源进行限制（fsize,data,stack,core,rss,as,memlock,msgqueue等），但暂不支持对程序可以使用CPU时间进行限制。（现在OJ一般都对ACMer提交的程序的运行时间有严格的限制，所以要将Apparmor用于OJ后台安全模块，必须自己另外实现对CPU时间的限制。）

（3）访问网络

Apparmor可以程序是否可以访问网络进行限制，在配置文件里的语法是：

network[[domain] [type] [protocol]]

了解网络编程的应该知道domain、type和protocol是什么。

要让程序可以进行所有的网络操作，只需在配置文件中写：

network,

要允许程序使用在IPv4下使用TCP协议，可以这样写：

networkinet tcp,

(4)capability条目

Capability statements are simply the word capability followed by the name of the POSIX.1e capability as defined in the capabilities(7) man page.

在linux的手册页里面有一个capablities列表，apparmor可以限制程序是否可以进行列表里的操作，如：

capabilitysetgid,（允许程序进行setgid操作）

四、配置文件的编写

前面提到，编写完配置文件后，要把文件放到/etc/apparmor.d这个目录下，其实有更方便的方法，直接在命令行里面用：

sudo genprof [filename]

就可以为指定的程序创建一个配置文件，并把它放到该目录。

```
lei@ubuntu:/etc/apparmor.d$ sudo genprof '/home/lei/apparmor-helper/demoexe'
[sudo] password for lei:
Connecting to repository.....

WARNING: Error fetching profiles from the repository:
RPC::XML::Client::send_request: HTTP server error: Method Not Allowed

Writing updated profile for /home/lei/apparmor-helper/demoexe.
Setting /home/lei/apparmor-helper/demoexe to complain mode.

Please start the application to be profiled in
another window and exercise its functionality now.

Once completed, select the "Scan" button below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.

Profiling: /home/lei/apparmor-helper/demoexe

[(S)can system log for SubDomain events] / (F)inish
```

建立的配置文件内容如下：

```
# Last Modified: Fri Feb  120:06:092013

#include      /home/lei/apparmor-helper/demoexe {      #include      }
```

注意，该文件默认使用enforcement模式，要修改模式，只需将配置文件改为：

```
# Last Modified: Fri Feb  120:06:092013

#include      /home/lei/apparmor-helper/demoexe  flags=(complain){      #include      }
```

红字前面的部分是文件的路径，作用是为这个配置文件绑定某个程序。

好，那接下来就可以在配置文件中添加相应的内容，在大括号中加上：

```
    /home/lei/apparmor-helper/data rw,     set rlimit stack<=1M,
```

然后再执行命令：

```
sudo /etc/init.d/apparmor reload
```

就可以重新加载配置文件，使配置文件生效。

```
lei@ubuntu:/etc/apparmor.d$ sudo /etc/init.d/apparmor reload
 * Reloading AppArmor profiles
Skipping profile in /etc/apparmor.d/disable: usr.bin.firefox
                                                                    [ OK ]
```

注意如果配置文件中语法有错误的话会加载失败。

这篇文章只是我在使用apparmor过程中的一点小总结，并不完善，例如配置文件还有很多细节我没提到，有一些工具可以比较方便地管理配置文件我也没提到，大家要研究apparmor的话还是要查阅其他更详细的资料。