Security Enhanced (SE) Android: Bringing Flexible MAC to Android

论文贡献

- 1. 明确并克服在Android中有效使用SELinux的若干挑战
- 2. 完整地将SELinux和中间件MAC整合到Android中
- 3. 具体演示SELinux如何缓解实际的Android漏洞和app漏洞
- 4. 将安全增强功能合并到由AOSP维护的Android平台中

背景

DAC存在问题

- 1. DAC是粗粒度的防护
- 2. DAC无法限制使用root或superuser身份的系统daemon和setuid程序

背景

SELinux优势

- 1. SELinux能够限制系统进程特权的滥用
- 2. SELinux提供了比DAC更强大的机制来隔离和沙盒化Android应用程序
- 3. SELinux提供了集中的策略配置，可以对其进行分析来找出潜在的信息流和特权提升路径

待解决问题

内核

- 1. 文件系统的支持
- 2. 兼容内核子系统和驱动程序

待解决问题

用户空间

- 1. Android除了内核几乎所有东西都与典型的Linux发行版不同。之前将SELinux整合到用户空间的方式不能直接应用到Android中。
- 2. SELinux通常在程序执行时执行自动安全上下文转换。原有的zygote模型并不能指定app的SELinux安全上下文。

待解决问题

策略

- 1. Android有自己独有的用户空间软件栈
- 2. Android的文件系统布局和使用模型与传统Linux不同
- 3. Linux参考策略太大，不适合资源有限的小型设备
- 4. Linux参考策略要求发行商和用户根据情况制定策略，需要用户具有理解或编写策略的能力

系统实现

内核支持

- 文件系统支持
  - 为了提供完整的安全标签功能，论文对yaffs2 getxattr进行修改，并且实现了对在创建新yaffs2文件时自动设置安全标签的支持
- Android子系统支持
  - Binder：定义新的LSM hook，并在binder驱动中调用这些hook
  - Ashmem：ashmem区域由open文件描述符表示并且由Linux的shmem对象支持，现有的SELinux足够提供对读写的基本控制

系统实现

用户空间支持

- 1. Android C库和动态链接器支持
  - SELinux用户空间代码广泛使用Linux扩展属性系统调用获取和设置文件安全性标签，因此必须首先扩展Android的C库实现
  - 在linker添加AT_SECURE，Linux内核提供此标志来通知用户空间是否发生了安全上下文切换
- 2. SELinux库和工具移植
  - 移植核心SELinux用户空间库和工具到Android，libselinux
  - 使libsepol和SELinux policy编译器适配MacOS X
  - 整合SELinux utilities的功能作为init的built-in命令

系统实现

用户空间支持

- 3. 给文件添加安全标签
  - 拓展mkyaffs2image和make_ext4fs这两个Android文件系统镜像生成工具支持文件安全标签的生成
  - 拓展Android recovery控制台和升级程序保证从recovery控制台生成的新文件也带有安全标签
- 4. init程序
  - 扩展了Android的init程序，在启动期间执行init.rc文件中的任何命令之前提早加载SELinux策略，并且扩展了ueventd程序以根据策略标记设备节点

系统实现

用户空间支持

- 5. app安全标签
  - 为了使由zygote进程产生的子进程的安全上下文不同，必须扩展Dalvik VM来为子进程设置SELinux安全上下文
  - 拓展Dalvik VM使得它能给子进程设置SELinux安全上下文在Dalvik VM对子进程进行设置部分插入了一个hook，用于调用libselinux库的一个新接口

系统实现

策略配置

- 1. SELinux策略配置
  - 重新定制Android用户空间软件栈策略配置策略的TE部分来定义系统daemon和app的域配置策略的MLS部分使不同app进程和文件相互隔离采用了在内核层建立一个小而固定策略集的方式

	SE Android	Fedora
Size	71K	4828K
Domains	39	702
Types	182	3197
Allows	1251	96010
Transitions	65	14963
Unconfined	3	61

系统实现

策略配置

- 2. 安全上下文定义：
  - app进程：mac_permissions.xml
  - app数据文件：seapp_contexts
  - 系统文件：file_contexts
  - 系统属性：property_contexts

安全性分析

总结

- SE Android的内核层MAC提供了一种有效的方法来防止应用程序的权限升级和防止应用程序通过内核级接口共享未经授权的数据。同时确保更高级别的安全功能不被绕过和被app篡改。

安全性分析

总结

- SEAndroid威胁：
  - 1. SEAndroid不能解决能通过了策略检查的攻击
  - 2. SEAndroid是一种内核级别的安全机制，不能缓解内核漏洞
  - 3. SEAndroid不能解决来自其他平台组件的威胁，例如能直接访问内存和存储器的系统组件

损耗分析

对镜像大小的影响

- system镜像大小相对增长了0.07%
- recovery镜像大小的增长与boot镜像的类似，增长了3%
- 镜像大小总共0.2%

	AOSP	SE Android	Increase
boot.img	4400K	4552K	+152K
system.img	194072K	194208K	+136K
recovery.img	4900K	5068K	+168K

损耗分析

性能测试

- AnTuTu性能测试
  - AOSP和SEAndroid上都运行了200次
  - 结果表明SEAndroid开销可以忽略

	AOSP		SE Android	
	Mean	**SD**	**Mean**	**SD**
total score	4172.68	148.83	4165.31	188.28
memory	507.05	51.81	514.27	65.42
integer	838.89	57.61	842.95	65.83
float	672.25	61.48	673.68	72.21
score2d	279.85	36.22	273.23	45.52
score3d	1230.67	0.86	1230.46	1.02
sdread	191.110	0.662	191.010	0.748
sdwrite	115.45	5.61	115.15	4.74
database	337.40	22.85	324.55	19.86

损耗分析

性能测试

- Softweg性能测试
  - AOSP和SEAndroid上都运行了200次
  - 结果表明SEAndroid开销可以忽略

	AOSP		SE Android	
	Mean	SD	Mean	SD
Total memory	588.88	68.61	591.71	67.28
Copy memory	535.11	62.35	537.68	61.13
Total CPU	3167.07	149.51	3113.31	138.51
MFLOPS DP	17.61	1.09	17.46	0.98
MFLOPS SP	41.85	5.06	41.22	5.20
MWIPS DP	200.86	8.83	197.16	10.10
MWIPS SP	289.18	19.04	283.73	14.93
VAX MIPS DP	139.03	6.19	136.73	6.62
VAX MIPS SP	191.31	16.08	187.69	15.12
Graphics Scores				
Total score	19.50	0.37	19.62	0.38
Opacity	6.32	0.16	6.37	0.18
Transparent	5.58	0.13	5.62	0.11
Filesystem Scores				
Total Score	236.99	20.88	234.77	20.05
Create files	0.38	0.02	0.44	0.03
Delete files	0.23	0.11	0.25	0.12
Read file	382.54	38.72	375.25	37.58
Write file	100.20	7.90	96.88	7.57
SDcard Scores				
Create files	1.45	0.15	1.62	0.17
Delete files	0.46	0.06	0.49	0.06
Read file	64.73	5.33	63.46	5.21
Write file	33.78	2.54	33.65	2.89

THANKS !