平台安全__技术综述

Mark Shackman

版本 1.2

1 引言

本文档简单介绍了 Symbian 操作系统的增强性平台安全，致力于对 Symbian 操作系统的体系结构受平台安全的影响而产生的变化进行简洁的技术总结。

应该注意到，这里呈现给大家的仅仅是平台安全的综述，所以简洁性是必要的，不涵盖 Symbian 操作系统体系结构中所有应该被考虑的服务、情景等。

2 为什么需要平台安全？

版本 9.x 是 Symbian 操作系统重要的演化版本。它特别适合面向中等规模的手机开发，甚至可以为独立软件开发商出售他们的产品提供更大的机会，并且包含大量新的特征和改进以促进未来高级开放的手机所需要的关键新兴技术的应用。为了全面广泛的支持诸如数字版权管理、设备管理和企业等级数据处理等新功能，Symbian 操作系统的重要的核心部分进行了非常大的改变以支持所必需的概念，例如数据保护，“锁定”或者限制某些 API 的用法。

改进的一个方面就是平台安全性的提升。它是对 Symbian 操作系统现有周边安全模型的演进，能够确保平台的稳定性，更大程度地防抵御恶意程序带来的伤害。平台安全在软件层面上提供两种方式实现上述功能：

2.1 检测

检测对软硬件或数据未经授权的访问企图的能力是任何安全系统明确需要的。

平台安全确保一个应用在使用一个敏感的 API 时，能够有权调用此 API 并使用其提供的功能。

2.2 限制

系统限制程序以不可接受的方式进行操作的能力，也是一个有效的安全系统所必要的组成部分，而不考虑这些操作是否有意。此类操作包括未经授权的硬件访问、企图读写受限的数据等。

在平台安全中，限制功能在本质上是通过下面的方式实现的：赋予执行代码不同层次的信任，以判定其在系统中能做什么，然后强制执行，从而使得程序不能以不受欢迎的方式进行操作。

3 平台安全的概念及术语

下列概念和术语是理解平台安全问题的核心。

3.1 能力

一个能力是一个保护实体。在 Symbian 操作系统中，如果功能（即 API）有必要被保护时，必有一个与之相关的能力，意欲使用此功能的代码必须保证以安全的方式使用对应的 API。

代码需要使用有保护能力的功能时，为了获得使用相应能力的特权，必须通过授权的过程。一旦此过程顺利完成，代码就被认为授权了此能力。授权一个能力可以有效地确信代码足够被信任，可以使用被能力保护的功能。

在手机中，没有用户界面的应用提供大量的功能，称之为服务。在实践中，为了使用敏感的 APIs，服务必需能力。通常，任何服务都有责任要求一个能力访问其相应的 API，以确保一个调用进程有其所必需的能力。Symbian 操作系统 APIs 中仅有 40%有此需要；所有其余的 APIs 不需要调用进程拥有任何能力。

一个应用所需要的能力在其工程定义文件（MMP）中被列出。这个数据也被 Symbian 操作系统本身、Symbian 操作系统的软件安装组件和 Symbian 签名所使用，以检查一个应用应该使用什么功能。

能力可以分为“基本”能力和“系统”能力。为了通过 Symbian 签名的授权，基本能力和用户能力是一致的，并且系统能力又被分为两类，这样就生成了三个能力集合：用户能力、扩展能力和电话制造商许可能力。

3.1.1 用户能力

“用户”能力集适用于被认证的 Symbian 签名应用。这授权使得此集合中的所有能力自动允许使用。所以当用户使用这些应用时从不要求授权。

此能力集合列表请见附录 A

3.1.2 扩展能力

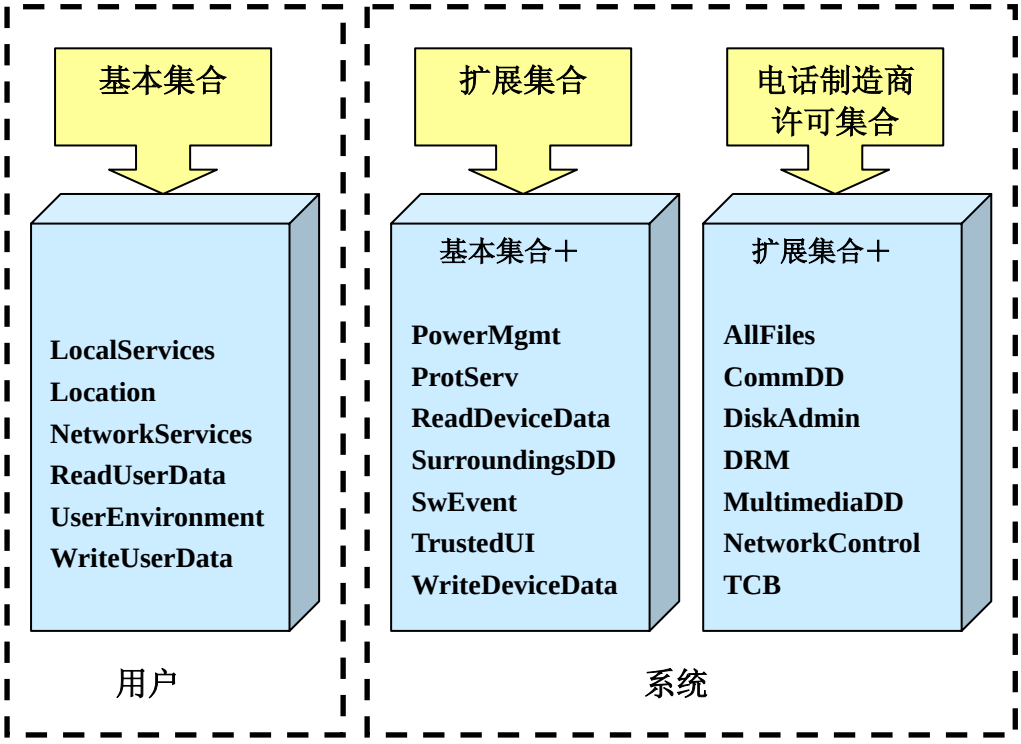
“扩展”能力集适用于使用非用户受保护功能的 Symbian 签名应用，这些功能需要经过额外的测试。这个集合包括来自于用户集的能力，也包括其他的提供更低层次访问系统函数的能力，比如 SwEvent 或 ReadDeviceDate。

此能力集合列表请见附录 A

3.1.3 电话制造商许可能力

电话制造商保留了对诸如 DRM、TCB 和 AllFiles 等最敏感能力的授予权。作为签名过程的部分，需要这些功能的应用必须获得电话制造商的许可。

此能力集合列表请见附录 A



3.2 可授权用户许可

电话制造商可能选择允许用户授权一些选择的能力。这些能力被称为“可授权用户”能力集，并且如果一个能力包括在这个集合内，软件安装工具将提示用户应用程序已经被授予了“blanket 权限”（参看 3.2.1）。如果用户授权被接受，仅需要用户授权的应用没有必要提

交以获得签名。然而应该注意到在此集合中的能力可能根据制造商或设备的不同而不同，因而不应该过于依赖。

3.2.1 blanket 和 single shot 许可

当一个程序企图使用一个能力受限的服务时，两种类型的授权可以允许程序使用这个服务：blanket 和 single shot。

如果授权部门或终端用户赋予程序 blanket 许可，则当此程序被安装时，被赋予这个能力。注意，一旦赋予 blanket 许可，终端用户除了卸载或重装应用否则不能撤销此许可。

少量的 APIs(通常是高层次)对应的能力不能被授权 blanket 许可时（即能力没有列在 MMP 文件中），其可以被 single shot 授权。single shot 许可是一次性授权，在每一次执行操作时，终端用户直接要求许可。single shot 可以提供给签名应用或者未签名应用，其依赖于电话制造商的配置选择。

3.3 标识符

在一个安全坏境中，一个服务需要知晓哪一个程序可以被允许使用它的 API。为了实现这个功能，服务可以维护这些程序的列表，或者像在平台安全模型中它能使用能力的范例。这个模型避免了需要对程序的特定身份的鉴定，因此服务能控制使用它的 APIs，而不必知道谁进行了调用。然而，有时需要识别一个程序，例如，当数据需要绑定到一个特有的程序时。偶尔，能够识别程序的出售者可能也是必要的。为了达到这个目的，定义了两种标识符。

3.3.1 SID(安全标识符)

从 Symbian 操作系统版本 9.x 开始，所有的可执行程序必须包含一个安全标识符，确保其在本地是唯一的。这是一个大部分的开发者不必考虑的执行细节。同时为应用明确的设定一个安全标识符也是可能的，默认情况下，它被设置匹配为总是需要的 UID3 值。

SID 概念帮助平台安全：

- 保护 APIs
- 限制特定的应用使用 APIs
- 当升级内容时，保护手机上的被使用的文件系统区域

如果必要的话，SID 的值可以在程序的 MMP 文件中使用关键字 SECUREID 来定义。为确保一个 SID 的声称拥有者可以被鉴别为签名程序的一部分，标准的 Symbian 操作系统 UID 范围被分为两部分－受保护的范围和未被保护的范围。所有的 UID 来自于这两个范围之一，具体依赖于应用是否要被 Symbian 签名。

3.3.1.1 受保护的范围

如果应用经过 Symbian 签名， UID 将必须从受保护的范围获得。这些 UIDs 的分派是有迹可循的，并且当签名一个应用时，测试机构确认 UID 对于此应用是全局唯一的且属于开发者。

软件安装程序确保未签名的应用不能从受保护的范围获得一个 UID，确保没有 UID 与好几个执行程序有联系（即所有的 UID 在本地是唯一的）。

受保护的范围包括所有的低于 0x7FFFFFFF 的 UID 值，因而也包括所有继承的 UID 的分配值。然而，如果开发者在开发一个版本 9.x 的具有 UID 派生值的应用时，希望此应用未签名，必须获得来自于未受保护的范围的新的 UID。

3.3.1.2 未受保护的范围

UID 的未受保护的范围可以为未签名的应用提供“合作性的“分派。他们不保障全局唯一性，却可以获得受保护的范围的 UID 在运行时刻才有的好处（例如，本地唯一性）。同时，Symbian 操作系统代码、已经存在于话机的“固件”应用和 Symbian 签名的应用可以被排除在受保护的范围以外的未签名应用保护，因而可以阻止他们使用复制的 UID。

3.3.2 VID（开发商标识符）

执行程序可能也包含一个开发商标识符来区别于原始的执行程序。如果一个应用需要一个 VID，它必须被签名。未签名的应用必须使用一个值为 0 的 VID（KnullUid），其为默认值。

VID 允许一个专用服务器仅接受由同一个开发商或一个特定的出售者集合创建的应用对 API 的调用，例如，网络运营商可能发布 APIs，却希望限定他们的使用。

对于受保护的和未被保护的 UID 及 VID 进一步的细节请参照 http://www.symbiansigned.com/app/page/uidfaq

4 平台安全的体系结构

这个部分详细说明了 Symbian 操作系统的体系结构在集成平台安全里所做的变化。

4.1 能力如何影响 API 调用

平台的增强安全性限制使用了在可信计算环境（TCE）的核心模块中的许多 API。希望使用这些 API 的应用必须由合适的能力创建，并且必须被授权以作为值得信任的应用访问这些 API。如果应用是签名的，并且二进制文件所要求的能力与在.SIS 文件头中授权的能力一致，安装程序将授权在.SIS 文件中所有的能力。随后当调用他们受保护的 API 时这些能力被个人的服务检查。

例如，使用 LocalServices 能力的程序能够要求消息服务通过红外发送数据，但是不能发送短消息。

4.2 能力如何影响 DLL

能力仅赋予给程序（即进程）。一个程序（一个.EXE 文件）加载一个库（一个.DLL 文件）的地方，仅如果加载的程序已拥有的所有能力被授权，库才被加载。如果库没有被加载，程序就会失败。程序和库的能力在源代码中（MMP 文件）被分配，并且在编译后不能改变。如果一个已经分配特定能力的进程调用 DLL 内的代码，此 DLL 必须被授权同样（或更多的）的能力，像那些程序调用的 DLL。注意，即使 DLL 没有使用被能力保护的 API，有不同能力的多种进程可能调用此 DLL。因此，为了确保满足所有的调用者的要求，DLL 自己必须包含足够的能力。

例如：

程序 P.EXE 被连接到库 L1.DLL

库 L1.DLL 被连接到库 L0.DLL

情况 1：

P.EXE 具有 Cap1 & Cap2

L1.DLL 具有 Cap1 & Cap3

L0.DLL 具有 Cap1 & Cap2

加载失败，因为 P.EXE 不能加载 L1.DLL (no Cap2)。

情况 2：

P.EXE 具有 Cap1 & Cap2

L1.DLL 具有 Cap1 & Cap2 & Cap3

L0.DLL 具有 Cap1 & Cap2 & Cap3 & Cap4

加载成功，并且新进程被赋予 Cap1 & Cap2.

4.3 软件安装程序

软件安装程序（SWInstall）组件被显著增强，通过安装在话机上的策略文件以提供运行时间安全。它执行能力检查和数据锁定。

4.3.1 可安装（.SIS）文件的验证

软件安装程序检查应用有权力接入它希望使用的能力，从而使一个.SIS 文件生效。它也确保应用被签名且一个认证链来支持可信根。软件安装程序能检查一个授权是否被废除，并且也能如标记根证书作为必选项，确保所有的安装包必须被签名。

软件安装程序比较安装文件要求的能力和根认证授权的能力，计算最大的能力集合，此集合能够授权作为与所有的有效签名相关联的能力集。如果.SIS 文件需要软件安装程序授权之外的能力，配置选项允许终端用户授权额外的能力。如果用户拒绝授权额外的能力，软件安装程序将不安装这一软件。

4.3.2 文件系统数据锁定的确认

软件安装程序确保文件系统的使用和接入是受限的，保护私有数据、分离数据和代码。进一步的细节见下面的 4.5 节。

4.4 API 变化

为了确保平台增强性的安全是易得的且有效地工作，大量的 API 作了变化。全部的细节超出了此文档的范围；他们将以后在 Symbian 开发库中发布。

4.5 数据锁定

平台安全不仅保护 API，而且也提供保护私有数据的便利。文件系统不但有必要的分离代码和数据（阻止执行数据空间中的代码），还必须重新被组织以实施数据分割。通过“锁定”进程到归档系统的特定部分，确保数据的私有性。

现在归档系统有下列结构：

/sys/	受限的系统区域，仅对有 TCB 能力（参见附录）的程序可以访问，可执行文件位于/sys/bin/并仅在此目录运行。
/private/	为所有的程序包含所有的私有数据，位于目录/private/<SID>/内。如果子目录 import/已经存在，软件安装程序可能在任何程序的安装时写数据到这个目录。
/resource/	包含公共数据，但对没有 TCB 能力的程序是只读的。

所有其他的目录是公共的，可以被任何程序读写。这便利了移动媒体的使用。

当安装新的程序或升级现存的程序时，软件安装程序强迫实施这个结构。因为仅有软件安装程序可以改变位于内在驱动的/sys/bin/中的可执行文件，其他的软件都不能篡改此可执行文件。

4.6 可移动媒体

终端用户可能选择在移动媒体安装程序，而不是安装在话机内存上。在这种情况下，平台安全体系结构必须能够确保可执行程序在安装后不能被篡改。

上述功能如下实现：软件安装程序计算并存储（在防篡改的/sys/目录）程序文件的初始哈西值，无论何时运行程序，都要重新计算比较此值。如果两个哈西值不匹配，或者如果内部哈西值不存在，程序则不运行。

4.7 备份与恢复

在平台安全中，文件备份和恢复依据文件类型作不同的实现。

可执行程序与关联的元数据的元素一起备份（包括初始的.SIS文档和包含在这些文档中用于安装文件所需的信息）。这维持了文件的能力，并且在相应的恢复操作期间确保关联的元数据又可以被用以检验恢复执行文件的完整性和数字签名的有效性，这些校验可通过设备上的一个根证书来实现。

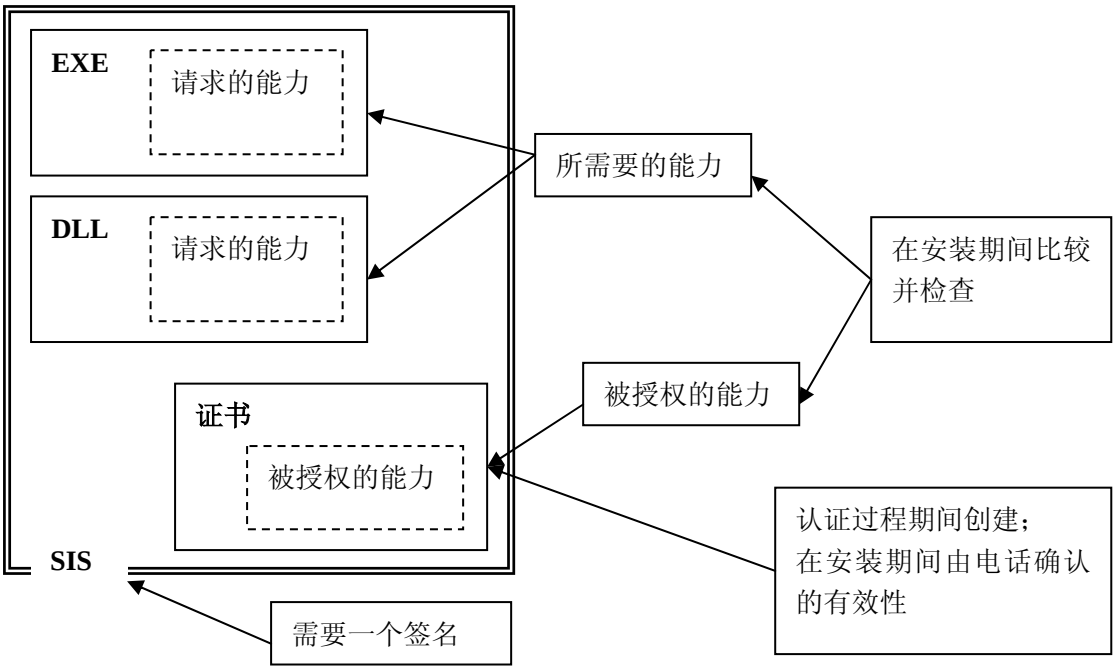
私有数据文件可能因为安装发生改变，因此不再匹配存储在关联的元数据内的哈西值。因而他们与拥有的进程一起被备份和恢复。

大多数公共数据文件使用与前面一样的方法进行备份和恢复。但有一些数据文件除外，比如仅在安装期间写入的目录/resource/。

注意：备份和恢复将在未来的Symbian 操作系统发布版本中完全引入.

5 证书

平台安全使用证书来授权使用能力。为了利用证书对被认证的应用签名，该应用必须通过特定的测试。下面的图标总结了由此证书提供使用的这些能力的机制。



5.1 证书

签名一个应用的进程有两个阶段。首先，应用使用一个鉴别开发者的发布者证书签名。除了检验开发者以外，签名还为提交的应用提供一个哈西值，目的在于防止篡改。

一旦.SIS文件被认证，然后用内容证书签名，内容证书有一个在话机上的Symbian根证书的信任链。此证书使应用在话机不显示警告时被安装，并且对受限的能力访问提供授权。这些过程的更详细的细节请参照http://www.symbiansigned.com/。

如果要识别一个欺诈的签名应用，软件安装程序被配置通过在线的证书状态协议（OCSP）以检查应用的内容证书，并且阻止用此证书签名的软件包的安装。

5.2 开发者证书

开发者可能希望应用提交给Symbian签名之前在相关硬件上测试一个应用。然而，不拥有签名证书，应用不能加载到话机上测试。

除了仅仅依靠模拟器或者一个特定的启用“全能力”的话机进行测试，Symbian将提供“开发”的证书，它将要被绑定到特定的话机（经由IMEI/ESN号）对于特定的话机锁定此证书，并且允许在标准的话机中测试应用。

5.3 获取证书

.SIS文件用Symbian签名的可信证书签名，获得.SIS文件的过程的全部细节请参照http://www.symbiansigned.com/ ，主要的步骤如下：

- 从VeriSign获得一个ACS发布商ID，确定你的公司的身份
- 为你的应用创建.SIS文件
- 用ACS发布商ID密钥为.SIS文件签名，并提交它（被压缩后，与.PKG文件和用户文档一起）给选择的测试机构

- 测试机构确保签名有效，并安装.SIS文件进行测试
- 如果.SIS文件通过检查，撤销ACS发布商ID，并且.SIS文件用与Symbian根相联系的有唯一标识符的内容证书重新签名。（在撤销过程中使用的就是这一标识符。）

6 补充资料

6.1 术语表

下面是在此文档中使用的技术术语和缩写词

术语	定义
Capability	接入受限的 API
DLL	动态链接库
ESN	电子序列号－每一部话机唯一的身份
EXE	可执行文件
IMEI	国际移动设备身份－每一部话机唯一的身份
Malware	恶意软件，被设计以中断或破坏系统
SID	安全标识符
SIS	Symbian 安装文件
SMS	短消息服务
SWInstall	Symbian　操作系统的软件安装组件
可信计算基（TCB）	在 Symbian 操作系统核心的组件
可信计算环境	Symbian 操作系统系统组件，可以接入 TCB
VID	开发商标识符

附录 A－能力列表

基本能力包括：

LocalServices	授权使用本地网络服务，一般不会使用户付费（例蓝牙，红外）
Location	授权使用指定话机位置的数据
NetworkServices	授权使用远程网络服务，一般会使用户付费（例话音呼叫，短消息服务）
ReadUserData	授权读取对话机用户来说是机密的数据
UserEnvironment	授权使用关于用户和他们即时环境的实时机密信息（例音频、视频和生物特征数据）
WriteUserData	授权写入对话机用户来说是机密的数据

ReadUserData和WriteUserData在有必要保护的地方通过保护数据来保护用户的隐私。在下面的图表例子中，用户可能不会关心是否有人看到公共数据，但一定不希望任何恶意软件访问私有数据，或者其余的人偶然地发现它。

数据类型	公共用户数据	私有用户数据
图像	来自于“中立”对象的图像或视频	个人的或者敏感的图像
文本	普通的随手写的文本	私密的记事本备忘录，PIN 号和密码
邮件	垃圾邮件	包含个人和敏感信息的消息
日历	公共假期，运动比赛	体检约定
联系方式	本地库，药剂师，干洗店	竞争企业的老板

以上能力本质上控制访问服务和数据。他们被更普通的水平定义，当安装应用时，一个服务能把它们呈现给话机的终端用户，允许终端用户控制一个应用的动作。

扩展能力包括：

PowerMgmt	授权对未用外设的电源管理，转换话机的待机状态，把话机断电
ProtServ	授权一个服务用一个受保护的名字注册。受保护的名字以“!”开头。内核将阻止没有 ProtServ 能力的服务使用这样的名字，从而阻止受保护的服务被假冒。
ReadDeviceData	授权读取话机私有设置或数据
SurroundingsDD	授权使用外围设备驱动器
SwEvent	授权产生键盘和笔输入事件
TrustedUI	授权创建一个可信 UI 会话，因而在安全 UI 环境中显示对话框
WriteDeviceData	授权写入控制话机行为的私有设置

话机制造商许可的能力包括：

AllFiles	授权读取全部的文件系统；授权写入其它进程的私有目录
CommDD	授权使用通信设备驱动
DiskAdmin	授权使用特定的磁盘管理操作
DRM	授权使用被保护的内容
MultimediaDD	授权使用多媒体设备驱动
NetworkControl	授权使用或修改网络协议控制
TCB	授权写入可执行程序和共享的只读资源

Symbian 操作系统 包含一个可信计算基（TCB），其包括一系列在Symbian 操作系统核心的组件，可以对平台上所有的软硬件不受限制的访问。TCB的能力仅被授权给操作系统内核，文件服务和（在开放性话机上的）软件安装程序。

可信计算基的外围组件是由可信计算环境组成的其它的系统组件。使用TCE(和TCB)中的APIs由扩展能力的拥有者判定。因而TCE内的组件依赖于他们的需求被授权一个扩展能力的子集。

支持开发者数据库http://www.symbian.com/developer/techlib/index.html

如希望得到Symbian开发者数据库中的新的文章，请订阅Symbian社区时事通讯http://www.symbian.com/developer/newsletter.html。

Symbian社区时事通讯每月带给你最新的关于Symbian 操作系统的新闻与资源。