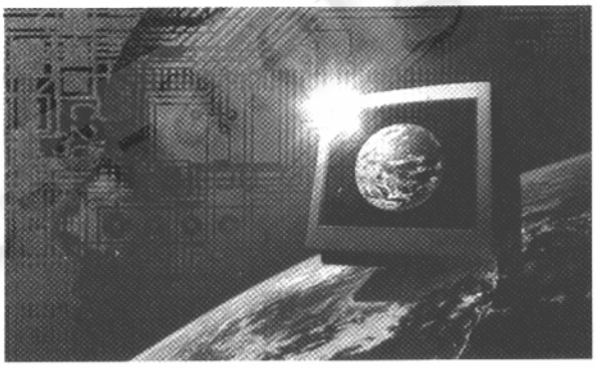
公共安全平台的研究与设计

梁志龙 张志浩（上海同济大学计算中心 200092）

摘要：结合当今网络安全产品无法由用户控制这一现实，本文提出了公共安全平台的概念，并设计了平台的基本模型，为用户提供了一种安全可靠且可以灵活控制的网络安全产品。

关键词：安全平台 应用编程接口 服务编程接口



1 前言

当前出现的网络安全产品有一个共同的特点：无法控制，即产品一旦成型，用户只有全盘接受，没有对产品的控制权。这就带来了一个问题，用户可能只需要产品提供的某些安全功能，或者还需要一些产品没有提供的功能，这是现在网络安全产品都无法解决的问题，而且，网络安全产品提供的功能都是符合一定标准的，而标准是众人皆知的，这也给了用户一种产品不可靠的感觉。怎样才能够解决这个棘手的问题呢？公共安全平台CSP（Common Security Planform）的提出给我们提供了一个很好的答案。使用公共安全平台开发的网络安全产品，用户不仅可以从产品中选择所需的安全功能，还能删除不必要的功能和添加自己定制的安全功能。简单地说，就是产品可以由用户控制。

2 平台定义

所谓公共安全平台，就是这样一个软件，任何中间程序和应用程序都可以使用它来解决所有的安全问题。这里说的中间程序是指为应用程序提供支持的工具包（Tool Kit）或中间件（Middleware）。它是公共的，因为它与上层的应用无关，无论是系统应用，还是网络应用，都能使用它；它又是安全的，因为它可以解决所有的安全问题，无论是业已存在的，还是尚未出现的。

3 平台设计

根据公共安全平台所要达到的目标，其设计应该遵循以下一些原则：

（1）分层（Layered）。所谓分层就是将一个事物在垂直方向上分解成若干相对独立的层次，层与层之间通过一个或多个方面的关系联结在一起。就像OSI要将网络模型划分为七个相互独立的层次一样，分层是将复杂问题简单处理的一种有效的方法。分层有助于简化分析的对象，了解事物内部的联系，帮助我们更清晰地把握事物的本质，更快地解决问题。公共安全平台要想灵活高效地为应用提供服务，就必须将底层的服务和上层的应用接口分开，以简化设计和实现，也使得应用在使用服务的时候不必关心太多的细节问题。

（2）模块化（Modularity）。模块化是指将同一层次的事物在水平方向上划分为相互独立的几部分，每个部分实现一定的功能，各个功能之间的关系将模块联在一起。

（3）灵活性（Flexibility）。公共安全平台要能够根据用户的需求，灵活地选择内部的模块，就好象多协议路由器灵活地解决异构网络之间的路由，ODBC灵活地为数据库应用程序提供与多数据库之间的连接一样。

（4）可扩充性（Extensibility）。因为公共安全平台不仅要能处理已经存在的安全问题，还要能应付将来可以出现的问题，所以，它必须是可扩充的，可以增加新的模块，而不需要改动整个平台。

（5）安全性（Security）。公共安全平台要为应用提供安全服务，其自身必须首先是安全的。这里的安全包括服务请求的合法性鉴别和服务模块的完整性检测等。

4 基本模型

公共安全平台的基本模型如图1所示。它从上而下分为应用层、中间层、接口层和服务层四个层次。

顾名思义，应用层包括所有的应用程序，它使用中间层的工具软件、中间件或直接调用接口层提供的应用编程接口API（Application Programming Interface）来获取平台提供的安全服务。从它看来，平台就像一个黑匣子，它看不到也不必看到平台的内部结构，但可以使用内部功能，这大大简化了应用程序的设计和实现。

中间层主要是指使用接口层提供的API实现的、为上层应用提供支持的工具软件和中间件，这一层的主要目的是进一步简化应用程序的实现。

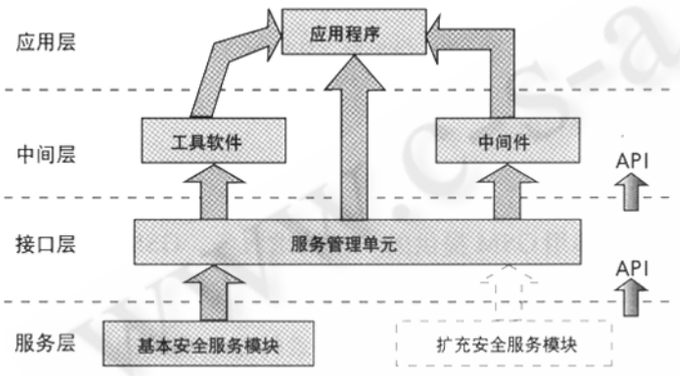


图1 公共安全平台的基本模型示意图

接口层是该平台的控制和管理中心。它向上面两层提供API，并负责将这些API转化为对下层相应服务的请求，使应用程序能够通过API真正获得内部的服务。后面将详细介绍这一层。服务层是公共安全平台的基础，只有在这里，才真正实现了各种各样的安全服务。公共安全平台囊括了所有现今流行的安全标准和技术，如用于数据加密的DES、3DES、RC2、ECB、MD2、MD5、SHA、RSA算法，用于数字签名的DSA、GOST、Ong-Schnor-Shamir、ESIGN算法等等，用于认证的Kerberos鉴别协议和ISO鉴权框架（或ISO X.509协议）等等，以及许多用于安全访问控制的防火墙技术。为了使应用程序能够通过接口层定义的API访问下层的服务，服务层还要向接口层提供对这些服务的访问接口，称为服务编程接口SPI（Service Programming Interface）。

概括地讲，服务层可以分为两个组成部分：基本安全服务模块FSSM(Fundamental Security Service Module)和扩充安全服务模块ESSM（Extended Security Service Module)。FSSM定义了最基本的服务类型，如数据加密、随机数生成、证书库、信任策略、认证计算和数据存储等，这些服务在安装平台时就已经编译好，并经过注册和安装，存放在服务信息库中（关于服务信息库，将在后面解释）。任何时候，接口层都提供使用这些服务的API，应用程序开发商可以直接进行调用。ESSM不属于平台的基本组成部分，但它增加了平台的可扩充能力，所以也必不可少。ESSM包含了FSSM中没有定义的服务类型（一般是那些不常用的服务，如密钥的恢复和生物测定等）以及将来可能增加的服务，这些服务可以以模块的形式编译好，注册和安装后，加到CSP中。但这些服务的提供者必须给出规范的服务编程接口SPI，以便于接口层可以使用这些服务，提供恰当的API给应用程序开发商。一旦被加载，所有的服务地位平等。

前面简单概述了接口层的作用和原理，下面将就其组成作详细的介绍。

接口层由一个服务管理单元SMU（Service Management Unit）组成。SMU单元是CSP的核心，它在应用程序使用服务的过程中起着承上启下的作用。当应用程序通过调用API请求底层服务时，SMU分析这些请求，找到对应的服务模块，并将这些请求转化为对相应SPI的调用，以达到使用服务的目的。应用程序不必知道服务是怎样实现的，也不必知道使用服务的具体步骤，它只要明白应该使用哪一个服务就行了。通俗地讲，就是应用程序不必知道怎么做，而只要知道做什么。如果应用程序需要的服务不存在，会发生什么问题呢？实际上，SMU中维护着一个服务信息库SIB（Service Information Base)，用于保存所有已经注册安装的服务模块、模块提供的服务、服务具有的功能以及这些功能的属性。举个例子，基本加密服务模块可能包含数据加密服务和数字签名服务，加密服务可能提供DES加密、MD5加密等多种功能，而DES加密又具有密钥长度、加密轮数等属性。SIB可以用文件系统来实现，也可以用数据库实现。所有的服务在可以被应用程序使用之前，都必须在SIB中注册登记。每当接收到应用程序的请求，SMU就检查SIB，判断服务是否存在，服务的功能或属性是否一致，任何一个条件不满足，就表示CSP无法提供应用程序需要的服务。为了确定CSP可以提供哪些服务，应用程序开发商在使用服务之前应该先查询一下SIB，因为所有服务在可以使用之前都必须在SIB中登记。下面的描述说明了使用服务的基本步骤：

(1) 在 SIB 中查询特定模块。如果不存在，返回；
(2) 在模块中，查找想要的服务。如果不存在，返回；
(3) 在服务中，查找想要的功能。如果不存在，返回；
(4) 在功能中，查找特定的属性。如果不存在，返回；
(5) 加载该服务模块，并连接到服务；
(6) 调用 API，使用服务提供的功能；
(7) 断开与服务的连接，如果确认没有其他应用使用，要卸载该服务模块，释放内存空间。

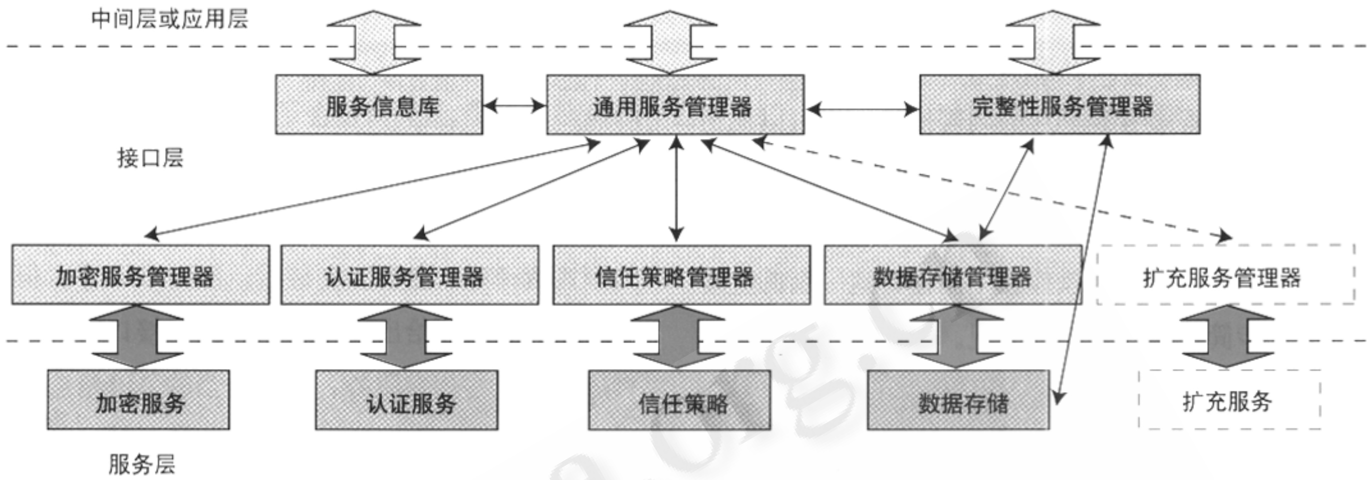


图 2 服务层和接口层详细结构图

SMU 的另一个组成部分是完整性服务管理器 ISM (Integrity Service Manager)，它的主要作用是检查服务模块的完整性，以确保服务模块在注册登记后，没有改动过。每个服务模块在向 SIB 登记安装时，除了给出服务类型、功能、属性等项目外，还必须给出模块的位置和大小，对安全性要求较高的模块可能还要给出使用模块的数字证书。当 SMU 加载服务模块时，它先从 SIB 中获得该模块的位置信息，找到该模块，并重新计算模块大小，与 SIB 保存的大小信息比较，如果两者不一致的话，就表示模块已经被修改，必须重新注册安装。对于签名后的模块，应用程序在调用 API 时，还必须给出认证信息。ISM 中提供了完整性检查的函数，可以被应用程序、SMU 和服务模块调用以检查其他服务或自身的完整性。

也许大家已经注意到，所有的服务模块都交给 SMU 管理，显得过于复杂，而且不清晰。因此，SMU 被分解成若干部分，每个部分称为一个服务模块管理器 SMM (Service Module Manager)，每个 SMM 负责管理一个或几个服务，所有的 SMM 由 SMU 用一个管理器管理，这个管理器就叫做通用服务管理器 GSM (General Service Manager)。服务层和接口层详细结构如图 2 所示。

GSM 向上层应用提供通用服务的编程接口，而不考虑服务的具体内容和操作。应用程序指定服务的详细内容，并调用 GSM 提供的 API 请求服务。GSM 分析这写请求，确定负责目的服务的管理器，它动态地装载该管理器，并将应用程序的服务请求转交给其处理。因为每个管理器只负责一个或几个安全服务，所以这种处理方式既灵活又高效，而且容易理解。

5 结束语

结合如今的网络安全产品无法让用户定制安全功能这一现实，本文提出了公共安全平台的概念，并设计出了基本模型。公共安全平台是一个分层的软件平台，它集成了现在所有的安全服务，并为应用程序提供标准的编程接口，动态的装载这些服务。这些服务以模块的形式注册登记到平台中，提供符合平台规范的编程接口，以使应用程序能通过安全平台使用这些服务。概括起来，公共安全平台的特点就是通用、灵活和高效，使用它实现的安全产品，既安全可靠又自由灵活，可以适应不同用户的需要。■

参考文献

1 Schneier, B. 应用密码学，协议、算法与C源程序，北京机械工业出版社，2000.1。

2 Anand Rajan, Matt Wood, David Bowler. Mechanics of the Common Security Services Manager(CSSM). Intel Architecture Labs, 2000。