7

安全

安全对于今天的网络来说是至关重要的，并且在明天的世界中将变得更加重要。 有了互联网，就有必要不断发明新的程序，以确保不泄露太多要素，如地点、被验证方的名称、消息的语义、私人信息等。 在各种可能的解决方案中，我们将详细讨论两个：安全元素的使用和安全云。 虽然第一种解决办法已经使用了很长一段时间，但第二种是一种新的范式，它正变得越来越普遍。

网络世界中的安全是一种模式，它没有一个简单的解决方案，除了改进现有的算法，其中已经有非常多的算法，以处理新的攻击。 然而，本章讨论了安全世界中的一个新解决方案：安全之云也就是一个云，其目的是确保运营商、公司和公众世界中的数据和网络的安全。 安全云的初始图如图7.1所示。 安全云包含许多用于安全的虚拟机，如身份验证服务器、授权服务器、身份管理服务器，但也包含防火墙，甚至是对应于特定应用程序的非常特殊的防火墙。 我们有时还会找到安全的元素服务器，其中可能包含数千个SIM卡或HSM（硬件安全模块）。

软件网络：虚拟化、SDN、5G与安全、第一版。 盖伊·普约尔。
2015年IS TE有限公司。 由IS TE有限公司和John Wiley&Sons公司出版。

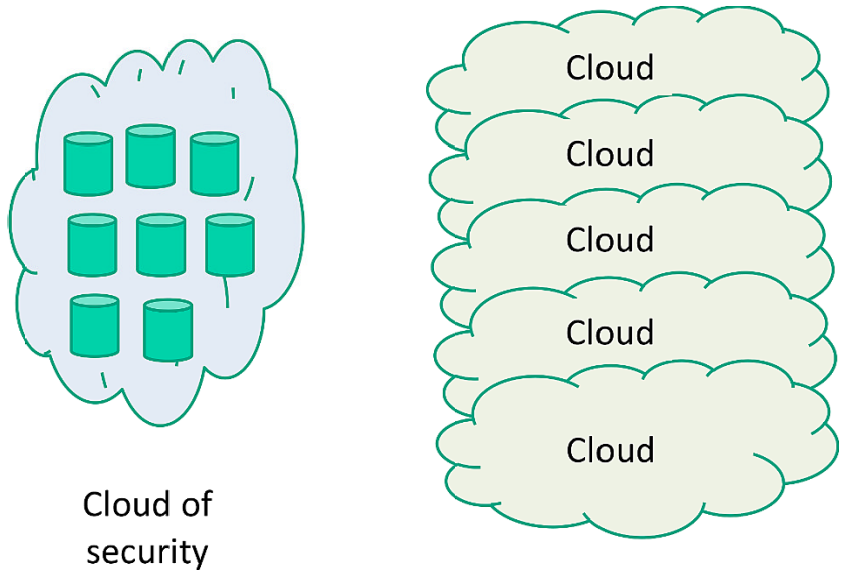

图7.1 *安全之云*

我们现在将从DPI（Deep Packet Inspection）开始，描述安全云中托管的三个服务器示例。DPI的目标是确定在通过网络的流动中传输的应用程序。为了做到这一点，DPI仔细检查流并寻找应用程序签名，这些签名通常可以通过检查应用程序的语法来找到。每个互联网应用程序都有自己的签名。DPI检查一系列位并确定签名。与检查端口号相比，此解决方案的优点是，可以验证通过的所有位，而不仅仅是帧和数据包的头。实际上，攻击者将其攻击封装在一种已知类型的消息中，这种消息很容易通过传统防火墙。然而，在高速流入的流量中检测签名特别复杂，需要顶级硬件，因此也很昂贵。随着将检测流量中的位以找到签名的功能转移到云上，DPI的成本可以大大降低。因此，我们将流量的确定功能转移到一个强大的数据中心。成本通常是传输需要发送到数据中心的流动的成本。市场上有各种各样的解决方案，视需求而定。例如，只有消息头可以被反馈，这大大减少了要检查的流量，但同时也带来了丢失封装位的风险。

第二个例子是防火墙。云计算的世界再一次从根本上改变了这些模块，将它们的软件转移到具有众多优势的数据中心。 第一个优点是每个应用程序都有专门的虚拟防火墙。 通过DPI，我们检测应用程序的性质，并将所涉流程发送到相应的防火墙。

防火墙有处理能力来检查流程的所有细节。 处理所有流程的低功率防火墙被一组非常强大的、专门的防火墙所取代。 缺点与流量有关，这些流量需要发送到专门的防火墙，然后必须返回给公司，尽管有可能的优点是能够隐藏防火墙，以防止对它们的拒绝服务攻击。

第三个例子是一个安全的元素服务器，我们将在本章中看到，它可以用于安全访问敏感服务，如移动支付。 这些安全元素服务器可以包含数千个，甚至数百万个安全元素，如智能卡，这些元素可以通过需要高安全性服务的安全通道到达。

此外，为了纳入云安全，我们可以引用许多服务器，如身份验证服务器、身份管理服务器、编码服务器（尽管这些服务器具有必须非常接近用户的特性）、入侵检测服务器等。

7.1. 安全元件

严格地说，这一章根本不讨论传统的安全问题，而是一个在过去几年逐步建立起来的新一代安全问题。 新一代使用安全元素作为基础。 实际上，高安全性不能仅仅靠软件来满足，软件总是会被内存转储和对密钥位置的良好了解所破坏实际上，高安全性不能简单地通过软件来满足，软件总是可以被内存转储和对密钥位置和其他管理系统的良好了解所破坏。安全元素有不同的形式，但今天最常见的是智能卡。因此，我们首先将智能卡描述为今天的元素。

图7.2展示了一个包含普通计算机所有物理元素的智能卡：微处理器、ROM、RAM、持久存储器、EEPROM、通信总线和输入/输出。在USB密钥中嵌入的新智能卡被释放之前，通信通道代表了一个弱点，但现在已经不是这样了。

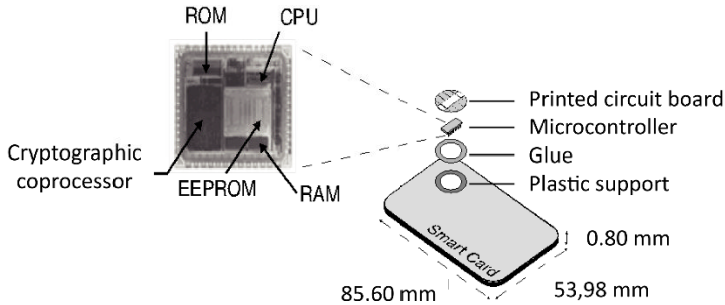

图7.2 *智能卡的硬件结构*

大多数智能卡的核心是一个8位微处理器，以3.5mhz的频率计算能力约为1-3mips（每秒百万条指令）。例如，这种微处理器需要17ms来执行编码算法DES（数据加密标准）。应该注意的是，智能卡处理器的能力正在以这样的速度增长，新的安全卡将能够支持更复杂的算法。

基于具有100万个晶体管的RISC处理器的32位体系结构构成了新一代微处理器，在33mhz下具有约30mips的计算能力。这种微处理器只需要大约50微秒就可以执行DES，300毫秒就可以使用2048位密钥对RSA进行加密。

除了处理器之外，不同类型的内存是微控制器的主要元素。它们用来保存程序和数据。 智能卡微控制器本身就是计算机。它们通常具有1至8kb的RAM、64至256KB的ROM和16至128KB的EEPROM。

长期以来，由于EEPROM不是专门为智能卡设计的，而且其小型化的物理限制已经实现，因此智能卡上可用的EEPROM数量受到限制。闪存使我们能够克服这一限制。因此，我们看到了第一个具有1 Mb持久闪存的智能卡原型的出现。

智能卡的保护主要由操作系统负责。数据访问的物理路由模式仅在卡的个人化之后才可用，就在卡被颁发给用户之前。通过访问控制机制保护的文件逻辑结构访问数据。

智能卡和公钥基础设施（pki）一样，广泛应用于移动电话网络（SIM卡）。这项技术使运营商能够利用他们的网络，同时大大限制了欺诈事件的数量，从而也确保了财务上的可行性。正如许多国家所承认的那样，它也是对电子签名的法律支持。

EAP智能卡直接处理智能卡中的EAP协议。主要应用是EAP-SIM和EAP-TLS。在智能卡上执行EAP-TLS协议有许多优点。首先，身份验证独立于任何给定的软件发布者（如Microsoft）。此外，所提供的安全性肯定优于个人计算机处理器以软件形式执行的EAP-TLS，因为感染PC的间谍软件总是有可能捕获密钥。智能卡的优点是所有的计算都在卡本身中执行，并且智能卡只输出加密流。密钥永远不会离开智能卡。

从理论上讲，EAP卡提供以下四种服务：

– *多重身份管理*：持卡人可以使用多个无线网络。这些网络中的每一个都需要一个身份验证三元组：EAP-ID（在消息EAP-RESPONSE.IDENTITY中传递的值）、EAP-Type（网络支持的身份验证协议的类型）和密码信用-即特定协议（EAP-SIM、EAP-TLS、MS-CHAP-V2等）使用的密钥或参数集。每个三元组由一个名称（标识）标识，可以有多种解释（SSID、帐户用户名、助记符等）；

– *将身份分配给卡*：卡的身份取决于主机网络。在内部，该卡可以具有多个身份，并适应PC和智能卡所连接的网络；

– *处理EAP消息*：由于智能卡具有处理器和存储器，它可以执行代码并处理接收到的EAP消息，并响应发送这些消息；

– *单播密钥的计算*：身份验证会话完成后，EAP隧道可用于传输各种类型的信息，如密钥或配置文件。例如，可以发送会话密钥，并使希望访问无线网络资源的终端可以使用会话密钥。

图7.3说明了身份验证服务器和EAP智能卡之间的身份验证过程。命令流量通过PC上的软件程序-即。首先是EAP软件实体，它一方面简单地将EAP数据包传输到RADIUS服务器，另一方面传输到智能卡-然后是机器的操作系统，它处理与智能卡的接口，最后是无线链路的IEEE802.11接口。

为了提高安全性，还可以在服务器端插入芯片卡，从而使来自认证服务器的EAP-TLS算法也在芯片卡上运行。有了新的芯片卡，可以存储多达1GB，这是可能的记忆日志所需的可追溯性。显然，客户越多，智能卡的数量就越需要增加。

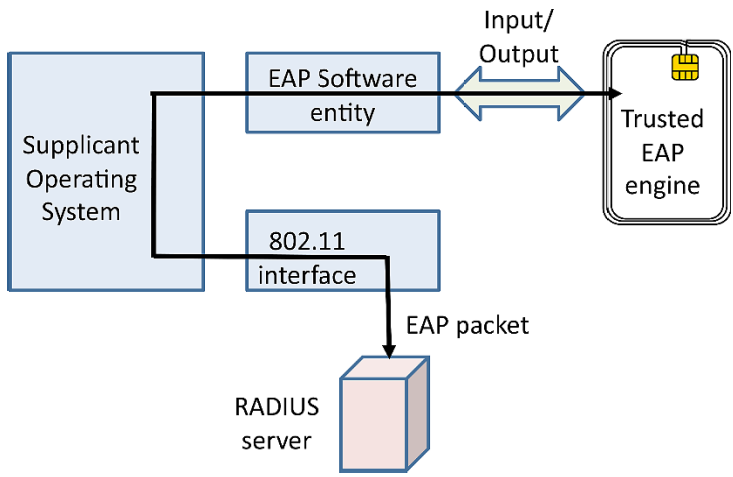

图7.3 使用EAP智能卡的认证程序

\

7.1. 虚拟安全元素

安全元素本身可以通过nor-al虚拟化过程进行虚拟化：使用物理机器并安装一个能够支持多个虚拟智能卡的管理程序。这个过程如图7.4所示，有三个虚拟机。

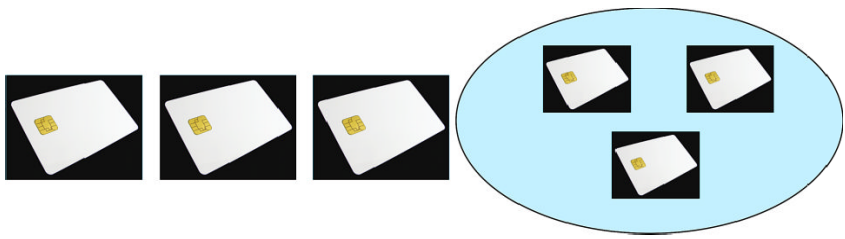

图7.4 *智能卡的虚拟化*

然而，正如我们刚才所描述的，硬件元素是在高度安全的地区必须：

在软件形式下，密钥总是可以被盗。 可能很难黑客攻击某些系统，但总是有风险的，没有人是愿意在高度安全的情况下；

在安全元素中，密钥不能被窃取，或者至少不能从卡本身被窃取。危险在于当钥匙被运送到安全元件时可能会被黑客攻击。

虚拟化的解决方案可以完全不同地看待，例如一组物理卡，其功能被转移到安全云中。如图7.5所示，这些安全元件在卡上被组合在一起；如有必要，这些卡可以以千为单位编号。

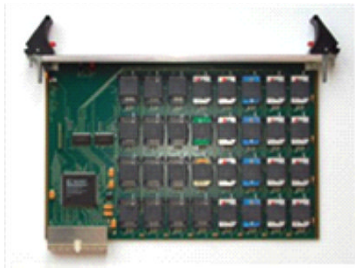

图7.5 *安全元素之云*

新一代安全性的一个范例是，安装一个与需要保护的每个元素相关联的安全元素，不管它是个人、对象、虚拟机还是其他任何东西。要访问Internet，客户机首先需要使用其安全元素对自己进行身份验证，而不管连接的对象是什么。从象征意义上讲，图7.6代表了每一个人——以及每件事物——连接到互联网所需要的东西。

图7.6 *互联网的关键*

显然，符号可以完全不同的形式存在d。 在进一步深入访问安全进程之前，让我们首先研究为环境提供安全性的不同解决方案。

7.2. TEE（可信执行环境）

图7.7显示了三种可能的主要情况，一种是基于软件的安全形式，一种是硬件安全形式，另一种是与TEE（可信执行环境）相关的中间安全形式。

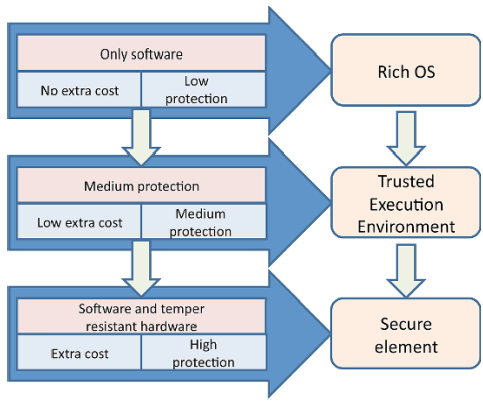

图7.7 *不同的安全解决方案*

正如我们所看到的，软件安全并不昂贵，但总的来说，它并不是很高的水平。对于一个非常好的攻击者来说，检索一个副本并能够找到一定数量的密钥往往是可能的。因此，通常尝试将硬件元素与密钥关联起来。安全尺度的另一端是始终有一个硬件元素来包含密钥或重要的安全元素，这甚至可以方便在安全框内执行算法。一个中介解决方案，需要一定数量的额外解释，今天在市场上是可用的：TEE（可信的执行环境）。

该TEE是智能手机或平板电脑或任何其他移动设备的主处理器内的安全区域，它确保敏感数据在机密环境中存储、处理和保护。TEE提供安全执行被称为“可信应用程序”的授权安全程序的能力意味着它可以通过对数据施加保护、保密性、完整性和访问权限来提供端到端的安全性。

智能手机制造商和芯片制造商已经开发了这种技术的版本，并将它们作为其专有解决方案的一部分内置到他们的设备中。因此，应用程序开发人员需要处理每个应用程序的不同版本的安全创建和评估的复杂性，以便符合每个单独的专有解决方案所建立的不同的规范和安全级别集。

使用TEE的第一个解决方案是在它上附加一个本地安全元件，如智能卡，它在许多移动终端上都有。智能卡用于容纳应用程序的安全部分。困难在于安装几个独立的应用程序，并能够修改它们，删除它们，并添加具有高度安全性的新应用程序。为此，开发了TSM解决方案。我们将在下一节讨论这一解决办法。

7.3. TSM

TSM（Trusted Service Manager）是一个中立的第三方，它用一个安全的元素保护将应用程序（特别是支付账户）下载到智能手机的整个过程的安全。商业和支付需要移动运营商和金融机构之间有一定程度的合作。TSM了解银行和移动电话所采用的安全机制，形成多家金融机构和运营商之间的联系，同时保证消费者信用卡信息的完全安全。

TSM允许通过NFC链路访问安全元素，从而使服务提供商能够分发和远程管理其非接触应用程序。图7.8显示了TSM涉及的不同参与者之间的关系。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：
https://d.book118.com/755120133213011230