二

28 你怎么证明你就是你 - 身份验证和访问控制

AAA

我们先从AAA开始（你一定很迷惑，什么是AAA）英文就是（authentication, authorization, and accounting）- 身份验证，授权和审计。我们先来看一下身份验证部分。

1. 身份验证就是你的用户名和密码。你输入用户名和密码以后，以此来获得进入的权限。没有此处的第二个组件，用户名和密码显得有一点毫无意义那就是 - 授权
2. 授权就是你的特权和访问权限。换句话说，也就是在你登入的系统中，你可以访问哪些软件，你可以访问哪些文件共享，你可以访问哪些计算机和服务器？因此，你的用户名和密码与授权信息是相关联的，从而告诉你可以访问的内容。
3. 从审计的角度来看，这里的最后一个组件很重要，你试想一下，如果出现问题，我们需要对问题进行故障排除，比如员工有没有按照预期的方式行事，我们会去将审查谁在何时何地做了什么；这就是这里的审计部分。

所以我们有了身份验证，那就是我们的用户名和密码；授权，该用户有权访问什么；最后是审计，该用户做了什么，他们什么时候做的？因此，AAA身份验证就是这样。它是用户名，访问权限以及它们所做的记录。有两个组织支持在现代网络中使用的AAA服务器。思科是其中之一。它称为（Terminal Access Controller Accesses-Control System Plus）- “终端访问控制器访问控制系统Plus”或简称为TACACS。

身份验证

我们在这里来对身份验证进行一下深度研究。有本地身份验证，可以在其中对工作站本身进行身份验证。在家用设备中，如果你在家中有一台计算机或笔记本电脑，你最有可能通过无线网络将其连接到Internet，但是你可能没有要连接到服务器。此处的本地身份验证只是用户名和密码，使你可以直接在本地计算机上访问资源。一般会被分为两类-管理员和普通用户。与管理员相比，通常普通用户只是具有查看的权限，而管理员具有在工作站上配置的权限，尤其是对配置文件（这个很好理解，不需要解释呀）。

本地的身份验证只适用于用于本地工作站本身（比如你电脑的登录，输入的用户名和密码只是针对你的笔记本）。域名（Domain）身份验证意味着我们将登录一台要加入某种Domain

的计算机。通常是使用Active Directory，这意味着我们将用户名和密码发送到domain控制器。然后，域控制器会将我们的设备添加到该domain中。当我们将设备连接到域控制器时，我们将使用称为Kerberos的协议来做（该Kerberos协议是开源的），由MIT及其包括IETF的联盟开发。 Kerberos所做的是对通信进行某种加密，以便当我们向服务器发送用户名和密码时，对通信进行加密，这就是这里的组成部分之一。另一个组件是确保发送用户名和密码的计算机是他自己，而不是在该网上其他试图假冒该设备的其他设备。因为这里可以进行某些类型的中间人攻击，即侦听设备和服务器的通信，然后稍后将通信重播回服务器，以欺骗服务器。Kerberos是服务器和客户端验证其身份的一种方式。除此之外，它还会加密该通信，以允许该用户名和密码成功到达服务器，对其进行验证，以查看是否允许该设备加入domain。

当你需要使用域身份验证时，或者是你早上准备开始工作了，打开你的电脑，输入用户名和密码来登录。这将与域控制器进行核对，以验证你是谁，并允许你登录并访问设备上的应用程序。现在，假设你在会计部门工作，并且需要使用一些会计软件比如QuickBook，并且这个软件的依赖位于我们数据中心中的服务器。这里的问题是，在大型公司，你每天都会使用很多不同的程序。你可能有一个内部网站和电邮。你可能会使用特定的专业软件，例如刚才提到的Quickbook，你可能还会使用某些绘图软件等等。可能需要使用许多很多软件（大公司就是有钱，全是买license）。这些软件中的大多数都将具有某种身份验证系统，要确保只有你才能使用该软件，该软件会阻止那些很熟练的程序员或其他工种，但是不是会计的人。这就是术业有专攻，你不是会计，不要动我的软件。因此，我们一般会使用一种叫做LDAP的东西。现在，LDAP已内置到Microsoft Server系统（特别是Active Directory）中，它允许我们执行的操作是允许我们将用户名和密码发送到我们的比如会计软件。然后，这个软件服务器会说“嘿，Active Directory”，该用户是否有权使用这个软件？如果是的话，说明此用户已被授权，然后该用户就可以登录到这个会计软件。

以上的例子其实很接近于所谓的单点登录（现在单点登录很火呀）。单点登录是一个很重要的概念，因为这意味着我只需要知道一个用户名和密码。这就和你的个人生活有一点不同，比如在我的个人生活中，我需要我的Gmail帐户密码，我的netflix的帐户密码，我的Facebook帐户密码，我的HBO账户，我的银行账户等等。对于所有不同的系统，我都需要所有不同的用户名和密码（你可以一个密码走天下，但是会不安全），并且没有一种很好的方法将它们统一在一起。 Facebook和Google对其单点登录产品进行了一些尝试，但是效果不是那么好。可是当我们在企业中使用时，效果就不一样了。用户只需要知道一个用户名和密码，就会感到非常满意。此外，它还提供了无与伦比的安全性，因为你不再被迫去创建许多密码，并且还需要记住许多不同的用户名和密码的组合。

你想一下这里是不是有一个小问题，那就是假设用户名和密码遭到泄露，是不是意味着拥有该用户名和密码的任何人都可以将设备加入网络中的domain，这样会不会危险。因此，我们可以采取的预防措施之一是向网络上的设备颁发证书。在设备联机时可以通过将证书的一部分发送到域控制器来验证它是否属于这个domain（我喜欢用英文单词在这里，中文的翻译总感觉有一点点变扭）。域控制器可能说，是的，此设备在我们的网络上有效，是自己

人，放进来把。这比仅使用用户名和密码来使设备加入Active Directory域要好一些，因为现在Active Directory域控制器必须专门为我们要加入domain的设备颁发证书。因此，我们使用证书和一些凭据在此处登录。这将防止有人携带自己的设备并将其加入domain。这就好比什么呢？比如说天地会的密码是”天王盖地虎，宝塔镇河妖“，是不是每一个知道这个口号的人都是自己人呢？不一定吧。你只要偷听到了就会知道，但是你有一个证书，上面陪着你的照片，这样是不是就不好蒙混过关了（可能有同学会说这样还是有漏洞，不要抬扛呀，任何软件和方案都有安全问题，只要你钻研，都能攻克，只是简单和难得区别）。我们通常会为无线设备使用基于证书的身份验证。这也确实非常有效。

日志和审核

在AAA中，最后一个就是审核，日志是属于审核的一部分。我们需要记录所有的traffic，这使我们可以在将来审核这部分。美国有一个法律那就是关于美国健康法的一部分是，医疗记录系统的用户不得查看不在其直接护理下的任何患者的健康信息。比如你在医院工作，发现蔡x坤是你的病人，你有接触病历软件的权限，你可能想了解阿坤怎么了。可能是出于好奇。可能希望将该信息出售给某家机构来引起轰动。所以，如果让你来设计这个审核来防止这种情况发生，你怎么做呢？设计目的是使我们能够准确的记录谁在何时何地做了什么；然后出现问题的时候，可以审核然后说，那个人这样做是对的吗？

多因素身份验证

我前面应该有提到过这个，我们现在来细谈一下多因素身份验证。现在是我们有史以来第一次能够真正实现多因素身份验证的年代。尽管仍然存在很多挑战，但比以前要好很多很多。多因素身份验证，这个想法是收集有关你的东西，与你有关的东西。因此，我们在这里需要做的一件事情是，你知道的事情，你拥有的一些东西，你是谁，你在哪，你在做什么。让我们看一下其中的例子。所以你知道的事情在这里可以是你的用户名。自定义ID一般会是你的电邮地址，因为用户名通常是你的用户名，而电邮地址一般都是公开的。所以，公司不希望你的用户名成为唯一的标准，这就是为什么我们还需要添加密码。因此，你拥有或者说知道用户名和密码，这就是我们对用户名和密码的单因素身份验证。这是我们知道的东西。我们可以通过添加我们拥有的东西来增强它。我们使用了一些我们知道的东西，例如用户名密码，我们还可以添加一些我们有的东西，比如钥匙卡，钥匙扣，某种类型的数字生成器，甚至可以是我们的智能手机。因此，我们在这里所要做的就是输入用户名和密码，然后可能还要刷智能卡。在银行工作的同学可能会知道，员工会得到一些小的安全身份证，这是一个随机生成数字的小设备。因此，每隔30秒左右会弹出一个新号码，然后你将使用该号码以及用户名和密码来在系统中进行身份验证。因为生成的数字有些随机，很难预测。我们也可以使用智能手机来做同样的事情。还记得我前面提到的一个App（Authenticator）。当我们要登录到系统时，我们可以请求我们的代码登录。然后，我们登录到系统中，可以输入我们的用户名，密码，然后还有就是这个App里的一个数字。这里的想法是你的用户名和密码就是你所知道的。如果有人出于某种原因得到了这些密码，也许你写下了你的用户名和密码，然

后又有人从你那里偷了密码，则可以使用第三种身份验证方式。

因此，窃取你信息的人将无法登录，除非他们有此第三因素。我们可以在这里使用的另一种东西就是你自己。这可能很简单，例如指纹，脸部扫描，视网膜扫描，手掌扫描。通常，这将是某种生物特征识别，而你很难复制给其他人。因此，也许你会再次输入用户名，密码和指纹。智能手机使用指纹读取器。有时，指纹读取器仅用作身份验证的一种形式。这有点危险，因为如果有人可以访问我的指纹并能够复制它，那么他们实际上可以在我的手机上进行身份验证。但是手机上还有其他应用程序需要更多，并且还需要用户名，密码和指纹才能进入。这里的另一个因素是你所在的地方。我马上想到的一个例子就是这项技术，我知道苹果称之为HomeKit。你可以做的就是在你要为自己做某事的地方使用它，比如你在自己的家中，你可以使用智能手机打开锁。这里是不需要用户名和密码的。从字面上看，它将只是在你所处的某个地方，你所拥有的某个事物以及你是谁。可以你你在家附近，拥有你的智能手机，并将指纹放在智能手机上。然后，这三件事加在一起就可以解锁你的房门。因此，在某个地方，您可以将自己拥有的东西和自己所有的东西结合起来使用，例如做一些事情，例如打开房屋的门，或者在回家后打开室内的灯。

上一页 下一页