目录

简介

在开放式网络计算环境，工作站不可能委托正确地识别其用户到网络服务。Kerberos提供一备选方法，藉以可信的第三方验证服务用于验证用户的标识。本文给予Kerberos验证模型的概述如实现为MIT的项目athena。它描述客户端、服务器和Kerberos用于的协议达到验证。它也描述要求的数据库的管理和复制。Kerberos视图如看到由用户、程序员和管理员描述。最后，目前使用Kerberos用

户认证Kerberos的作用在更大athena图片与应用列表一起给。我们描述Kerberos认证的新增内容到Sun网络文件系统作为集成的Kerberos一案例研究与现有应用程序。

Kerberos 作者

- Jennifer G. Steiner，项目athena，麻省理工学院，剑桥， MA 02139， steiner@ATHENA.MIT.EDU
- Clifford Neuman，计算机科学系， FR-35， University of Washington，西雅图， WA 98195， bcn@CS.WASHINGTON.EDU。在设计和初始实施相位Kerberos期间， Clifford Neuman是项目ATHENA职员的成员。
- Jeffrey I. Schiller，项目athena，麻省理工学院，剑桥， MA 02139， jis@ATHENA.MIT.EDU

Kerberos 简介

本文给Kerberos概述， Miller设计的认证系统和Neuman。对于开放式网络计算环境，和描述我们的体验使用它在MIT的项目athena。在关于动机的部分，我们解释新证书型号为什么为开放式网络是需要的，并且什么其需求是。什么是Kerberos ？区分列表Kerberos软件的组件并且描述他们如何在提供呼应验证服务。在Kerberos Names部分，我们描述Kerberos命名方案。

Kerberos如何工作存在Kerberos认证构建模块-票和验证器。这导致两身份验证协议的讨论：一个用户的最初的验证Kerberos的(类似于登陆)和一个潜在的用户和网络服务的一潜在的制作商的相互验证的协议。

Kerberos要求信息数据库关于其客户端的;Kerberos Database部分描述数据库、其管理和协议其修改的。从Outside Looking In部分的Kerberos描述Kerberos建立接口给其用户、应用程序程序员和管理员。在更大的图片部分，我们如何描述项目Athena Kerbero适应到Athena环境的其余。我们也描述不同kerberos验证域的交互作用或者领域;在我们的情况，关系在运行在MIT的实验室的项目Athena Kerbero和Kerberos之间计算机科学的。

在问题和公开问题部分，我们提及未解决的待解决的问题和的问题。最后一部分给予Kerberos的当前状态在项目athena。在附录，我们详细描述Kerberos如何应用对网络文件服务验证希望获得访问到远程文件系统的用户。

Kerberos 概念

在本文中我们使用可能是模棱两可的，新建对读者的术语，或者不同地在别处使用。在我们之下陈述我们的使用那些期限。

用户，客户端，服务器？由用户，我们含义使用一程序或服务的人。客户端也使用某事，但是不一定是人;它可以是程序。通常网络应用程序包括两部分;在一计算机运行并且请求远程服务的一个程序和另一个程序在远程计算机的运行和进行该服务。我们称那些应用程序的客户端和服务器端，分别。通常，客户端代表用户将联系服务器。

使用Kerberos系统，假如是用户或网络服务器的每个实体，是在一感觉客户端，因为使用Kerberos服务。因此与其它服务的客户端区分Kerberos客户端，我们使用期限负责人指示这样实体。注意Kerberos主管可以是用户或服务器。(我们描述命名Kerberos主管在后面的章节。)

服务与服务器？我们使用服务，一些操作抽象说明执行。进行那些操作的进程呼叫服务器。到时，可能有几个服务器(通常运行在不同的机器)执行指定服务。例如，在阿西纳有在的一BSD UNIX远

程登录命令服务器运行我们的每一台分时机器。

密钥，专用密钥， Password? Kerberos用途专用密钥加密。每位Kerberos主管仅分配大量，其专用密钥，已知到首席的那和Kerberos。一旦用户，专用密钥是单向功能的结果应用对用户密码。我们使用密钥作为速记专用密钥。

*凭证？*不幸地，此词有Sun网络文件系统和Kerberos系统的一个特殊含义。我们明确地陈述我们是否含义NFS凭证或Kerberos证书，否则用语用于正常英文感觉。

*万事达和从？*运行在超过一计算机的Kerberos认证软件是可能的。然而，只总是有Kerberos数据库的一明确复制。计算机安置的此数据库呼叫主机器或者主控。其他机器可能拥有Kerberos数据库的只读复制，并且这些呼叫从属。

开发 Kerberos 的动机

在一个非联网的个人电脑环境，资源和信息可以由物理的保护保护PC。在分时计算环境，操作系统保护从互相的用户并且控制资源。为了确定什么每个用户能读或修改，识别每个用户分时系统是必要的。这是实现的，当用户登录。

在要求服务从许多独立的计算机的用户中网络，有三个途径一能采取到访问控制：一什么都不能执行，取决于在用户登陆防止未经授权的访问的计算机;一个人能要求主机证明其标识，但是委托主机的词至于谁用户是;或者一个人能要求用户证明每项要求的服务的他/她的身份。

在所有机器在严格的控制下的一个已关闭环境，一个能使用第一方法。当组织控制通信所有的主机对网络，这是一合理的方法。

在更多开放环境，一个也许选择性地委托仅那些主机在组织控制下。在这种情况下，必须要求每台主机证明其标识。rlogin和rsh程序使用此方法。在那些协议，验证由检查连接被建立了的互联网地址完成。

在Athena环境，我们一定能满足从不在组织控制下的主机的请求。用户有他们的工作站完全控制：他们能重新启动他们，提出他们独立，甚至启动他们自己磁带。同样地，必须采取第三方法;用户必须证明每项所需的服务的他/她的身份。服务器必须也证明其标识。物理巩固运行网络服务器的主机是不满足的;在别处某人在网络可能化妆象指定服务器。

我们的环境在识别机制设置几个需求。首先，它一定安全。避免它一定是足够困难潜在攻击者没找到认证机制是最弱的链路。观看网络的某人不应该能得到必要的信息扮演另一个用户。其次，它一定可靠。对许多服务的访问将取决于验证服务。如果它不可靠，服务系统整体上不会是。第三，它应该透明。理论上来讲，用户不应该知道发生的验证。最后，它应该可扩展。许多系统能与阿西纳主机联络。不是所有这些将支持我们的机制，但是软件不应该中断，如果他们。

Kerberos是满足上述要求的我们的工作结果。当用户走上到工作站时他们登陆。只要用户能告诉，此最初的识别是满足证明他们的标识到所有所需的网络网络服务系统处于登录会话的。Kerberos安全依靠在几个验证服务器的安全性，但是不用户登录，亦不在终端服务器安全将使用的系统。认证服务器适当地提供一已认证的用户方式证明他/她的身份到在间网络分散的服务器。

验证是一安全在网络环境中的一个标准构件。如果，例如，服务器肯定认识客户端的标识，是否能决定提供服务，是否应该给用户特殊权限，应该接收服务的账单，等等。换句话说，授权和核算机制可以被建立在Kerberos提供，造成对孤立PC或分时系统的等同的安全的验证顶部。

什么是 Kerberos？

Kerberos是根据型号的可信的第三方验证服务提交由Needham及Schroeder。委托，也就是说其客户端中的每一个认为Kerberos的判断至于其其他客户端中的每一的标识个是准确的。时间戳(代表当前日期和时间)的大量在重播的检测被添加到原始模型帮助。当消息窃取网络和被再发出的以后时，重播发生。关于重播更多完整说明和验证其他问题，请参阅Voydock和肯特。

Kerberos 起什么作用？

Kerberos保持其客户端和他们的专用密钥数据库。专用密钥是属于的大量仅已知对Kerberos和客户端。在案件中客户端是用户，它是加密密码。要求验证的网络服务向Kerberos登记，象希望的客户端使用那些服务。专用密钥协商在注册。

由于Kerberos认识这些专用密钥，它能创建说服一个客户端的消息别的确实是谁声称是。Kerberos也生成临时专用密钥，呼叫会话密钥，给对两个客户端和没人。会话密钥可以用于加密在双方之间的消息。

Kerberos提供三个明显的级别防护。应用程序程序员根据应用程序的需求确定哪些是适当的。例如，一些应用程序要求只真实性设立在网络连接的开始，并且能假设，从指定网络地址的进一步消息起源于已验证当事人。我们验证的网络文件系统使用此安全级别。

其他应用程序要求每个消息的验证，但是不关心是否透露消息的内容。这些， Kerberos提供安全消息。私人留言提供高水平安全，每个消息不仅验证，而且加密。Kerberos服务器使用私人留言，例如，发送在网络的密码。

Kerberos 软件组件

Athena实施包括几个模块：

- Kerberos应用程序库
- 加密库
- 数据库程序库
- 数据库管理程序
- 管理服务器
- 身份认证服务器：
- db复制软件
- 用户程序
- 应用程序

Kerberos应用程序库为应用程序客户端和应用服务器提供一个接口。它包含，除了别的以外，创建的或读的认证请求的惯例和创建的安全或私人留言惯例。

在Kerberos的加密根据DES，数据加密标准。加密库实现那些惯例。加密几个方法带有，在速度和安全之间的交换。呼叫传播CBC模式，也提供对DES密码块链(CBC)模式的一分机。在CBC中，错误通过密码器的当前块仅被传播，而在PCBC，错误被传播在消息中。这使全部消息无用，如果错误出现，而不是部分的它。加密库是独立的模块，并且可能用其他DES实施或一个不同的加密库替换。

另一个可替换的模块是数据库管理系统。数据库程序库的目前的Athena实施使用ndbm，虽然最初使用了Ingres。能使用其他数据库管理库。

Kerberos数据库需要是直接的;记录为每首席保持，包含负责人的名称、专用密钥和有效期，与一些管理信息一起。(有效期是日期，在后条目不再有效。它通常设置为几年到在注册的未来。)

其他用户信息，例如真名，电话号码，等等，由另一个服务器保存， Hesiod nameserver。这样，敏感信息，即密码，可以由Kerberos处理，相当使用高安全性测量;当Hesiod保存的非敏感的信息涉及不同地时;它可以，例如，是发送的未加密在网络。

Kerberos服务器使用数据库程序库，象管理的数据库工具。

管理服务器(或KDBM服务器)提供一个读写网络接口给数据库。程序的客户端在网络的所有计算机可能运行。服务器端，然而，在安置Kerberos数据库的计算机必须运作为了做对数据库的变动。

认证服务器(或Kerberos服务器)，另一方面，执行在Kerberos数据库的只读操作，即，会话密钥的负责人和生成的验证。因为此服务器不修改Kerberos数据库，在安置Kerberos主数据库的只读复制的计算机可能运行。

数据库复制软件管理Kerberos数据库的复制。有数据库的复制在几台不同的机器的，有认证服务器运行的复制的在每计算机的是可能的。这些从属机器中的每一台接收Kerberos数据库的更新从主机器的在给定时间间隔。

最后，有登陆对Kerberos，更改Kerberos密码和显示或者毁坏的Kerberos票最终用户程序(票稍后解释)。

Kerberos 名称

一部分的验证实体命名它。验证进程是验证客户端是在请求命名的那个。名称包括什么？在Kerberos，用户和服务器被命名。就认证服务器而言，他们是等同的。名称包括主名、实例和领域，被表示为name.instance@realm。

主名是用户或服务的名称。实例用于在主名的变化中区分。对于用户，实例可能需要特殊权限，例如“根”或“admin”实例。对于在Athena环境的服务，实例通常是服务器运行计算机的名称。例如，rlogin服务有在不同的主机的不同的实例：rlogin.priam是在主机指定PRIAM的远程登录命令服务器。Kerberos票只是有效对于单个指定服务器。同样地，独立的票要求获得访问到同一服务的不同的实例。领域是维护身份验证数据一个管理实体的名称。例如，不同的机构可能其中每一个有他们自己的Kerberos计算机，安置一个不同的数据库。他们有不同的Kerberos领域。(领域进一步在Interactionwith讨论其他Kerberi。)

Kerberos 工作原理

此部分描述Kerberos认证协议。如上所述， Kerberos验证模型根据Needham及Schroeder密钥分配协议。当必须设立用户请求服务，他/她的身份。要执行此，票被提交到服务器，与认证一起票最初发出到用户，未窃取。有三个相位对验证通过Kerberos。在第一阶段，用户获取使用的凭证请求对其他服务的访问。在第二阶段，一特定服务的用户请求验证。在最终阶段，用户提交那些凭证到终端服务器。

Kerberos 证书

有用于Kerberos验证模型的两种证件类型：票和证明人。两个根据专用密钥加密，使用不同的密钥，但是他们加密。票用于安全地通过票发出在认证服务器和终端服务器之间人的标识。票也通过能使用确保的信息，使用票的人是发出的同一个人。验证器包含，当比较那在票证明的其他信息，当前票的客户端是票发出的同样一个。

票是有效对于单个服务器和单个客户端。它包含服务器的名称，客户端的名称，客户端的互联网地

址，时间戳、寿命和随机会话密钥。此信息加密使用票将使用服务器的密钥。一旦票发出，可能由已命名客户端多次用于获得访问到指定服务器，直到票到期。注意，因为票在服务器的密钥加密，允许用户通过票到服务器，而不必担心用户是安全的正在修改票。

不同于票，可能一次只使用验证器。新的，每次客户端要使用服务，必须生成。因为客户端能构件验证器，这不提出一问题。验证器包含客户端、工作站IP地址和当前工作站时间的名称。验证器在是票的一部分的会话密钥加密。

得到最初的Kerberos票证

当用户走上到工作站，只有信息一件能证明他/她的身份：用户密码。初始交换用认证服务器设计最小化机会密码将减弱，当同时不允许用户正确验证她/他自己，不用该密码时知识。登录流程看来给用户是相同的象登陆对分时系统。在幕后，虽则，它相当不同的。

提示用户输入她/他的用户名。一旦它被输入了，请求发送到包含用户名和特别服务的名称的认证服务器叫作票授权服务。

认证服务器检查知道关于客户端。如果那样，它生成以后将使用在客户端和票据许可服务器之间的随机会话密钥。它然后创建包含客户端名、票据许可服务器名称，当前时间、一个寿命票的，客户端IP地址和创建的随机会话密钥的票据许可服务器的一张票。这是所有已加密在密钥仅已知对票据许可服务器和认证服务器。

认证服务器与随机会话密钥和一些其他信息一起的复制然后送回票，到客户端。此仅答复在客户端的专用密钥加密，已知对Kerberos和客户端，从用户密码派生。

一旦答复由客户端接收，用户为她/他的密码询问。密码转换对DES密钥并且用于解密从认证服务器的答复。票和会话密钥，与某些另一信息一起，存储以后使用，并且用户密码和DES密钥从内存清除。

一旦交换完成，工作站拥有能使用证明其赋予票据的票据的寿命的用户标识的信息。只要在工作站的软件以前未被窜改，将允许别人扮演在票的寿命的之外用户的信息不存在。

请求Kerberos服务

暂时地，请让我们假装用户已经有所需的服务器的一张票。为了获得访问到服务器，应用程序建立验证器包含客户端名和IP地址的和当前时间。验证器在接收与服务器的票的会话密钥然后加密。客户端与到单个应用有些定义的服务器的票一起然后发送验证器。

一旦验证器和票由服务器接收，服务器解密票，使用在票包括的会话密钥解密验证器，在票的信息与那比较在请求接收的验证器、IP地址和当前时间。如果一切配比，允许请求继续。

假设，时钟同步对在几分钟内。如果在请求的时间在将来是太更的或过去，服务器对待请求作为尝试重赛先前的请求。服务器也允许记录所有通过与有效的时间戳的请求。为了进一步阻止重放攻击，请求接收与同一张票和时间戳象已经接收的一个可以丢弃。

最后，如果客户端指定它希望服务器证明其标识，服务器加一到时间戳在验证器发送的客户端，加密在会话密钥的结果，并且送回结果到客户端。

在此交换结束时，服务器肯定，根据Kerberos，客户端是谁说是。如果相互验证出现，客户端也被说服服务器是地道的。而且，客户端和服务器共享没人认识的密钥，和能安全假设，在该密钥加密的一个相当新近的消息产生与另一个当事人。

得到Kerberos服务器执照

收回票只是有效对于单个服务器。同样地，获取客户端要使用的每服务的一张独立的票是必要的。单个服务器的票可以从票授权服务获取。因为票授权服务是本身服务，它利用在前面部分描述的服务访问协议。

当程序要求已经不是请求的票时，发送请求到票据许可服务器。请求与赋予票据的票据一起包含票是请求的服务器，和验证器的名称被构件正如前面部分所描述。

票据许可服务器如上所述然后检查验证器和赋予票据的票据。如果有效，票据许可服务器生成将使用的新的随机会话密钥在客户端和新的服务器之间。它然后构件包含客户端名、服务器名、当前时间、生成的客户端IP地址和个新会话密钥的新的服务器的一张票。新的票的寿命是剩余寿命和服务的默认的最低赋予票据的票据的。

票据许可服务器与会话密钥和其他信息一起然后送回票，到客户端。这时，然而，回复在是赋予票据的票据的一部分的会话密钥加密。这样，那里是没有需要对于用户再输入她/他的密码。

Kerberos 数据库

至此点，讨论操作要求对Kerberos数据库的我们只读访问。这些操作由验证服务执行，在两台重要和从属机器能运作。

在此部分，我们讨论要求对数据库的写访问的操作。这些操作由管理服务执行，呼叫Kerbero数据库管理服务(KDBM)。当前实施规定变动可能只做对Kerberos主数据库;从属复制只读。所以，KDBM服务器在Kerberos主机可能只运行。

注意，而验证能仍然出现(在从属)，管理请求不可能被服务，如果主机器发生故障。在我们的体验，因为管理请求是不常见的，这未提交一问题。

KDBM处理从用户的请求更改他们的密码。此程序客户端，发送请求对在网络的KDBM，是Kpasswd程序。KDBM也接受从Kerberos管理员的请求，可能添加负责人到数据库，以及更改现有主管的密码。管理程序的客户端，也发送请求对在网络的KDBM，是kadmin程序。

KDBM 服务器

KDBM服务器接受请求添加负责人对数据库或更改现有主管的密码。此服务是唯一因为票授权服务不会发行它的票。反而，必须使用验证服务(使用得到赋予票据的票据)的同一服务。此的目的将要求用户输入密码。如果这没那么是，则，如果用户离开她/他的工作站未看管，路人可能走和更改她/他的他们的密码，应该防止的事。同样，如果管理员离开她/他的工作站无防守，路人可能更改在系统的所有密码。

当KDBM服务器收到请求时，通过比较更改的请求方的已验证主体名称授权它对请求的目标的主体名称的。如果他们是相同的，请求允许。如果他们不是相同的， KDBM服务器参见访问控制表(存储在重要的Kerberos系统的一个文件)。如果请求人的主体名称在此文件被找到，请求允许，否则拒绝。

按照惯例，与NULL实例(默认实例)的名称在访问控制表文件没出现;反而，使用管理实例。所以，为了用户能变为Kerberos的管理员必须创建和添加该用户名的一个管理实例到访问控制表。此规则允许管理员使用一个不同的密码Kerberos管理she/he然后会使用正常登录。

对KDBM程序的所有请求，允许或拒绝，是否被记录。

kadmin 与 kpasswd 程序

Kerberos的管理员使用kadmin程序添加负责人对数据库或者更改现有主管密码。当他们调用kadmin程序时，管理员要求输入他们的管理实例名称的密码。此密码用于拿来KDBM服务器的一张票。

使用Kpasswd程序，用户可能更改他们的Kerberos密码。当他们调用程序时，他们要求输入他们的旧密码。此密码用于拿来KDBM服务器的一张票。

Kerberos 数据库复制

每个Kerberos领域有一台Kerberos主机，安置身份验证数据库的主拷贝。在别处是可能的(虽然不必要)有其他，数据库的只读复制在从属机器的在系统。优点有为复制是那些通常援引的数据库的多个副本：更加高性能和更加好的性能。如果主机器发生故障，验证在其中一台可能仍然达到从属机器。能力执行在任何一个的验证几台机器减少瓶颈的可能性在主机器。

保留数据库的多个副本引入数据一致性问题。我们发现非常简单方法为交易足够了与不一致。主数据库被转存每个小时。数据库发送，全文，到从属机器，然后更新他们自己的数据库。在主主机的一个程序，呼叫kprop，发送更新对对等体程序，呼叫kpropd，运行在其中每一台从属机器。第一kprop发送将发送新的数据库的校验和。校验和在Kerberos主数据库数据库密钥加密，两台主控和从Kerberos机器拥有。数据在对kpropd的网络然后转接在从属计算机。从属传播服务器计算接收数据的校验和，并且，如果匹配主控发送的校验和，最新信息用于更新从属的数据库。

在Kerberos数据库的所以所有密码在主数据库数据库密钥加密，从主控通过的信息到在网络的从对窃听者不是有用。然而，重要的是从主主机的仅信息由从属接受，并且窜改数据检测，因而校验和。

Kerberos 简介

此部分描述Kerberos从实用的观点，首先如看到由用户，然后从应用程序程序员的观点，和终于，通过Kerberos管理员的任务。

用户眼中的 Kerberos

如果所有进展顺利，用户几乎不注意Kerberos存在。作为登录过程一部分，在我们的UNIX实施，赋予票据的票据从Kerberos获取。更改用户的Kerberos密码是密码程序的一部分。当用户注销时，并且Kerberos票自动地毁坏。

如果用户的登录会话比赋予票据的票据(当前8个小时)的寿命持续长，用户将注意Kerberos的在线状态，因为，当下次一Kerberos验证的应用程序被执行，将发生故障。它的Kerberos票超时。那时，用户能运行kinit程序获取票据许可服务器的一张新的票。和，当登陆时，必须提供密码为了获得它。执行klist命令的用户出于求知欲可能对所有票惊奇哪些静静地获取代表她/他的服务的哪些要求Kerberos认证。

从程序员的观点看 Kerberos

写入Kerberos应用程序的程序员已经经常添加验证到包括客户端和服务器端的一现有的网络应用程序。我们称此进程“Kerberizing”程序。Kerberizing通常介入进行呼叫到Kerberos库为了执行验证在服务的初始请求。它可能也介入呼叫到DES库加密随后发送在应用程序客户端和应用服务器之间的

消息和数据。

最常用的库功能是在客户端的在服务器端的krb_mk_req和krb_rd_req。krb_mk_req惯例采取作为参数名称、目标服务器的实例和领域，将是请求的和可能发送的数据的校验和。客户端然后传送在网络的krb_mk_req呼叫返回的信息对应用程序的服务器端。当服务器收到此消息时，做一呼叫对库例行程序krb_rd_req。惯例返回关于发送方的宣称的标识的真实性的一个判断。

如果应用程序要求在客户端和服务器之间的该发送的消息请是秘密的，则库呼叫可以被做到krb_mk_priv (krb_rd_priv)加密(在两边现在共享的会话密钥的解密)消息。

Kerberos 管理员的工作

Kerberos管理员的工作开始与运行程序初始化数据库。必须运行另一个程序注册在数据库的重要负责人，例如与管理实例的Kerberos管理员的名称。必须开始Kerberos认证服务器和管理服务器。如果有从属数据库，管理员必须安排程序传播数据库更新从主控到从属周期地开始。

在这些初始步骤采取了后，使用kadmin程序，管理员操作在网络的数据库。通过该程序，新建的负责人可以被添加，并且密码可以更改。

特别是，当一个新的Kerberos应用程序被添加到系统时， Kerberos管理员必须采取一些个步骤获得它工作。在数据库必须注册服务器，并且分配专用密钥(通常这是一自动地生成的随机的密钥)。然后，在服务器设备的一个文件必须从数据库解压缩和安装一些数据(包括服务器密钥)。默认文件是/etc/srvtab。服务器呼叫的krb_rd_req库例行程序(请参阅前面部分)使用信息文件解密在服务器的专用密钥加密的发送的消息。当密码被键入在终端验证用户， /etc/srvtab文件验证服务器。

Kerberos管理员必须也保证Kerberos机器物理的安全和也是明智维护主数据库的备份。

Kerberos 的广阔前景

在此部分，我们如何描述Kerberos适应到Athena环境，包括其使用由其他网络服务和应用程序，并且如何与远程Kerberos领域呼应。关于Athena环境的更多完整说明，请参阅G.W. Treese。

在其他网络服务中使用 Kerberos

几个网络应用程序修改了使用Kerberos。使用Kerberos， rlogin和rsh命令首先设法验证。有有效Kerberos票的一个用户能rlogin对另一阿西纳计算机，而不必设置.rhosts文件。如果Kerberos认证发生故障，程序后退在授权他们的通常方法，在这种情况下， .rhosts文件。

我们修改邮政协议使用Kerberos验证希望从“邮局获取他们的电子邮件的用户”。消息发送程序，呼叫Zephyr，是最近开发在阿西纳，并且使用Kerberos验证。

报名参加的新用户程序，呼叫寄存器，使用服务管理系统(SMS)和Kerberos。从SMS，它确定想成为的新建的阿西纳用户输入的信息，例如名称和MIT标识号码，是否有效。它然后检查与Kerberos发现请求的用户名是否是唯一。如果所有进展顺利，一个新的条目被做对Kerberos数据库，包含用户名和密码。

对于使用的详细讨论Kerberos获取Sun的网络文件系统，请参考附录。

与其它 Kerberi 的交互

预计不同的管理组织将要使用Kerberos用户认证。也预计在许多情况下，一个组织的用户在别的将要使用服务。Kerberos支持多个管理域。名称的规格在Kerberos的包括呼叫领域的字段。此字段包含内用户将验证管理域的名称在。

服务在单个领域通常注册，并且只接受该领域的一个认证服务器发出的凭证。用户在单个领域(本地范围)通常注册，但是可能的为了她/他能获取另一领域发出的凭证(远程领域)，依赖本地范围提供的验证。凭证有效在远程领域指示用户最初验证的领域。在远程领域的服务是否能选择根据安全要求的度和在最初验证用户的领域的信任级别尊敬那些凭证。

为了执行交叉领域验证，是必要的每个对的管理员领域选择密钥将共享在他们的领域之间。本地范围的一个用户能然后请求从本地验证服务器的赋予票据的票据在远程领域的票据许可服务器的。当使用时该票，远程票据许可服务器认为请求不是从其自己的领域，并且使用以前被交换的密钥解密赋予票据的票据。它然后发行票，通常会，除了客户端的领域字段包含客户端最初验证领域的名称。

此方法能被扩展允许一通过直到到达领域的一系列的领域验证与所需的服务。为了执行此，虽然，记录采取的整个路径是必要的和用户验证最初的领域不仅的名称。在这种情况下，由服务器知道的所有是A说B说C说用户是令人讨厌者。此语句可能只委托大家沿路径是否也委托。

Kerberos 问题与未解决的问题

有用Kerberos认证机制关联的一定数量的问题和公开问题。在问题中请是如何决定票的正确寿命，如何允许代理和如何保证工作站完整性。

票寿命问题是选择在安全和便利之间的适当的折衷问题。如果票的寿命长，则，如果票和其相关的会话密钥窃取或被误置，他们可以用于长时间。如果用户忘记注销公共工作站，这样信息可以窃取。或者，如果用户在允许多个用户的系统验证，有根源的访问的另一个用户也许能找到信息必要使用窃取的票。关于给票一个短的寿命的问题，然而，是，当超时时，用户将必须获取要求用户再输入密码的新的。

开放问题是代理问题。已认证的用户如何能允许服务器获取代表她/他的其他网络服务？这是重要的示例是将获得访问到已保护文件直接地从文件服务的使用服务。此问题另一示例是什么我们称认证转发。如果用户登录工作站并且登录到远程主机，是好的，如果用户访问同样服务联机本地，当运行在远程主机时的一个程序。什么做此困难是用户也许不委托远程主机，因而认证转发在所有的情况下不是理想。我们目前没有一解决方案对此问题。

另一是重要在Athena环境的问题和一个，是如何保证软件运行的完整性在工作站的。这非常不是在私有工作站的一问题，因为使用它的用户掌握它。在公共工作站，然而，某人也许到来了和已经修改登录程序保存用户密码。唯一的解决方案当前可用在我们的环境将使困难为了人能修改在公共工作站的软件运行。一更加好的解决方案要求用户的密钥从未留下用户知道可以是委托的系统。这可能执行的一种方式是，如果用户拥有了一智能卡能够执行在认证协议要求的加密。

Kerberos 状态

Kerberos原型版本进入在九月的制作1986年。从一月1987年， Kerberos是验证其5,000个用户、650个工作站和65个服务器项目athena的唯一的手段。另外， Kerberos在.rhosts文件位置当前使用控制访问在数雅典娜的分时系统。

Kerberos 致谢

Kerberos由Steve Miller和Clifford Neuman最初设计有建议的从Jeff Schiller和Jerry Saltzer。自那时起，许多其他人参与了项目。在他们中是Jim Aspnes、Bob Baldwin、John Barba、Richard Basch、Jim Bloom、Bill Bryant、Mark Colan、Rob French、Dan Geer、John Kohl、John Kubiatowicz、Bob McKie、Brian Murphy、John Ostlund Ken Raeburn、Chris Reed、Jon Rochlis、Mike Shanzer、Bill Sommerfeld、Ted T'so、Win Treese和Stan Zanarotti。

我们是感恩的对Dan Geer、Kathy Lieben、Josh Lubarr、Ken Raeburn、Jerry Saltzer、Ed Steiner、建议改善本文更加早期的草稿的Robbert van Renesse和Win Treese。

Jedlinsky、J.T.科尔和W.E.佐默费尔特， “Zephyr通知系统”，在Usenix会议文集(Winter， 1988)。

M.A. Rosenstein、在Usenix会议文集(Winter的D.E. Geer和P.J.莱文， 1988)。

R. Sandberg、D.戈尔登伯格， S.克莱曼， Sun网络文件系统的D.沃什和B.利昂、“设计和实施”，在Usenix会议文集(Summer， 1985)。

附录：对Sun的网络文件系统的Kerberos应用程序

项目athena工作站系统的关键组件是插话在用户工作站和她/他的专用文件文件存储(主目录)之间的网络。所有专用存储在投入此目的一套驻留计算机(当前VAX 11/750s)。这允许我们提供在公共可用的UNIX工作站的服务。当用户登录到这些公共可用的工作站之一，相当然后验证她/他的名称和密码一个当地居民密码文件时，我们使用Kerberos确定她/他的真实性。登录程序提示输入用户名(和在任何UNIX系统)。此用户名用于拿来Kerberos赋予票据的票据。登录程序使用密码生成解密的票一DES密钥。如果解密是成功的，用户的主目录通过咨询Hesiod命名服务查找并且通过NFS装载。登录程序然后轮控制到用户的shell，能然后运行传统每个用户定制文件，因为主目录“当前附加”到工作站。Hesiod服务也用于修建在本地密码文件的一个条目。(这是为查寻在/etc/passwd的信息。)的程序的目的

从远程文件服务发送的几个选项，我们选择Sun的网络文件系统。然而此系统不能用我们的需要网状连接用一个关键的方式。NFS假设，所有工作站归入两个类别(观察从文件服务器的观点) ：委托和不信任。不信任系统不能访问任何文件，委托能。可信的系统完全委托。假设，可信的系统由友好管理管理。特别地，化妆，因为文件服务系统的所有有效用户和因而获得访问对关于在系统的每个文件从委托工作站是可能的。(“根”拥有的仅文件被豁免。)

在我们的环境，工作站的管理(在UNIX系统管理传统意义)使用它，当前是在用户的手里。我们对在我们的工作站的根密码不隐瞒，因为我们意识到一个确实不友好的用户能由事实训练她或他在物理位置坐和计算机一样并且访问所有控制台功能。所以我们在信任的NFS解释不能真委托我们的工作站。要提供在我们的环境的适当的访问控制我们必须做对基础NFS软件的一些修改，并且集成Kerberos到方案。

未经 Kerberos 修改的 NFS

在我们开始NFS的实施(从University of Wisconsin)，验证提供了以在每NFS请求包括的数据的形式片段(呼叫一“凭证”在NFS术语方面)。此凭证包含关于唯一用户ID (UID)请求方和组标识符(GIDs)的列表的信息请求人的会员。NFS服务器然后使用此信息访问检查。在委托和一个非信任的工作站之间的区别是其凭证是否由NFS服务器接受。

被 Kerberos 修改过的 NFS

在我们的环境， NFS服务器必须接受从工作站，如果和，只有当凭证指示工作站的用户的UID和没

有其他的凭证。

一个明显的解决方案将更改凭证的本质从UID仅仅指示器的，并且对盛放的Kerberos的GIDs验证数据。然而，如果此解决方案采用，一项重大的影响性能是有偿的。凭证在每NFS操作交换包括读的所有磁盘并且写入活动。包括在每磁盘处理的一个Kerberos认证根据我们的信封计算将添加盛放的加密一个一般编号(完成在软件方面)每处理，并且，传送不能接受的性能。(它也将要求安置Kerberos库库例行程序在内核地址空间。)

我们需要一混合的方法，下述。基本想法是有从客户端工作站接收的NFS服务器地图凭证，对在服务器系统的一有效(和可能不同的)凭证。此映射在每NFS处理的服务器的内核被执行和设置在“登上”时间由参与Kerberos被减轻的验证在建立有效内核证件映射之前的一用户级进程。

要实现我们添加一次新的系统呼叫到内核的此(仅要求在服务器系统，不在客户端系统)该为映射功能的控制提供地图流入凭证从客户端工作站到凭证有效为使用在服务器(若有)。基本映射功能映射元组：

对在服务器系统的一有效NFS凭证。CLIENT-IP-ADDRESS从客户端系统供应的NFS请求包解压缩。**注意**：在客户端生成的凭证的所有信息除了UID-ON-CLIENT丢弃。

如果映射不存在，服务器在两种方式之一中起反应，取决于它配置。在我们的友好配置中我们默认不可用图表示的请求到用户的凭证“没人”谁不得以进入特许访问并且有一唯一UID。当有效映射不可以为一流入NFS凭证时，被找到不友好的服务器返回NFS访问错误。

我们新的系统呼叫是使用的添加和删除条目从内核常驻地图。它也提供能力冲洗映射对在服务器系统的一特定UID的所有条目，或者冲洗从一给的CLIENT-IP-ADDRESS的所有条目。

我们修改(处理在服务器系统的NFS安装请求)的登上守护程序接受一种新的事务处理类型，Kerberos认证映射请求。基本上，作为安装进程一部分，客户端系统与她/他的UID-ON-CLIENT的征兆一起提供一个Kerberos认证工具(加密在Kerberos认证工具)在工作站。服务器的登上守护程序转换Kerberos主管名称到本地用户名。此用户名在专用文件然后查寻产生用户的UID和GIDs列表。对于效率，此文件是有用户名的ndbm数据库文件作为密钥。从此信息， NFS凭证被修建并且被递交对内核作为<CLIENT-IP-ADDRESS的有效映射，此请求的CLIENT-UID>元组。

请求在卸下时间发送对登上守护程序从内核删除以前已添加映射。也是可能的发送请求在登出时间无效当前用户的所有映射有问题的服务器的，因而整理存在的剩余的映射(他们虽则不应该)，在工作站使可用为下个用户前。

修改后的 NFS 的 Kerberos 隐含安全问题

此实施不完全安全。最初，用户数据在间在未加密，并且interceptable的网络仍然发送，表。低级，每处理验证根据<CLIENT-IP-ADDRESS， CLIENT-UID>对提供的未加密在请求包。此信息可能被伪造，并且安全因而折衷了。然而，值得注意的是，，只有当用户有效利用时她/他文件(即，当登陆)时是到位有效映射并且攻击此表被限制对，当有问题的用户登陆时。当用户没有登陆，相当数量IP地址伪造不会允许对她/他的未经授权的访问文件。

Kerberos 参考文献

1. S.P. Miller、B.C. Neuman， J.I. Schiller和J.H. Saltzer，部分E.2.1 ：Kerberos认证和授权系统， M.I.T。项目athena，剑桥，马萨诸塞(十二月21， 1987)。
2. E. Balkovich、S.R. Lerman和R.P. Parmelee， “计算在高等教育：阿西纳体验”， ACM的通信

，第28(11)卷，页。1214-1224， ACM (November， 1985)。
3. R.M. Needham和M.D.施罗德，“使用验证的加密在计算机大型网络”， ACM的通信，第21(12)卷，页。993-999 (December， 1978)。
4. V.L. Voydock和S.T.肯特，“在高级网络协议的安全机制”， Computing Surveys，第15(2)卷，ACM (六月1983)。
5. 美国国家标准局，“数据加密标准”，联邦信息处理标准出版物46，政府印刷局，华盛顿特区，DC (1977)。
6. SP染色者，“Hesiod”，在Usenix会议文集(Winter， 1988)。
7. W.J. 布耐恩特， Kerberos程序员的指南， MIT项目ATHENA (在准备)。
8. W.J. 布耐恩特， Kerberos管理员的指南， MIT项目ATHENA (在准备)。
9. G.W. Treese，“在1000个工作站的伯克利Unix ：阿西纳更改到4.3BSD,"在Usenix会议文集(Winter， 1988)。
10. C.A. DellaFera， M.W. Eichin， R.S.法国、D.C. Jedlinsky， J.T.科尔和W.E.佐默费尔特，“Zephyr通知系统”，在Usenix会议文集(Winter， 1988)。
11. M.A. Rosenstein、在Usenix会议文集(Winter的D.E. Geer和P.J.莱文， 1988)。
12. R. Sandberg、D.戈尔登伯格， S.克莱曼， Sun网络文件系统的D.沃什和B.利昂、“设计和实施”，在Usenix会议文集(Summer， 1985)。

相关信息

- Kerberos 支持页
- 技术支持和文档 - Cisco Systems