

RSA双因素身份认证技术在电力信息安全管理中的应用

随着浙江电网信息化建设的发展,供电公司的网络设备大量增长,而以往的网络设备登录大部分采用静态口令登录方式,存在很大的安全隐患。为提高供电公司网络信息安全管理水平,控制网络安全风险。基于RSA双元素身份动态认证工作原理及方式,浙江某供电公司用RSA双因素动态身份认证技术,建立稳定、安全并容易使用的动态口令防护系统,提高使用者的身份认证,保障电网信息系统的安全。

汤亿则 徐志强 黄红兵/国网浙江省电力公司
金加和/浙江省行政首脑机关信息中心



汤亿则/高级工程师

关键词/Keywords

RSA ·
双因素 ·
动态口令 ·
信息安全 ·

电力行业是我国国民经济发展中最重要的基础能源产业,是关系国计民生的基础产业,肩负着重要的社会及经济责任^[1]。随着网络信息技术迅速发展,电力企业对其依赖越来越严重。因网络技术的开放,随之而来的是各种安全威胁,其中安全问题尤其突出的是用户登录过程中的身份认证问题,即用户在计算机网络中确认操作者身份,一般通过用户登录口令实现。当前网络主机系统一般采用用户名+口令的方式登录,主要为静态身份认证,而静态身份认证最大缺点如果盗用合法账号及口令登录系统,系统仍给予他合法的访问权限,因而动态身份的认证则显得更安全。

一般来讲关于网络系统的安全技术一共有5种,分别是身份认证、数据完整性、授权访问、不可否认和保密性。其中最关键、最基本的环节就是身份认证,因为它是进入网络系统的第一个环节,可以授权用户对系统的访问。

随着“SG186”为主体的信息化工程在电力公司的实施,浙江省内的电网

公司、供电站、变电站和营业网点都已经实施网络化管理,网络信息安全保护等级要求账户登录设置足够强,目前用户登录主要输入静态口令。静态口令存在很大的安全隐患,如密码容易被软件工具破解、输入时被人偷窥等,因此静态密码是一种非常弱的身份认证手段。因此,用动态口令身份认证是发展的趋势,也是企业网络信息化管理的需求。

RSA双因素身份动态认证

一个较安全的身份认证系统就是RSA双因素身份认证。首先管理员给相关授权用户发放相关认证设备(通常称之为令牌),然后这个认证设备会随着时间变化定时生成一个随机的、不可预测的和唯一的数字号码。相关人员在第一次使用它的时候,需要对这个认证设备设定一个私人密码(即PIN码,可以类比为银行卡的取款密码)。在使用过程中,用户个人密码与此设备上的号码相组合,就会形成所谓的双因素认证码(称为pass code以区别静态口令的password)。RSA当中的同步身份认证技术能够使这个认证设备与认证服务器在相同的时间生成相同的号码,这样就可以保证持有这个认证设备的合法用户安全地进行访问。

1. 与RSA 双因素身份认证相关的系统组件

代理软件RSA Authentication/Agent、认证服务器AM(即RSA Authentication Manager)、认证应用编

程接口 (API) 及认证设备组成了RSA Secur ID, 如下图所示。

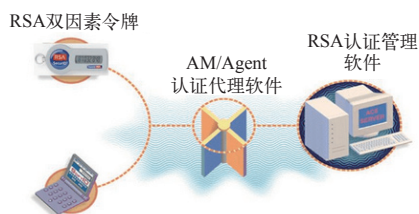


图 RSA双因素身份认证系统组成

(1) 认证令牌RSA SecurID

目前认证令牌市场有很多种类, 以RSA 700型硬件令牌为主, 内设芯片和电池, 该令牌的形状如同一把普通的钥匙。该令牌已经内置了128位种子文件, 种子文件在特定时间进行同步计算, 每分钟自动产生一动态认证令牌码。认证令牌给客户用的时候已做了初始化处理, 客户可以设置个人识别码 (Personal Identification Number, PIN), 每次这个令牌的使用者在使用令牌访问资源的时候, 同时需要输入PID码再加上令牌的组合, 即pass code, 也即双因素口令。

时间是可以有相同标准的 (例如都取北京时间), 也因此该认证设备与服务器可以同时各自单独进行运算, 并且会出现相同的结果, 这个原理使得RSA的双因素身份认证能够顺利实现身份认证。

(2) 代理软件 (RSA AM/Agent)

代理软件有一个重大的作用, 可以保护重要的网络资源。当某用户打算在网上访问某项内容时, RSA认证代理软件就会将确认请求发到服务器上以方便用户进行认证。

RSA Authentication/Agent是一种设备专用代理软件, 很多网络设备、相关浏览器和网络服务器软件系统中都内置了此软件, 它可以允许安全管理员不再编写代码, 而是通过点击鼠标来为用户提供相应的设置, 方便用户选择。

(3) 认证管理软件

此种认证管理软件是一个认证管理系统, 它将集中管理功能与性能非常好的认证引擎结合到一起。例如, 当一个认证请求指令发送到已经安装此认证管理软件的服务器时, 此认证管理软件

将使用相关算法来确认正确的认证码。如果所输入的数字是正确的, 那么认证合格通过, 该用户操作者可以访问相应的网络资源。

2. 身份认证口令构成

PASS CODE, 这是一个完整的口令, 它在使用RSA信息安全公司所提供的解决方案Secur ID后, 让用户使用者自己设置PIN码, 一般是4~8位。

3. 安装平台

Windows操作系统、AIX、Solaris和HP-UX可以让RSA Authentication Manager得以运行。1个RSA认证管理者可以为用户提供上百万的容量。RSA认证管理者是有高级和基本两种许可证的。基本许可证可以保证用户安装1台从服务器和一台主服务器; 而高级许可证保证多达6个服务器域 (Realm) 使用, 每个服务域由1台主服务器以及10台左右的从服务器构成。这种架构一方面可以保证它高效运行; 另一方面可以适合特大的电网网络相关结构。

工程实例

江苏某供电公司2013年正式使用RSA SecurID动态认证系统, 当前公司网络设备主要有: 防火墙、H3C交换机、路由器、CISCO交换机和认证管理软件。

1. RSA SecurID认证服务器及Radius服务器部署

硬件安装环境用的是服务器HP DL380G52, 操作系统应用的是标准的Windows Server 2012 R2, 并分别安装主认证服务器RSA Ace/Server和从属服务器Replica Server。这2个服务器之间会进行自动同步运算, Primary Ace/Server将会完成全部信息修改工作, 并且Primary Ace/Server会随时将不同信息定时与Replica Ace/Server进行同步, 以保证信息可靠一致。这两个服务器是可以一起同时提供相关认证服务的, 不管哪一台服务器出现问题都不会让相关认证服务发生中断现象。当Primary Ace/Server出现问题, 并且信息没有办法进行修改时, 可以考虑将Replica Ace/Server升级或者将Primary Ace/Server先前的备份进行恢复。

2. 关于服务器的主机保护

供电公司有大型服务器，服务器运行关键应用系统和存储重要数据信息，对公司整体的运行起着关键作用。但是这些服务器正在使用一个简单的密码身份验证，系统管理员和普通用户，都可以使用密码登录到主机系统。这样非法用户可以使用其他用户帐户和密码进入系统，存在严重的安全隐患。确保系统安全的目的是为用户提供数据处理环境，保护计算机设备、设施，消除软件环境的安全隐患，防止网络攻击，支持信息安全平台。RSA不仅为Windows操作系统提供代理软件，它也支持3个主流的UNIX操作系统（例如IBM AIX、HP-UNIX和SUN Solaris）。除此之外，还支持Linux中的代理软件，并为某些特定的操作系统提供定制的代理软件。

安装了RSA ACE/Agent for Windows，RSA配置后可以获得相应的用户身份验证。当用户登录到主机，主机会先提示相关用户输入正确的用户名和密码。当用户输入用户名和密码之后，主机根据用户名查找记录，确认是否需要强烈的双重认证。如果需要，用户输入正确的标记代码和PIN密码才能进入主机系统，否则将被拒绝访问。

3. 数据库保护

世界上领先的数据库管理软件供应商是Oracle，使用由其提供先进的安全选项（ASO）软件保护SQL。当用户想要访问Oracle数据库时，Advanced Security Option会对其进行加密，并执行相关的安全检查，RSA ACE/服务器技术通过每个用户之前的RSA SecurID令牌认证用户的身份。使用Oracle的先进的安全选项和RSA SecurID令牌，所有的网络应用程序基于Oracle数据库都可以提供RSA SecurID密码来增强身份验证。

4. 无线网络和端口安全保护

有的时候，用户需要通过无线网络登录公司网络时，就需要采用这种双因素身份验证，只有通过验证合格的用户才可以登录公司网络。RSA SecurID可以提供以802.11 b协议为基础的无线网络，还能够以802.1 x端口安全保护为基础来进行双重身份认证。

5. 应用保护

以Oracle应用程序为例，关于Oracle Portal和Oracle应用程序，RSA专门提供了AM/代理插件，插入在Oracle Portal和Oracle应用程序中，帮助企业使用令牌双因素身份验证来进行用户身份认证，并替换以前的用户名和密码身份验证。用户仅需要一个认证就可以直接登录到相关应用程序，避免用户记住麻烦的静态密码。但是关于用户访问控制的权限是由Oracle ERP来独立完成的，所以同样的用户信息必须存储在Oracle ERP和RSA认证服务器中，并且要求同一用户的用户名需要保持一致。

结束语

针对目前电力行业安全信息管理系统，使用RSA双重动态身份认证技术实现浙江某电力公司网络和服务安全保护，建立一个稳定、安全和易于使用身份认证系统，以提高信息安全管理水平，确保供电网络和应用系统平稳运行，为电力行业的正常业务发展提供有效的保护。

参考文献

- [1] 王栋，刘识，王怀宇，等．电力行业三级信息系统等级保护典型设计研究[J]．电力信息化，2012，10(8)：81-84．
- [2] OPPENHEIMER P．自顶向下的网络设计[M]．3版．北京：人民邮电出版社，2011．
- [3] CONVERY S．网络安全体系结构[M]．北京：人民邮电出版社，2013．
- [4] 张鑫，陈雪华，刘新．电力系统信息安全基线标准体系的构建[J]．电力信息与通信技术，2013，11(11)：110-114．
- [5] 国家电网公司．国家电网公司“十二五”信息化发展规划[R]．2011．
- [6] 国家电网公司．国家电网公司信息系统安全保护等级定级指南（试行）[R]．2006．
- [7] 国家电网公司．国家电网公司信息安全加固实施指南（试行）[R]．2009．

（收稿日期：2014-12-10） EA