Windows 2003 活动目录安全性研究①

Active Directory Security Based on Windows 2003

胡建军　王万军　李志浩　(甘肃联合大学 数学与信息学院 甘肃 兰州 730000)

摘　要：本文探讨了分布式环境下 Windows 2003 活动目录的安全性，包括活动目录自身的安全性和活动目录资源的安全性，并就如何增强活动目录安全给出了相应对策。

关键词：活动目录 认证 复制 安全 Kerberos v5 协议

2000 年 12 月微软首次在 Windows Server 2000 引入了活动目录技术，之后在 2003 年 4 月微软又一次发布了活动目录的改进版本。由于活动目录能够很好地支持分布式资源的管理与访问，因此利用它架构网络已成为一种发展趋势，然而活动目录的安全问题是不容忽视的问题，因为它影响着网络的性能，目前针对活动目录安全的讨论主要集中在资源的访问控制上，而针对活动目录自身安全的研究不是很多且不够全面，为此本文探讨活动目录自身安全性和活动目录资源安全性问题。

1　登录认证

Windows 2003 活动目录采用的是 Kerberos v5 缺省认证协议。用户在访问域中的资源时，必须要通过域控制器的验证，然后由域控制器自动给用户建立一个访问令牌，当用户获得该令牌之后，他携带令牌才能申请访问域中的资源。

1.1 认证过程简介

假设客户端是 Windows xp/2000/2003/vista 用户，且启用了 Kerberos v5 认证协议，图 1 是用户在同一域中和不同域之间对资源访问的一个实例。下面具体分析用户对资源的访问过程[1-3]：

（1）用户从客户端计算机上输入账户名和密码，即图 1 的第一步“（1）”,域控制器 A 启用 Kerberos v5 认证服务进程查询活动目录数据库对客户信息验证，如果是合法用户，则 Kerberos v5 认证服务进程向客户端计算机返回一个访问令牌，即图 1 的第二步“（2）”，该令牌包含用户的 SID（安全标识符）和用户的通用组、全局组、域本地组成员资格，否则丢弃用户信息。

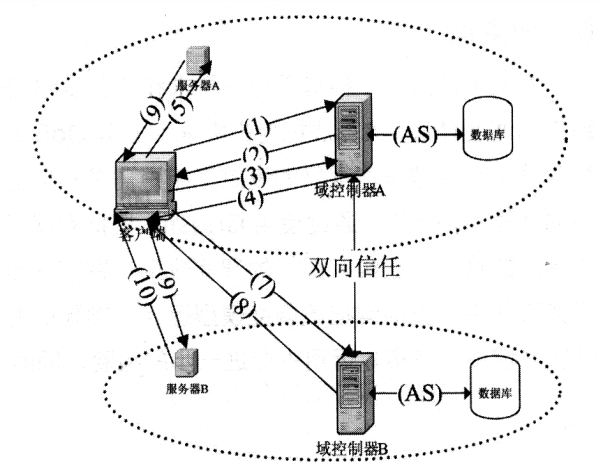

图 1　域认证及资源访问

（2）如果在（1）中用户成功地拿到一个令牌，则客户端计算机将缓存登录会话，并一直保持该登录会话，直到客户注销操作系统。

（3）如果用户要访问同一域服务器 A 的资源，首先应从域控制器 A 获得访问服务票据，然后拿着访问服务票据去访问服务器 A 的资源。即用户拿着令牌在域控制器 A 上申请票据授权证，即图 1 的第三步

① 收稿时间:2008-07-27

“（3）”，域控制器 A 验证用户的访问权限后，回送票据授权证，即图 1 的第四步“（4）”，接着用户拿着票据去访问服务器 A 中的资源，即图 1 的第五步“（5）”，服务器 A 验证票据后，向用户开放联机服务，即图 1 的第六步“（6）”。

（4）如果用户要访问不同域服务器 B 的资源，首先应从域控制器 B（由于域控制器 A 和 B 存在双向信任关系，因此用户无需再获取令牌，）获得访问服务票据，然后拿着访问服务票据去访问服务器 B 的资源。即用户拿着令牌在域控制器 B 上申请票据授权证，即图 1 的第七步“（7）”，域控制器 B 验证用户的访问权限后，回送票据授权证，即图 1 的第八步“（8）”，接着用户拿着票据去访问服务器 B 中的资源，即图 1 的第九步“（9）”，服务器 B 验证票据后，向客户开放联机服务，即图 1 的第十步“（10）”。

1.2 认证安全分析及防范

从上述用户对网络资源的访问可以得出以下结论[4-6]：

（1）Kerberos v5 服务不能避免“拒绝服务”和“口令猜测”的攻击，因此对于“拒绝服务”攻击要靠管理员和用户检测解决，对于“口令猜测”攻击要对修改 Administrator 用户名并设置复杂密码，要定期改变密码和用户名，同时应杜绝 Guest 账户的入侵。随时查看系统安全日志，监视网络的运行，及早预防攻击。

（2）由于客户端缓存了访问令牌，这就为他人入侵系统提供了可能，为此用户在离机前应该注销系统或使系统进入保护状态，也要随时保持计算机是一个安全环境，以防木马病毒的入侵。

（3）跨域访问存在安全隐患。由于活动目录的双向信任关系，致使在跨域访问时，无需跨域认证，只要有共享令牌，就可以返回给用户访问票据，这会给管理带来许多麻烦。对于跨域安全问题，建议设置安全的访问控制列表，注意双向信任关系的使用，把资源作为全盘问题考虑。

（4）用户数量很多时，活动目录认证会产生网络瓶颈问题。例如有 N 个用户对 M 个资源同时进行访问，域控制器需要创建 N 个访问令牌（每用户一个），每个用户访问 M 个资源需要 M 个票据，因此，N 个用户访问 M 个资源需要处理 N*M 个票据，随着用户数量的增多，域控制器的负担会越来越重，因此如果将诸如电子邮件服务的认证交给活动目录，则势必会加重域控制器的负担，造成认证瓶颈问题。对于认证瓶颈问题，如果网络服务认证确实需要活动目录认证，最好是多安装几台域控制器，以便使认证分散在不同的域控制器上，减少网络瓶颈。

2 目录信息同步

活动目录使用多主机集中松散一致性复制模型，多主机是指林中的所有域控制器均可以接受改变，它们地位是平等的；松散一致性是指在任意特定域控制器上的数据库拷贝不能保证同时与其它域控制器一致；集中是指对目录的改变将通过全部拷贝逐步传递，最终集中统一为相同的值。该模型的优点是避免了单主复制模型中主域控制器失效后需要手工恢复的不便，具有高性能、可扩展和较强容错能力等优点。而缺点是由于多主域控制器都是可读可写的，容易引发活动目录复制冲突，另外由于更新是实时的，会消耗一定的网络资源。

2.1 复制原理

活动目录是通过同步机制给用户提供统一目录视图的。活动目录根据网络的带宽和管理员设置的站点开启了两个同步进程，一个是知识一致性检查 KCC（Knowledge Consistency Checker）进程，另一个是站点间拓扑产生器 ISTG（Inter-site topology Generator）进程，这两个进程保证了活动目录数据的一致性，活动目录的复制过程如图 2 所示。下面分别介绍这两个进程的工作过程[1-3]：

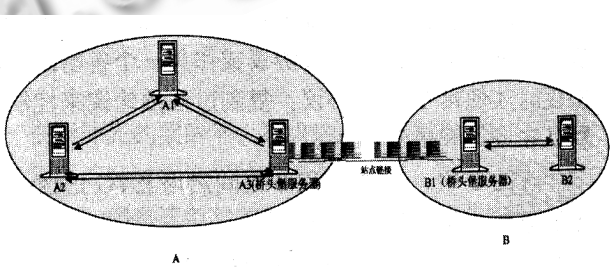

图 2　活动目录复制过程

（1）KCC 是一个站点内同步进程。KCC 是域控制器的内建进程，默认情况下该进程每 15 钟运行一次，尽管它不能看到物理网络，但是它会自动在站点内的每一部域控制器与域控制器间，自动产生环状路径的目录复制拓扑结构，以保持复制拓扑的完整性。活动目录复制系统允许复制拓扑的循环（拓扑环以 3

个为宜)。尽管如此，在任意时刻，如果某一站点内的复制无法进行或出现单点故障，KCC 将会介入并新建所需数量的连接对象以继续进行活动目录复制。除此之外，活动目录域也会定期地分析一个站点里的目录数据更新复制路径，以确保这条目录数据复制路径是有效的。该进程需要高速、可靠的网络连接；复制流量是未经压缩的；它采用 RPC over IP 复制协议。

在图 2 中，A 站点和 B 站点分别启用 KCC 进程。

(2) 在站点间也存在复制拓扑，站点间的复制拓扑是由站点间拓扑产生器 ISTG 建立和维护的。每个站点都会自动指定一台域控制器作为 ISTG，默认情况下在每个站点中的第一台域控制器充当 ISTG 的角色，不能手工指定 ISTG 角色。ISTG 服务器可以在站点中自动选择一台或多台域控制器成为桥头堡服务器，来执行站点间的复制。

在不同站点间进行复制，默认情况下 KCC 是不知道复制拓扑的。这时就要求在两个站点间创建一个站点链接，KCC 把这个站点链接作为站点间复制的逻辑路径。可以把两个或两个以上的站点链接通过站点链接桥连接起来，以规范网络的路由选择，需要注意的是一定要确保站点链接桥所连接的不同站点链接中有相同的站点。默认情况下，KCC 自动在一个站点内指定桥头堡服务器，当该桥头堡服务器不能正常工作时，KCC 自动指定其他服务器作为桥头堡服务器。站点间的复制流量是经过压缩的；复制采用的协议是 RPC over IP 或 SMTP,但 SMTP 只能用于不同域的域控制器之间的复制，大多数情况下，采用 RPC over IP，仅当网络链接不支持 RPC 协议或作为一个备份的传输协议时才使用 SMTP 协议；复制过程由轮询来控制，默认轮询时间是 3 小时。

在图 2 中，站点 A 和 B 之间启用 ISTG 进程。

2.2 复制安全分析与防范

(1) 站点内复制。对于 KCC 复制进程，由于每 15 钟运行一次，如果在目录同步时还未完成修改，则会导致目录不同步现象，因此在修改目录数据时应先断开网络连接，待修改完成之后再连接网络；信息在站点内复制是没有加密和压缩的，这会遭到截获和篡改攻击，因此要随时检查物理链路是安全和高速可靠；域控制器本身要绝对安全，以防权限低的用户执行权限高的用户职责，从而导致错误的数据同步；KCC 进程要求域控制器有严格的同步时钟，否则冲突解决会很困难，因此要随时校正域控制器的时钟。

(2) 站点间复制。对于 ISTG 复制进程，由于是远距离传输，保证物理链路安全是首要问题，因此要在 Internet 上建立 VPN (Virtual private network) 链路，同时要应用防火墙技术；该进程仍然存在时钟同步问题，对于该问题，要考虑时差调整，这要根据实际环境测量计算；域控制器本身也要绝对安全。

3 其他安全性考虑

除前面讨论的活动目录安全性问题外，还有许多安全性问题，比如文件资源安全、打印机资源安全等，资源的访问存在非授权用户的入侵，而这些安全问题往往是因不必要的授权引起的，因此对于这些安全性问题，一般都要通过使用 NTFS 文件系统的访问控制列表和组策略配置实现，有关这方面的资料很多[2,4,7]，这里就不再赘述。

4 结束语

Windows 2003 活动目录为用户访问分布式资源提供了统一视图，也为管理员集中维护网络提供了便利，它不仅集成了关键服务，而且集成了关键的应用如 DNS、MSMQ (消息队列服务) 服务、电子邮件等。本文从活动目录自身的安全性问题出发，分析了活动目录在认证和复制方面存在的安全性问题，就如何加强活动目录安全给出了相应的对策。

参考文献

1 颜逸品.Windows 2000 Server 企业网络建构实务——Active Directory 篇.北京:中国铁道出版社,2001.

2 商宏图.Windows Server 2003 活动目录.北京:机械工业出版社,2005.

3 Oppermann C.Windows 2000 Active Directory 程序设计.北京:机械工业出版社,2002.

4 Boswell W.Windows server 2003 技术内幕(基础篇).北京:清华大学出版社,2004.

5 王亚弟,束妮娜,韩继红,等.密码协议形式化分析.北京:机械工业出版社,2006.

6 牛少彰,江为强.网络的攻击与防范---理论与实践.北京:北京邮电大学出版社,2006.

7 刘晓辉,王春海,盖俊飞,等.Windows server 2003 组网教程(管理篇).北京:清华大学出版社,2005.