Windows安全原理与技术

— 第五章：身份验证

王轶骏， Eric Ericwyj@sjtu.edu.cn

SJTU.INFOSEC.A.D.T, 2008

Windows 2000安全模型对资源可用性的控制

- 身份验证
  - 系统对请求访问特定资源的个体或客户的身份进行验证。
- 访问控制
  - 系统根据授予用户和资源的权限执行访问控制检查。

Windows 2000的身份验证

- 交互式登录过程
  - 要求用户登录到域帐户或本地计算机帐户。
- 网络身份验证过程
  - 要求用户向特定的网络服务提供对身份的证明。

身份验证协议

- 过去简单的身份验证机制使用共享密钥（口令）。
  - 容易被截获、假冒。
- Window 2000则使用了大量保护共享密钥的机制和协议。
  - Kerberos v5
  - NTLM
  - SSL/TLS
  - 硬件令牌（智能卡）

交互式登录

- 本地计算机登录
  - 能提供对本地计算机中资源和服务的访问权限。
- 域帐户的登录
  - 能提供对本地计算机和域中网络身份验证服务的访问权限。

交互式登录组件

- **winlogon**
  - 加载其余两个组件。
  - 处理与验证策略无关的用户界面操作。
    - 创建可用的桌面
    - 向操作系统注册一个安全维护序列（SAS, Secure Attention Sequence）
    - 维护工作站状态
    - 实现超时处理
  - 向GINA发送事件通知消息，提供可供GINA调用的各种接口函数。
  - 保证其操作对其他进程不可见。

交互式登录组件

- **GINA动态链接库**
  - 提供了winlogon用户标识和验证用户的输出函数。
    - WlxActivateUserShell、WlxDisplaySASNotice、WlxInitialize、WlxLoggedOnSAS、WlxLoggedOutSAS、WlxLogoff、WlxNegotiate、WlxScreenSaverNotify、WlxShutdown、WlxStartApplication、WlxWkstaLockedSAS
  - 微软提供的GINA是**MSGINA.dll**，但允许被用户替换来自行定制系统的用户识别和身份验证。
    - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

      "GinaDLL"="ginadll.dll"

交互式登录组件

- 网络提供程序的动态链接库
  - 提供通过标准协议到其他类型网络（如Novell）的辅助身份验证功能。

Winlogon初始化

- 注册SAS
  - 默认为Ctrl+Alt+Del
- 生成三个桌面
  - 屏幕保护桌面
  - Winlogon桌面
  - 应用程序桌面

Winlogon可维护的三种状态

- 已注销状态
  - 发生在没有任何交互式登录会话期间。
- 已登录状态
  - 允许用户访问应用程序桌面，并执行任何所需的任务。
  - 可以切换到其他两种状态。
- 已锁定工作站状态
  - 提供了一个安全桌面
  - 可以通过用户身份验证切换到已登录状态，或者通过管理员身份验证切换到已注销状态。

已锁定状态

已注销状态

已登录状态

Winlogon的超时处理

- Winlogon能为它所提供给GINA的安全对话框实现超时处理能力。
- 出现在已锁定状态和已注销状态时。

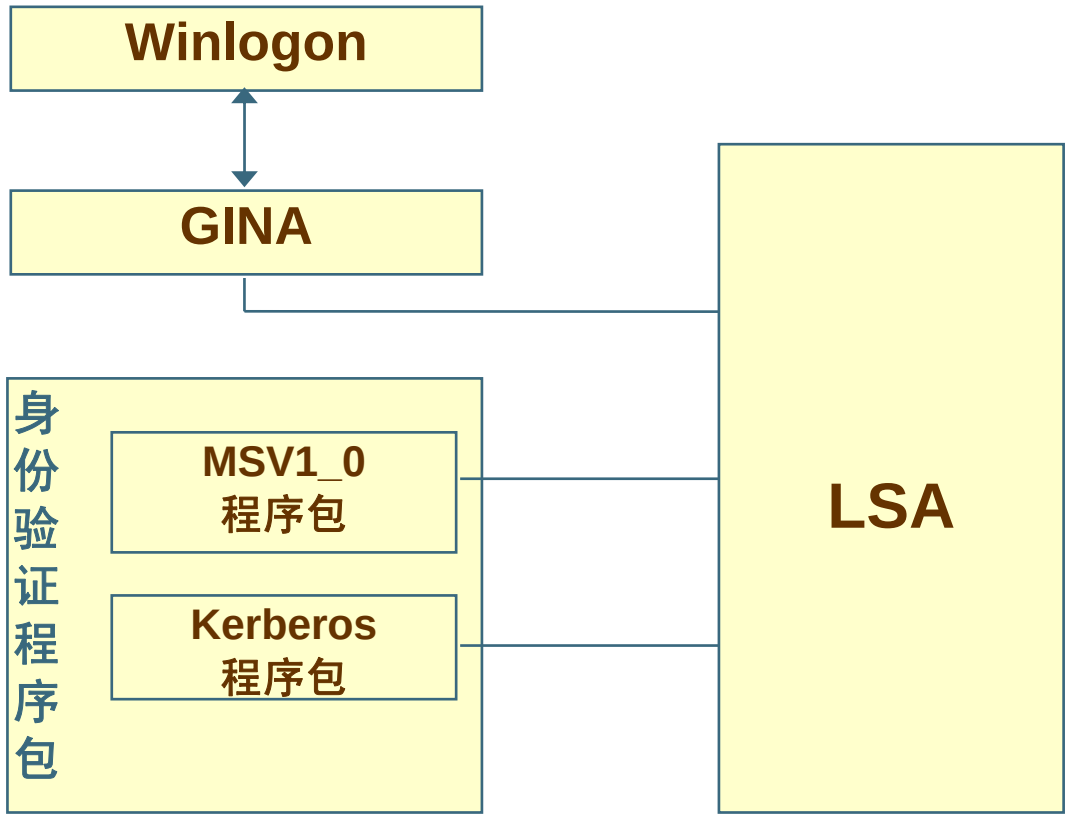
安全对话框的超时处理能力

身份验证程序包

- 身份验证程序包的任务
  - 验证用户
  - 为用户新建LSA登录会话
  - 返回一组绑定到用户安全令牌中的SID
- 身份验证程序包位于某一动态链接库（DLL）中
  - 在系统启动期间被本地安全授权机构（LSA）所链接。
  - 接受输入的登录证书，通过验证程序决定是否允许用户登录。
- Windows 2000安装的身份验证程序包
  - MSV1_0
  - Kerberos v5

本地安全授权机构（LSA）

- LSA负责在本地登录和远程登录中验证用户身份，并维护本地安全策略。



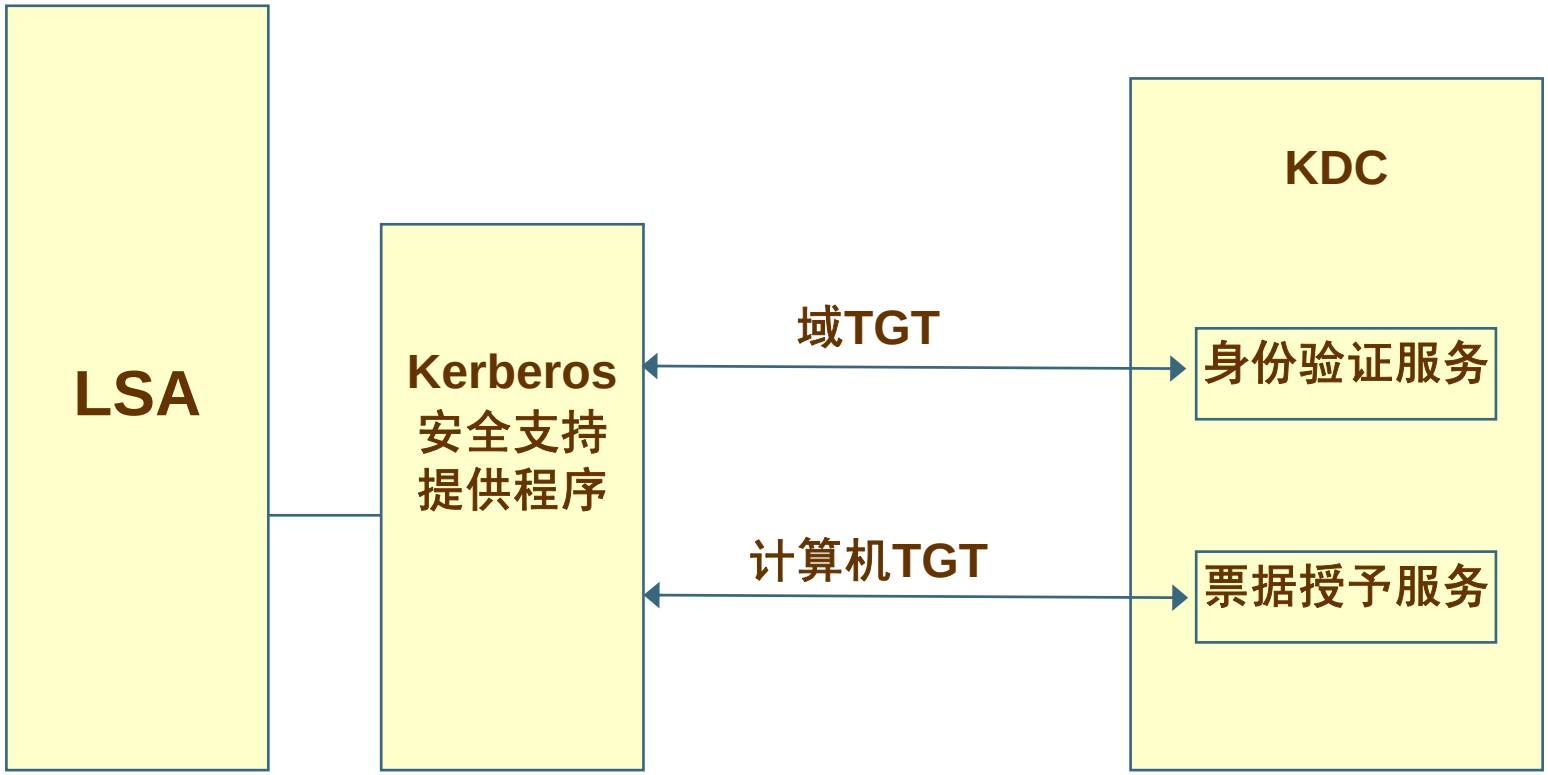
交互式登录到本地计算机

- 用户按下SAS热键。
- Winlogon切换到Winlogon桌面，并调用GINA来显示登录对话框，等待用户输入用户名和口令。
- 当用户输入信息之后，GINA将它传送给LSA进行验证。
- LSA调用适当的验证程序包（MSV1_0），并且将口令使用单向散列函数转换成非可逆的密钥形式，然后在SAM数据库中找寻匹配的密钥。
- 若SAM找到了账户信息，就向身份验证程序包返回用户的SID和用户所在组的SID。
- 验证程序包向LSA返回这些SID。
- LSA使用这些SID创建安全访问令牌，并把令牌句柄和登录确认信息返回给Winlogon。
- 用户进入Windows桌面。

交互式进入域帐户

- 用户通过按下SAS热键。
- Winlogon切换到Winlogon桌面，并调用GINA来显示标准的登录对话框，提示用户输入用户名、口令和域名称。
- 当用户输入了UPN和口令并选择了正确的域名，GINA就会将这些信息传到LSA进行验证。
- 当LSA接收到用户的登录信息后，将口令使用单向散列函数转换成非可逆的密钥形式，然后将其存储在以后还可以检索到的证书缓存区中。
- LSA通过Kerberos验证程序包向KDC发送一个含有用户身份信息和验证预处理数据的验证服务请求。

- KDC收到该验证服务请求之后，用自己的密钥对其解密来验证用户是否确实知道口令。
- 一旦KDC证实了用户的身份，就会为客户返回一个登录会话密钥（用客户密钥加密），并且向Kerberos验证程序包返回一个TGT（用KDC自己的密钥加密）。
- Kerberos验证程序包将登录会话密钥解密并将它同TGT一起存储到证书缓存区中以备后用。
- Kerberos验证程序包为本地计算机向KDC发送一个票据请求，KDC则会用ST响应。
- LSA确定用户是否为任何本地安全组的一部分，以及用户在这台计算机上是否拥有任何特权。据此而得到的SID与来自会话票据的SID一起被LSA用来创建会话令牌。该令牌句柄和登录确认信息返回到Winlogon。
- 用户进入Windows桌面。


LSA
Kerberos
安全支持
提供程序
域TGT
计算机TGT
KDC
身份验证服务
票据授予服务

域验证

- 每个Windows 2000服务器和工作站都包括一个Kerberos安全支持提供程序。

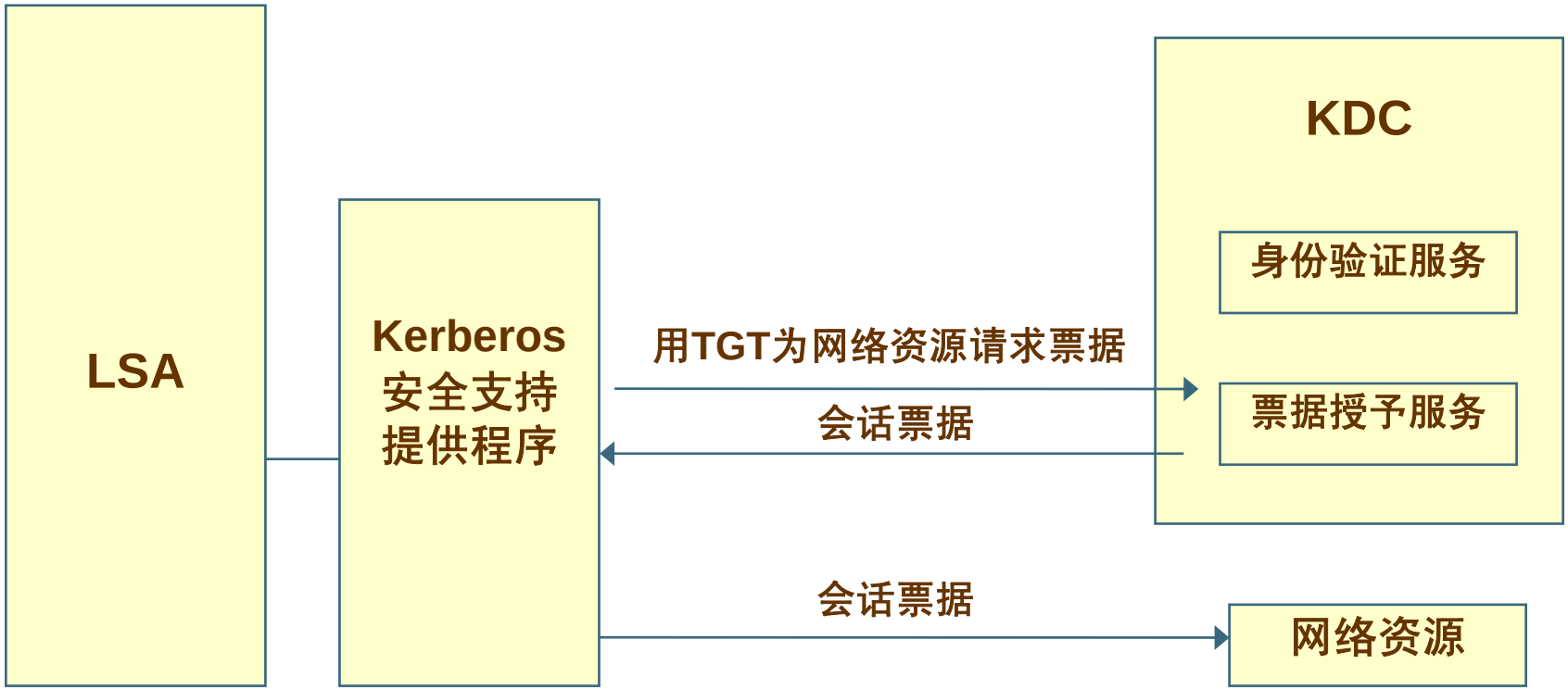
  （Security Support Provider, SSP）

- 验证顺序
  - 最近的KDC为首选KDC。
  - 从DNS中寻找其他KDC。
  - 找不到任何KDC，则使用MSV1_0进行验证。

网络身份验证过程

- 对于本地登录的用户而言，其每次请求网络服务时都要重复的手工进行。
- 对于域帐户登录的用户而言，其每次请求网络服务的时候都会透明的完成，无须任何手工操作。
  - 单一登录特性（Single Sign-on, SSO）

网络身份验证


LSA
Kerberos
安全支持
提供程序
KDC
身份验证服务
票据授予服务
用TGT为网络资源请求票据
会话票据
会话票据
网络资源

NTLM身份验证协议

- NTLM协议是Windows NT 4.0系统中身份验证的默认协议，它在Windows 2000中仍然为了低版本客户和服务器的兼容性而保留。
  - Windows 95
  - Windows 98/Me
  - Windows NT

NTLM协议的安全缺陷

- NTLM是微软开发的专用协议，而不是开放式的工业标准 。
- NTLM不提供双向的认证，只有服务器认证客户端 。

NTLM协议的使用场合

- Windows 2000 Professional客户端向Windows NT 4.0的域控制器验证身份。
- Windows NT 4.0 Workstation客户端向Windows 2000域控制器验证身份。
- Windows NT 4.0 Workstation客户端向Windows NT 4.0域控制器验证身份。
- 未加入到域中的计算机的身份验证。

Kerberos v5身份验证协议

- **Kerberos协议的起源：**

  美国麻省理工学院的Athena项目。

  - 为分布式环境提供双向验证的方法。
  - 被IETF（Internet工程任务组）在RFC 1510中所采纳。
- **Kerberos v5是Windows 2000的默认身份验证协议。**
  - 协议的安全性基础：
    公钥加密协议。
  - Kerberos客户的实现：
    Kerberos安全支持提供程序接口（SSPI）。
  - Kerberos密钥分发中心（KDC）与域控制器上的安全相结合：
    使用活动目录服务作为安全账户数据库。

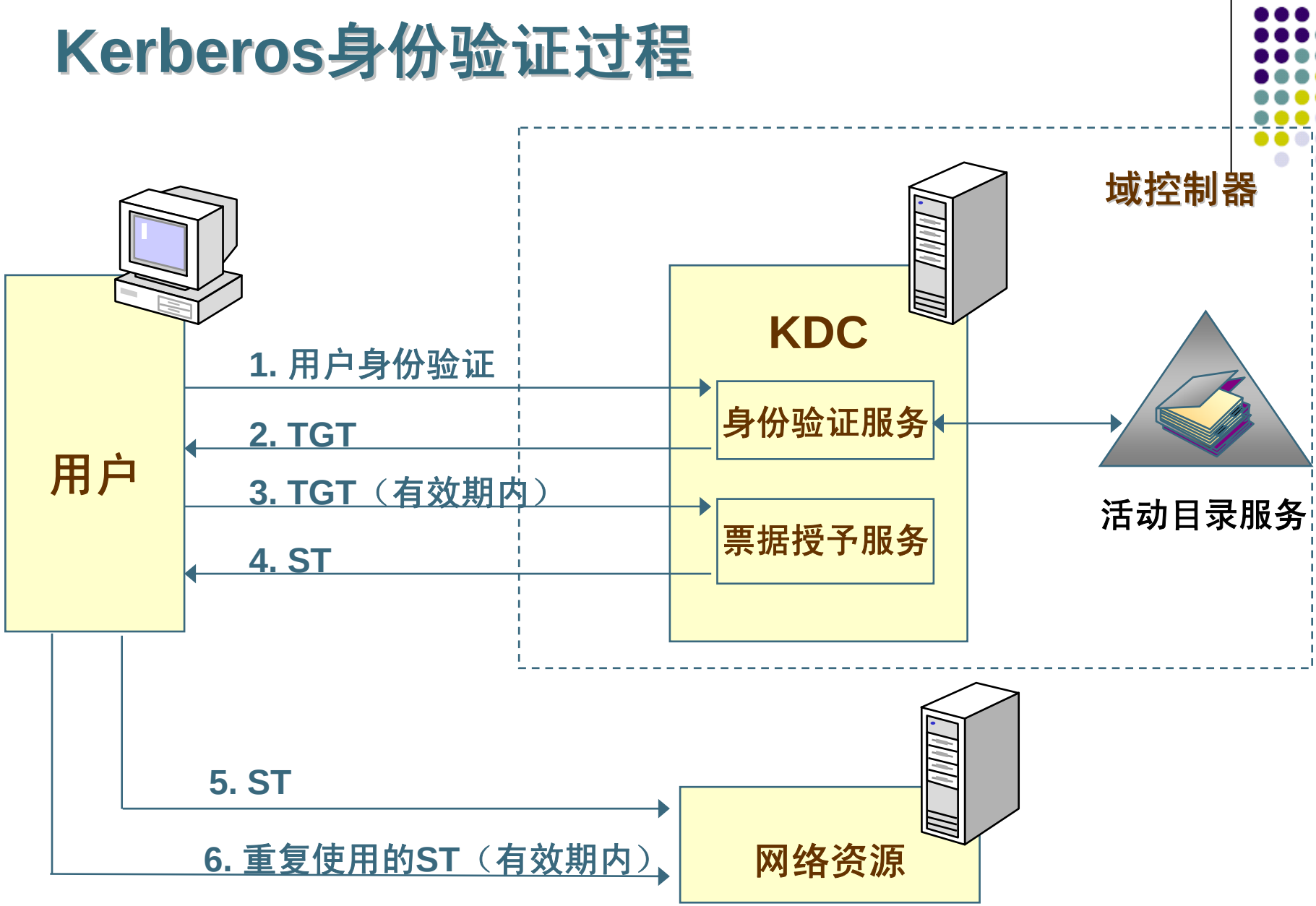
Kerberos身份验证概述

- Kerberos协议是一个基于票据的系统。
  - 客户向网络验证，并从KDC请求票据用以访问网络资源。
- Kerberos协议的技术依据：共享机密身份验证。
  - 若仅有两个人知道秘密，那么两人中的任何一个人都可以通过确认另一个人是否知道这个秘密来确认对方的身份。

Kerberos密钥分发中心（KDC）

- 身份验证服务（AS）
  - 对用户进行验证，并发行供用户用来请求会话票据的TGT（票据授予票据）。
- 票据授予服务（TGS）
  - 在发行给客户的TGT的基础上，为网络服务发行ST（会话票据）。

Kerberos身份验证过程



Kerberos票据的内容

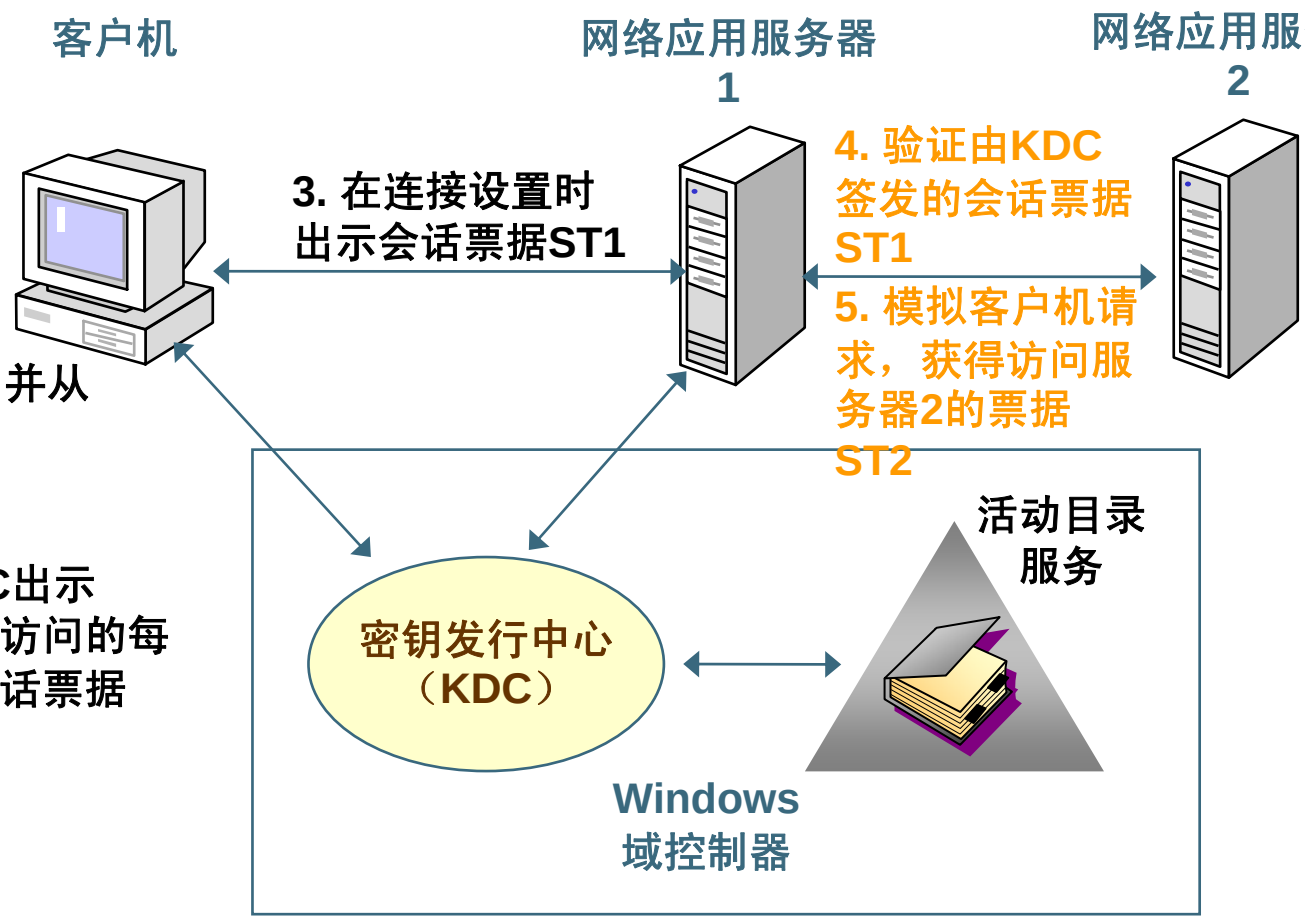
- 非加密部分
  - 票据格式的版本号
    - 在Windows 2000 Kerberos v5协议中，该版本号为5。
  - 发布票据的域的名称
  - 密钥发行中心的服务器名称
- 加密部分
  - 客户和服务之间为安全传输而共享的会话密钥
  - 客户所在域的名称
  - 客户名称
  - 票据起始时间
  - 票据生存时间（有效时间）

票据的有效期

- TGT过期状态下
  - 当客户请求新的ST时，KDC将响应一个错误消息，客户必须从KDC请求一个新的TGT。
- ST过期状态下
  - 当客户请求访问位于服务器上的某个资源，那么该服务器将响应一个错误信息，客户必须从KDC请求一个新的ST。
  - 若ST是在客户已连接到资源的期间过期的，那么客户不会立即断开连接，但当客户下一次请求访问该资源时，就需要上述过程来进行访问。

Kerberos的身份验证委派

- 客户端身份验证可以交给应用程序涉及的服务器。
  - 服务器会模拟客户端，并代表客户端来执行访问请求。
  - 所有身份验证凭据和票据的传递并不需要用户输入。
  - 虽然服务器会模拟客户端，但对原始客户端的审核记录会被保存。


客户机
网络应用服务器 1
网络应用服务器 2
3. 在连接设置时出示会话票据ST1
4. 验证由KDC签发的会话票据ST1
5. 模拟客户机请求，获得访问服务器2的票据ST2
1. 客户机登录，并从KDC接收TGT
2. 客户机向KDC出示TGT以换取需要访问的每个资源所需的会话票据ST1
密钥发行中心（KDC）
活动目录服务
Windows 域控制器

Kerberos协议的优点

- 服务器更加高效的验证
- 相互验证
- 授权验证
- 简化信任管理
- 协同工作能力

SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

Any Questions ?

确定 取消