网络安全协议及分析
认证协议Kerberos

密码与网络安全系　刘虹

2025年春季学期

课程体系

第一章 概述

第二章 链路层扩展L2TP

第三章 IP层安全IPSec

第四章 传输层安全SSL和TLS

第五章 会话安全SSH

第六章 代理安全Socks

第七章 网管安全SNMPv3

第八章 认证协议Kerberos

第九章 应用安全

本章学习目标

- Kerberos协议流程
- Kerberos票据和认证符
- Kerberos消息

提纲

一、Kerberos协议流程

二、Kerberos票据和认证符

三、Kerberos消息

Kerberos协议

- Kerberos来源于希腊神话“三个头的狗——地狱之门守护者”。
  - 采用客户端/服务器结构与对称加密技术，并且能够进行相互认证，即客户端和服务器端均可对对方进行身份认证。
  - 可以用于防止窃听、防止replay攻击、保护数据完整性等场合，是一种应用对称密钥体制进行密钥管理的系统。

Kerberos协议

- Kerberos所应对的安全威胁
  - 同一工作站的某个用户可能冒充另一个用户操作该机器。
  - 用户可以更改工作站的IP地址冒充另一台工作站。
  - 攻击者可能实施重放攻击。
  - 攻击者可能操纵某台机器冒充服务器。

Kerberos协议

- 主要思想：当收到来自某个用户的服务请求时，应用服务器需要对其身份进行认证，而最直接的方式是验证用户口令。为减轻应用服务器的负担，Kerberos将验证用户身份的工作交给可信第三方。
  - 引入可信第三方
  - 引入票据许可服务器
  - 引入时间参数
  - 引入会话密钥和认证符
  - 实现双向认证
  - 密钥转化

Kerberos协议

引入可信第三方

- 基于可信第三方（定义可信第三方为**认证服务器**，即Authentication Server，AS）的认证要求第三方分别维护与用户和应用服务器共享的密钥。
- 在访问应用服务器之前，用户所使用的客户端代理用户向AS发送认证请求，其中包含用户名和口令。AS收到这个请求后，将客户端提供的信息与本地维护的信息进行比较，若一致，则认可用户身份，并返回用于访问应用服务器的凭证——用应用服务器密钥加密的票据。

票据：{客户端用户名 | 客户端主机IP地址 | 应用服务名}

Kerberos协议

- 在获取票据后，客户端向应用服务器发送服务请求，其中包括用户名和票据。服务器用自己的密钥解密票据，如果解密成功，说明票据确实为可信第三方颁发。
- 服务器比较以下三项内容：
  - 票据中的用户名与客户端提供的用户名是否一致，由此防止攻击者使用他人的票据。
  - 票据中的IP地址与客户端IP地址是否一致，由此防止攻击者假冒客户端。
  - 票据中包含的服务名与自己的服务名是否一致，由此防止用访问其他服务的票据来访问自身的服务。

Kerberos协议

引入票据许可服务器

- 客户端首先向AS证实自己的身份，并获取一张票据许可票据（Ticket GrantingTicket，TGT），该票据可重用。
- 当需要获取访问某项应用服务的票据时，客户端向**票据许可服务器**（Ticket Granting Server，TGS）提出请求，并将TGT作为自己的身份凭证。
- 在向TGS证实用户身份时，客户端仅传输用户名。TGS以该用户名为关键字在本地库中查找相应密钥，并用其加密TGT，之后返回给客户端。通过上述途径，避免了明文口令的传输。

Kerberos协议

引入时间参数

- 为提高通信效率，Kerberos票据可重用，即同一用户可以多次使用某个票据。票据生命期不能设置为无限长。

为描述票据的有效期， Kerberos在票据中加入两个时间参数：

- **生命期**：描述票据的有效期限。
- **时间戳**：描述票据的颁发时间。

票据：{客户端用户名 | 客户端主机IP地址 | 应用服务名 | 生命期 | 时间戳}

Kerberos协议

- **引入会话密钥和认证符：**可信第三方在为用户颁发票据的同时，还将为其和应用服务器生成共享的会话密钥。用户在访问应用服务器时需证明自己拥有该会话密钥，这通过认证符实现。
  - 第三方将会话密钥发送给客户端，同时将会话密钥包含在票据中以通过客户端发送给服务器，由此实现**会话密钥的共享**。密钥分发时分别用用户和服务器的密钥加密，由此确保其安全性。
  - 服务器收到客户端请求后，首先用自己的密钥解密票据即可获取**会话密钥**，随后用会话密钥解密认证符。若解密成功，说明用户拥有相应的会话密钥。
  - 服务器将解密票据所获取的客户端**用户名、IP地址**与解密认证符所获取的这两项信息进行比较，若一致，则客户端用户身份认证通过。
  - 服务器检查票据中包含的票据**生存期及时间戳**以确保这个票据确实还在有效期内。

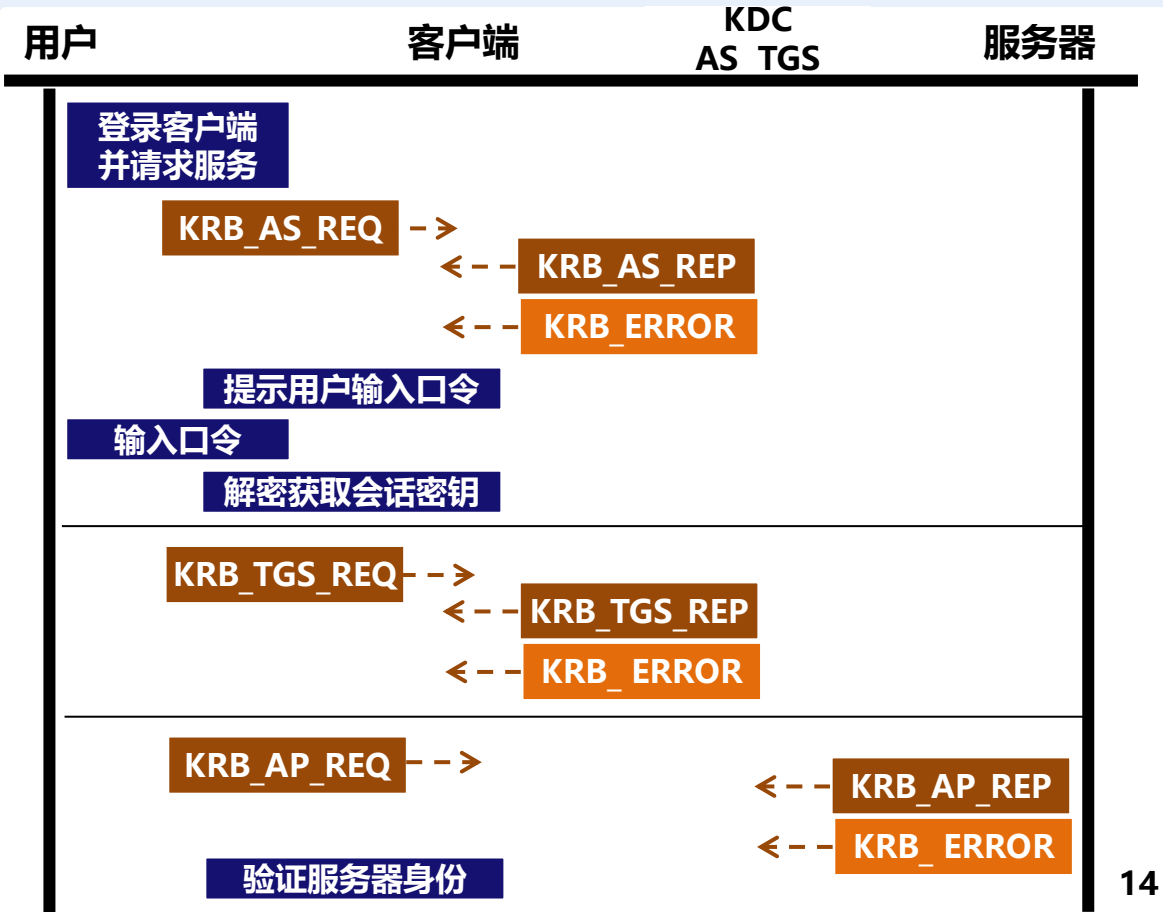
Kerberos协议

实现双向认证

- 客户端向服务器发送请求后并非立即开始应用通信，而是要等待服务器返回一个应答，包含用会话密钥加密的信息。
- 如果客户端能够正确解密该信息，说明服务器拥有正确的会话密钥，从而验证了服务器的身份。
- 除验证用户和服务器的身份外，会话密钥也可用于保护随后通信数据的机密性、完整性，或者用于通信双方交换子密钥。

Kerberos协议

- 主要流程
  1. 获取票据许可票据TGT
  2. 获取应用服务票据
  3. 访问应用服务

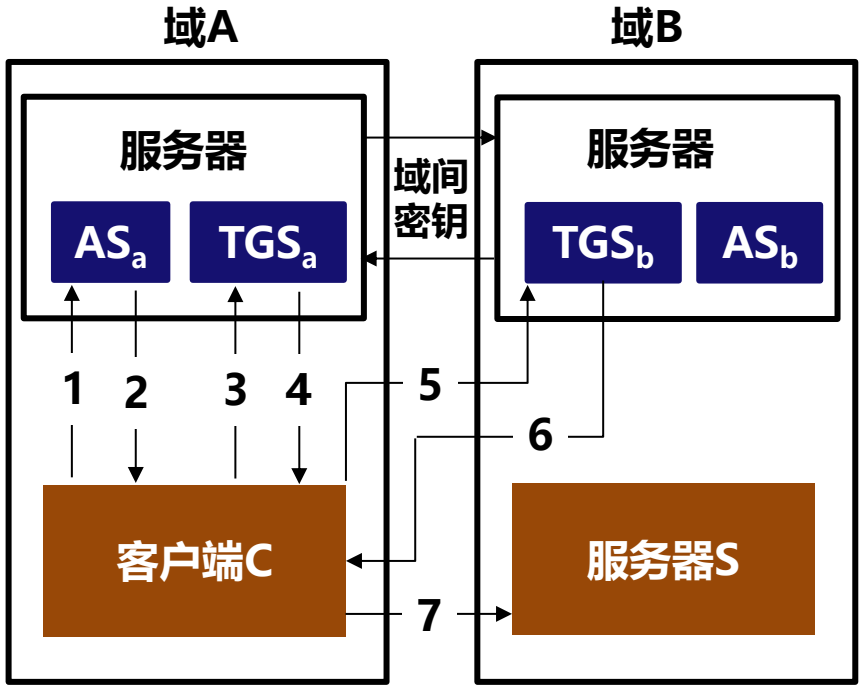


Kerberos协议

- Kerberos跨域认证：
  - Kerberos认证系统包括：多个使用Kerberos认证服务的用户（客户端）和服务器，至少一个AS和TGS。
  - 每个组织或单位都可能建立一个Kerberos认证系统，该系统称为“域”。

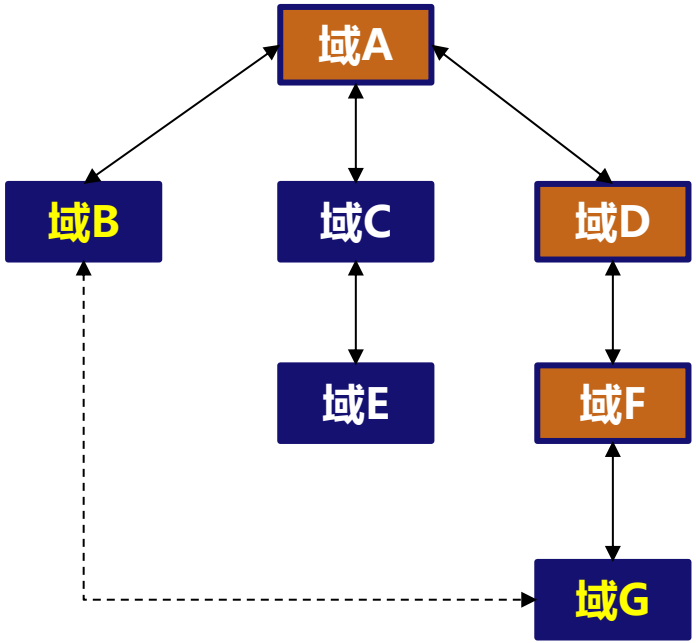
Kerberos协议

- Kerberos跨域认证：**跨越单个域**
  - 访问AS_a以获取访问票据许可服务器TGS_a的票据许可票据TGT_{tgsa}；
  - 以TGT_{tgsa}为凭证，访问TGS_a，以获取访问TGS_b的TGT_{tgsb}
  - 以TGT_{tgsb}为凭证，访问TGS_b，以获取访问服务器的票据$Ticket_s$
  - 以$Ticket_s$为凭证，访问域B的服务器S



Kerberos协议

- Kerberos跨域认证：**跨越多个域**
  - 在实际网络中会存在多个域，Kerberos允许跨越多个中间域进行认证，这些域之间构成了一个认证链，每两个直接跨域认证的域之间都共享域间密钥。



Kerberos协议

- **用户到用户U2U认证：**

  Kerberos使用的密钥可被分为两类：长期密钥和短期密钥。

  - **用户-Kerberos服务器，以及应用服务器-Kerberos服务器之间的共享密钥称为长期密钥，因为它们可能在很长一段时间内保持不变。**
  - **会话密钥则属于短期密钥。**

- **当客户端向TGS请求访问应用服务器的票据时，同时出示自己和服务器的TGT。**

  - **TGS同时验证这两个票据及认证符，认证成功后用服务器TGT中包含的会话密钥加密新票据，并返回给客户端。**

提纲

一、Kerberos协议流程

二、Kerberos票据和认证符

三、Kerberos消息

二 Kerberos票据和认证符

- 选项和标志
  - **初始认证**：与初始认证相关的选项和标志包括INITIAL、PRE-AUTHENT、HW-AUTHENT、OPT-HARDWARE-AUTH。
  - **可更新票据**：在设置票据有效期时应综合权衡效率和安全性。
  - 可推迟票据
  - 无效票据
  - 代理功能
  - 跨域认证策略
  - U2U使用模式

二 Kerberos票据和认证符

- 票据构成

Kerberos票据
tkt-vno（票据版本）
realm（服务器域）
sname（服务器名）

enc-part（加密区域）
flags（标志）
key（会话密钥）
crealm（客户端域）
cname（客户端实体名）
transited（传输编码）
authtime（认证时间）
starttime（起始时间*）
endtime（终止时间）
renew-till（更新终正时间*）
caddr（主机地址*）
authorization-data（认证数据）

二 Kerberos票据和认证符

- 认证符
  - 整个认证符使用会话密钥加密处理。

authenticator
authenticator-vno（认证符版本）
crealm（客户端域）
cname（客户端实体名）
chsum（校验和*）
cusec（客户端当前秒数）
ctime（客户端时间戳）
subkey（子会话密钥*）
seq-number（序号*）
authenticator-data（认证数据*）

提纲

一、Kerberos协议流程

二、Kerberos票据和认证符

三、Kerberos消息

三 Kerberos消息

- 消息交换
  - 认证服务交换：
    - KRB_AS_REQ、 KRB_AS_REP、 KRB_ERROR
  - 票据许可服务器TGS交换：
    - KRB_TGS_REQ 、 KRB_TGS_REP、KRB_ERROR
  - 应用服务认证交换
    - KRB_AP_REQ 、 KRB_AP_REP、KRB_ERROR
  - 安全交换：KRB_SAFE
  - 机密交换：KRB_PRIV
  - 信任状交换：KRB_CRED

三 Kerberos消息

- 认证服务交换
  - 一是客户端在初始认证时向AS申请信任状，此时获取的通常是TGT；
  - 二是用于应用服务器需绕过TGS，直接确认用户掌握其秘密信息的场合。
- 一个典型的实例就是口令更改服务，若客户无法证明其知道原口令，则应用服务器会拒绝其请求。

三 Kerberos消息

- TGS交换
  - 客户端需要获取访问某个应用服务器的信任状；
  - 客户端需要更新/有效化已有的票据；
  - 客户端需获取一张代理票据。
- 应用服务认证交换
  - 在获取访问应用服务器的信任状后，客户端即可开始应用服务认证交换。

三 Kerberos消息

- 安全交换
  - 安全交换用于检测通信双方交换的消息是否被更改。该功能的实现依托KRB-SAFE消息中包含的冲突检测校验和（cksum）。
  - 当应用需要进行该项检测时，可搜集应用相关数据及控制数据并计算校验和。
  - 控制数据包括时间戳、序号以及发送方地址等。

三 Kerberos消息

- 机密交换
  - 当某个通信方保障消息的机密性和完整性时，它使用机密性交换，对应KRB_PRIV消息。
  - 该消息中包含应用数据和控制信息，并进行加密处理。
  - 序号和时间戳字段必须至少包含其一。

三 Kerberos消息

- 信任状交换
  - 信任状交换使用KRB-CRED消息，其中包含一系列票据以及与票据有关的其他信息，这些信息被加密处理。
  - 当某个应用收到KRB-CRED消息后，它会对其进行验证。
  - 验证过程与机密交换的前四项检查类似。

三 Kerberos消息

- 用户到用户U2U认证交换
  - 使用U2U认证交换时，客户端必须首先通过一条消息获取密钥分发中心KDC颁发给服务器的TGT，该消息的形式由具体应用指定。
  - U2U交换过程：
    - 应用服务器向客户端发送TGT；
    - 客户端向KDC发送KRB-TGS-REQ消息；
    - KDC向客户端返回KRB-TGS-REP消息；
    - 客户端向应用服务器发送KRB-AP-REQ消息。

小结

- Kerberos提供了用户级的身份认证功能，基于对称密码体制和可信第三方，其思想如下：
  - 用户与第三方、服务器与第三方分别共享密钥。当用户请求服务器的服务时，其所在的客户端代表其向第三方提供用户名，第三方则返回用于访问服务器的票据并为其和服务器生成一个共享的会话密钥。
  - 票据中包含会话密钥、用户名、客户端地址以及生命期等控制信息，并使用服务器密钥加密；会话密钥则使用客户端密钥加密。
- 在请求服务器认证用户身份时，客户端向服务器提供票据及认证符。认证符中包含了时间戳，并使用会话密钥加密。

小结

- Kerberos协议包括AS交换、TGS交换、应用服务交换。
  - 第一步：用以访问AS以获取访问TGS的TGT
  - 第二步：利用TGT访问TGS以获取访问应用服务的票据
  - 第三步：利用该票据访问应用服务。
- Kerberos还实现了跨域认证等功能，使得一个域的客户端访问另一个域的服务器成为可能。此时每个域的Kerberos服务器都与另一个域建立共享密钥，并注册为另一个域的实体。

办公地点：理科大楼B1209

联系方式：17621203829

邮箱：liuhongler@foxmail.com