CS 465 Computer Security

Kerberos

Kent Seamons
Student Learning Goals

- Understand Kerberos design
  - You do not need to memorize the protocol definitions in Tables 4.1 and 4.3. I will give them to you on an exam. You should be able to explain each element in the messages and its purpose (K4 and K5).

- What are the significant threats to Kerberos and how are they countered?
Why Study Kerberos?

- It has been in use for 20+ years
- Integrated with real systems
  - Windows 2000
  - Andrew File System (AFS)
  - Distributed Computing Environment (DCE)
- Example of a complete solution to the problem of authentication in open networks
Kerberos

- What is Kerberos?
  - An authentication service developed at MIT
  - Solves the problem of authentication between workstations and services in an open distributed environment
  - Centralized authentication server used to authenticate users to servers and servers to users
  - Uses symmetric encryption (initial design)

- Threats
  - Impersonation
    - Gain access to another person’s workstation
    - Change network address of a workstation
  - Eavesdropping
    - Replay
    - Offline attacks on message contents
Design Goals

- Secure
  - Eavesdropper should not be able to obtain enough information to impersonate a user
- Reliable
- Transparent
  - User should only have to enter password
- Scalable
  - Support a large number of clients and servers
Simple Protocol (1)

(1) C -> AS: \[ \text{ID}_c \ | \ | \ P_c \ | \ | \ \text{ID}_v \]

(2) AS -> C: \[ \text{Ticket} \]

(3) C -> V \[ \text{ID}_c \ | \ | \ \text{Ticket} \]

\[ \text{Ticket} = E_{k_v} [ \ | \ | \ \text{ID}_c \ | \ | \ \text{AD}_c \ | \ | \ \text{ID}_v ] \]

\[ C = \text{client} \quad P = \text{password} \]
\[ \text{AS} = \text{authentication server} \quad \text{AD} = \text{network address} \]
\[ V = \text{server} \quad K = \text{secret encryption key} \]
\[ \ | \ | = \text{concatentation} \]
\[ \text{ID} = \text{identifier} \]
Simple Protocol (1)

- Problems
  - User must enter password repeatedly for multiple services
  - Plaintext pw transmission
Simple Protocol (2)

Once per user logon session:
(1) C -> AS: \( ID_c \mid ID_{tgs} \)
(2) AS -> C: \( E_{k_c}[Ticket_{tgs}] \)

Once per type of service:
(3) C -> TGS \( ID_c \mid ID_v \mid Ticket_{tgs} \)
(4) TGS -> C \( Ticket_v \)

Once per service session:
(5) C -> V \( ID_c \mid Ticket_v \)

\[ Ticket_{tgs} = E_{k_{tgs}}[ID_c \mid AD_c \mid ID_{tgs} \mid TS_1 \mid Lifetime_1] \]
\[ Ticket_v = E_{k_v}[ID_c \mid AD_c \mid ID_v \mid TS_2 \mid Lifetime_2] \]
Simple Protocol (2)

- Problems
  - Attacker can replay a ticket from spoofed network address
  - No server authentication
Table 4.1 Summary of Kerberos Version 4 Message Exchanges

(a) Authentication Service Exchange: to obtain ticket-granting ticket

1. $C \rightarrow AS$: $ID_c \parallel ID_{tgS} \parallel TS_1$

2. $AS \rightarrow C$: $E_{K_c} [K_{c,tgS} \parallel ID_{tgS} \parallel TS_2 \parallel Lifetime_2 \parallel Ticket_{tgS}]$

   $Ticket_{tgS} = E_{K_{tgS}} [K_{c,tgS} \parallel ID_C \parallel AD_C \parallel ID_{tgS} \parallel TS_2 \parallel Lifetime_2]$

(b) Ticket-Granting Service Exchange: to obtain service-granting ticket

3. $C \rightarrow TGS$: $ID_v \parallel Ticket_{tgS} \parallel Authenticator_c$

4. $TGS \rightarrow C$: $E_{K_{c,tgS}} [K_{c,v} \parallel ID_v \parallel TS_4 \parallel Ticket_v]$

   $Ticket_{tgS} = E_{K_{tgS}} [K_{c,tgS} \parallel ID_C \parallel AD_C \parallel ID_{tgS} \parallel TS_2 \parallel Lifetime_2]$

   $Ticket_v = E_{K_v} [K_{c,v} \parallel ID_C \parallel AD_C \parallel ID_v \parallel TS_4 \parallel Lifetime_4]$

   $Authenticator_c = E_{K_{tgS}} [ID_C \parallel AD_C \parallel TS_3]$

(c) Client/Server Authentication Exchange: to obtain service

5. $C \rightarrow V$: $Ticket_v \parallel Authenticator_c$

6. $V \rightarrow C$: $E_{K_{c,v}} [TS_5 + 1]$ (for mutual authentication)

   $Ticket_v = E_{K_v} [K_{c,v} \parallel ID_C \parallel AD_C \parallel ID_v \parallel TS_4 \parallel Lifetime_4]$

   $Authenticator_c = E_{K_{c,v}} [ID_C \parallel AD_C \parallel TS_5]$
Kerberos

- The Authorization Server and the Ticket Granting Server form a Key Distribution Center (KDC)
- Kerberos depends on a distributed time service (timestamps)
Figure 4.1 Overview of Kerberos
Figure 4.2  Request for Service in Another Realm
Kerberos V5

- Pre-authentication
  - What is it?
  - What attack does it prohibit?
  - What are its limitations? (see required reading article)

- Including the network address in the ticket does not work with NAT
  - Solution – drop the network address from the ticket
  - What vulnerability does this expose? How is it addressed?
Review Questions

- What are two ways an attacker can obtain sample ciphertext from messages 1 or 2 that can be used for an off-line attack? Explain how Kv5 addresses one of the attacks.
- What is the purpose of the authenticator in message #3? In message #5?
- What is the effect if we remove the authenticator in message #3?
- Explain how mutual authentication is achieved in each pair of messages in Kerberos.
- What is the Key Distribution Center (KDC)?