МЕРЕЖНИЙ ПРОТОКОЛ АУТЕНТИФІКАЦІЇ KERBEROS V5

Алещенко Ю.А.
Науковий керівник – к.т.н., доц., с.н.с. Огар В.І.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. КРіСТЗІ, тел. (057) 702-14-30),

The paper examines the Kerberos v5 network authentication protocol, developed in the 1980s by the Massachusetts Institute of Technology (MIT), which is tailored to protect information on an enterprise computer network. Kerberos uses private key cryptography, usually using DES or Triple-DES (3DES) encryption

Для аутентифікації в службі Kerberos використовуються посвідчення. Розрізняються два види посвідчень (credentials):

– мандати (tickets)

– аутентифікатори (authenticators).

Мандат використовується для безпечної передачі даних про клієнта.

Мандат Kerberos має наступну форму:

$$T_{C,S} = s, E\left(K_s, \left[c, a, v, K_{C,S}\right]\right),$$

де s – сервер, c – клієнт, a – мережевий адрес клієнта, v – початок та закінчення часу дії мандату, K_s – секретний ключ сервера, $K_{C,S}$ – сеансовий ключ для клієнта та сервера, $T_{C,S}$ – мандат клієнта на використовування сервера. Запис $E(K, [d])$, означає, що деякі дані d, зашифровані ключем K. Клієнт не може розшифрувати мандат, так як не знает секретного ключа сервера, але він може пред'являти його серверу необмежену кількість разів протягом дії мандату.

Аутентифікатор – деякий блок інформації, зашифрований за допомогою секретного ключа. Аутентифікатор пред'являється разом з мандатом. Клієнт створює аутентифікатор кожний раз, коли йому необхідно використовувати служби сервера.

Аутентифікатор Kerberos має наступну форму:

$$A_{C,S} = E\left(K_{C,S}, [C, t]\right),$$

де s – сервер, c – клієнт, t – початок та закінчення часу дії мандату, $K_{C,S}$ – сеансовий ключ для клієнта та сервера, $A_{C,S}$ – аутентифікатор клієнта та сервера. На відміну від мандату, аутентифікатор використовується тільки один раз, зміст цього блоку даних повинно змінюватися при кожному новому сеансі, інакше зловмисник може проникнути в систему, використовуючи перехоплене повідомлення.

Схема роботи протокола Kerberos продемонстрована на рис.1. Виділяють три основні стадії:

- Клієнт запрошує у сервера аутентифікації мандат на звернення до сервера видачі мандатів (Ticket-Granting Server, TGS). В ролі сервера аутентифікації виступає центр розподілу ключів (Key Distribution Center,

KDC). KDC направляє клієнту мандат, що містить унікальний сеансовий ключ (session key) для майбутнього сеансу. Копія сеансового ключа, пересилається на сервер, шифрується з допомогою довготривалого ключа цього сервера (кроки 1-2);

- Для підключення до конкретного серверу клієнт запрошу у TGS мандат на запит до серверу. В ролі TGS також виступає KDC. Якщо дані - вірні, KDC відправляє мандат клієнту (кроки 3-4);
- Клієнт пред'являє серверу отриманий мандат разом з аутентифікатором. Якщо посвідчення клієнта правильне, сервер надає клієнту доступи до служб (кроки 5-6).

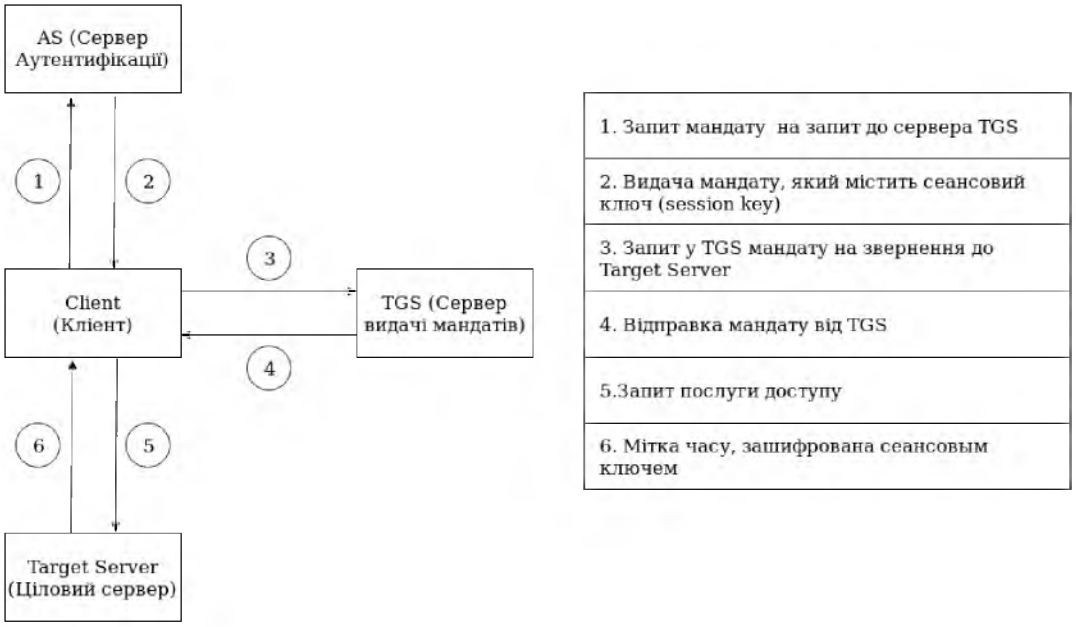

Рисунок 1 - Схема роботи протокола Kerberos