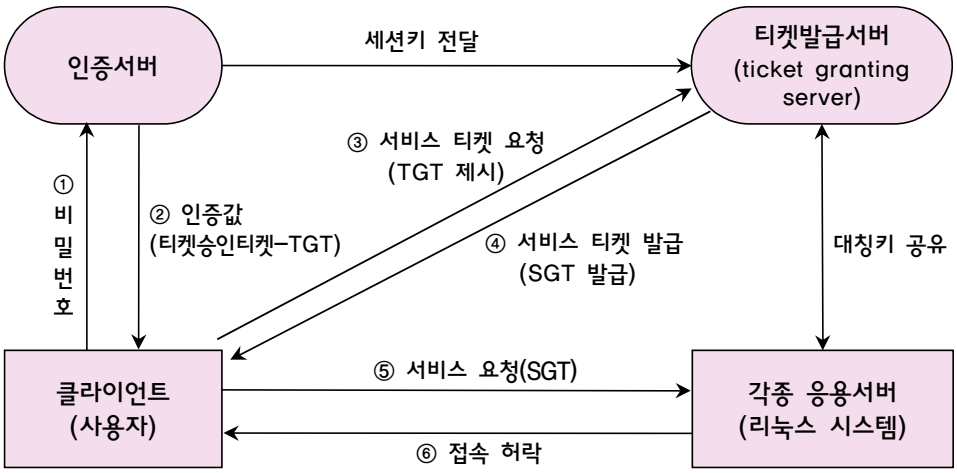
3. 커버로스(Kerberos)

- 커버로스는 네트워크상에서 **사용자 인증** 서비스를 제공하는 대표적인 메커니즘이다.
- 커버로스는 **키-분배센터**(KDC)이며, 동시에 **중앙집중식 인증 프로토콜**이다.
- Windows 2000, 리눅스 등 많은 시스템에서 커버로스를 응용한다.

◉ **커버로스 시스템 구조**



- 클라이언트 : 네트워크 사용자 컴퓨터
- 인증서버 : 클라이언트를 인증하는 인증서버(authentication server, AS)
- 티켓발급서버 : 클라이언트에게 티켓을 발급하는 컴퓨터(TGS)
- 응용서버 : 클라이언트가 접속하려는 컴퓨터(TGS가 발급한 티켓이 필요, **실질서버**)

① 커버로스는 기본적으로 티켓(ticket) 인증 방식의 대칭키 기반 키 확립 프로토콜이다.

- 키 확립을 위해 **"일회용 세션키"**가 사용된다.
- 매 세션마다 세션키를 확립하는 것은 많은 비용이 필요하다.
- 따라서, 확립된 세션키를 일정기간 동안 사용하는 방식을 채택한다.
- 이와 같은 원리를 티켓(ticket) 방식이라 한다.
- 커버로스는 **클라이언트-서버** 프로그램으로 설계되었다.

② 티켓승인티켓에는 세션키의 용도와 유효기간 등이 포함되어 있다.(암호 형태)

③ 커버로스는 분산환경에서 대칭키를 이용하는 중앙집중식 인증 방식이다.

- 인증서버는 사용자를 인증해주는 서버이며, 사용자는 인증서버와 대칭키를 공유한다.
- **인증값**은 서비스 티켓을 승인 받기 위한 **티켓승인티켓(TGT)**이다.
- 인증서버가 사용자에게 발급한 TGT는 재사용 할 수 있다.**(TGT는 한번만 발행)**
- TGT는 특정 응용 서비스를 사용하기 위한 **다른 티켓(SGT)**을 얻는 데 필요하다.

TGT(여권)	• TGT는 **여권처럼** 사용자의 신원을 확인하며, **다수**의 SGT를 얻을 수 있도록 한다.
SGT(비자)	• SGT(Session Granting Ticket)는 네트워크의 **응용서버**를 사용하기 위한 것이다.

⑤ 통상적으로, 인증서버와 티켓발급서버는 하나의 같은 컴퓨터에서 운용되고 있다.

- 인증서버와 티켓발급서버가 커버로스 서버이며, 곧 KDC이다.
- 티켓발급서버는 각종 응용서버와 대칭키를 공유한다.

⑥ 응용서버는 실제로 사용자에게 각종 서비스를 제공하는 네트워크의 서버들이다.

- 응용서버는 telnet, ftp 같은 서비스를 제공하는 서버들이다.
- 즉, ftp, telnet, rcp, rlogin, rsh, ssh 등은 커버로스 기반 응용프로그램들이다.

⑦ 커버로스는 싱글사인온(Single Sign On) 인증 방식으로 구현된다.

- 인증서버와 응용서버 사이에 티켓발급서버를 두면, 인증 횟수를 최소화 할 수 있다.
- 사용자의 비밀번호를 기반으로 하는 인증 과정을 인증서버와 한 번 성공하면,
- 사용자는 또 다시 비밀번호를 입력하지 않고
- 인증값(TGT)을 이용하여 각종 응용서버에 접속할 수 있는 티켓들을 발급받을 수 있다.

⑧ 커버로스는 내부적으로 키-분배센터(KDC, Key Distribution Center)를 운영한다.

- 커버로스는 **인증 프로토콜**이며, 동시에 **키-분배센터**(KDC)이다.
- KDC에는 모든 참가자들의 비밀키와 계정이 보관되어 있다.(매우 중요함)
- KDC에 오류가 발생하면 전체 서비스를 사용할 수 없다.

⑨ 커버로스 시스템은 타임스탬프를 이용하여 메시지들의 전후 순서를 보장한다.

- 시스템 간에 클록 동기화가 요구되는 시스템이다.
- 커버로스 시스템은 **타임스탬프**를 이용하여 **재전송 공격(replay attack)**을 막는다.

⑩ 커버로스는 Needham-Schroeder 프로토콜에 기반한다.

- Version 5 : Version 4의 보안 결함을 수정, 지금은 Version 5를 사용한다.

커버로스(Kerberos)

– 버전 4와 버전 5 비교

버전 4의 한계와 버전 5의 등장
버전 4에 어떤 문제점이 있고 버전 5에서는 어떻게 보완했는지 살펴본다.

---

① **버전 4**는 **DES 암호** 알고리즘 사용으로 제한되어 있었다.
- 현재, DES 암호 알고리즘은 다른 암호 알고리즘에 비해 보안강도가 떨어진다.
- **버전 5**에는 클라이언트와 서버가 통신할 때, 알고리즘을 선택하는 프로토콜이 추가되었다.
- **버전 5**에서는 **모든 대칭키 암호 알고리즘을 사용**할 수 있다.

② 티켓의 유효기간
- 버전 4는 티켓의 유효기간에 **제한을 둔다.**
  → 티켓 유효기간(Lifetime)은 5분 단위로 하고, 8bit를 사용하여 부호화를 한다.
  → 표시할 수 있는 최대유효기간은 2^8 × 5 = 1280분이다.
  → 약 21시간 정도이다.
  → 장시간의 유효기간을 필요로 하는 시스템에는 부적합하다.
- 버전 5는 티켓의 유효기간에 특별한 **제한을 받지 않는다.**
  → 버전 5에서는 티켓의 유효시작시간과 만료시간을 설정할 수 있다.

③ 버전 4는 IP **프로토콜**에서만 가능하다.
- 버전 4는 ATM이나 ISO와 같은 다른 종류의 프로토콜을 고려하지 않았다.
  서로 다른 기종의 네트워크 사이에는 호환이 불가능하였다.
- 버전 5에서는 네트워크 유형도 설정할 수가 있다.
  → 버전 5는 대부분의 네트워크 사이의 **호환성**을 제공한다.

④ 버전 4는 외부 공격에 취약하다는 것이 증명되었다.
- 버전 4에서는 PCBC(Propagating Cipher Block Chaining)라고 하는
  비 표준모드의 암호문 블록을 교환하는 기법을 사용하였기 때문이다.
- 버전 5에서는 표준모드인 CBC 기법을 사용하도록 보완하였다.

커버로스(Kerberos)에서 인증 절차

커버로스에서 가장 단순한 인증 절차를 하나 살펴본다.

C → AS : IDc || Pc || IDv	클라이언트(C)가 인증서버로(AS)로 자신의 아이디와 비밀번호(password), 그리고 접속할 서버를 선택하여 입력한다.
⇓	
AS → C : Ticket	인증서버(AS)는 클라이언트(C) 정보를 확인하고, 유효한 정보이면 클라이언트에게 서버 이용 티켓(Ticket)을 발급한다.
⇓	
C → V : IDc || Ticket	클라이언트(C)는 발급 받은 티켓으로 응용서버(V)의 서비스를 이용할 수 있다.

◉ **용어 정리**

- IDc(Identifier of user on client) : 클라이언트(사용자)의 아이디
- Pc(Password of user on client) : 클라이언트(사용자)의 비밀번호
- IDv(Identifier of server) : 서버의 아이디(서버마다 구분되는 아이디가 존재)
- Ticket = EKv[IDc || Pc || IDv] → EKv는 암호화한 상태를 의미한다.
- Kv : 인증서버(AS)와 서버(V)간의 공유하는 대칭키(비밀키)
- V : 각종 서버를 지칭한다.
- || : 각종 정보를 이어서 붙여 쓰는 것을 의미한다.

◉ **커버로스(Kerberos) 장단점**

장점	• 커버로스는 데이터의 기밀성을 보장한다. → 통신 내용을 암호화 하므로 • 커버로스는 싱글사인온(Single Sign On) 인증 방식이다.
단점	• 키 분배 센터에 오류가 발생하면 전체 서비스를 사용할 수 없다. • 키 분배 센터가 단일 오류 지점(single point of failure)이 된다.

기출문제 분석

1. 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은? [2019년 국회 9급]

① 신뢰받는 제3자인 키 배포 기관이 구성원들 중간에 개입하는 방법이다.
② 커버로스는 세션키를 이용한 티켓 기반 인증 기법을 제공한다.
③ 토큰을 이용한 인증 프로토콜이다.
④ 인증서버가 사용자에게 발급한 티켓(즉, 티켓-승인 티켓)은 유효기간 내에 재사용할 수 있다.
⑤ 분산 시스템 환경에서 SSO(Single Sign On) 시스템을 구축할 수 없다.

♤ **커버로스(Kerberos)**

• 분산 시스템 환경에서 SSO(Single Sign On) 시스템을 구축할 수 없다.**(×)**
→ 커버로스는 SSO(Single Sign On)을 지원한다.

// 커버로스는 싱글사인온(Single Sign On) 인증 방식으로 구현된다.
• 인증서버와 응용서버 사이에 티켓발급서버를 두면, 인증 횟수를 최소화 할 수 있다.
• 사용자의 비밀번호를 기반으로 하는 인증 과정을 인증서버와 한 번 성공하면,
• 사용자는 또 다시 비밀번호를 입력하지 않고
• 인증값(TGT)을 이용하여 각종 응용서버에 접속할 수 있는 티켓들을 발급받을 수 있다.

정답 : ⑤

2. 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은? [2015년 지방 9급]

① 네트워크 기반 인증 시스템으로 공개키 기반구조를 이용하여 사용자 인증을 수행한다.
② 인증서버는 사용자를 인증하며 TGS(Ticket Granting Server)를 이용하기 위한 티켓을 제공한다.
③ TGS는 클라이언트가 서버로부터 서비스를 받을 수 있도록 티켓을 발급한다.
④ 인증서버나 TGS로부터 받은 티켓은 클라이언트가 그 내용을 볼 수 없도록 암호화되어 있다.

♤ **커버로스(Kerberos)**

• 네트워크 기반 인증 시스템으로 **공개키** 기반구조를 이용하여 사용자 인증을 수행한다.**(×)**
→ 커버로스는 티켓 인증 방식의 **대칭키** 기반 키 확립 프로토콜이다.

정답 : ①

3. 중앙집중식 인증 방식인 커버로스(Kerberos)에 대한 다음 설명 중 옳은 것은 무엇인가? [2016년 서울 9급]

① TGT(Ticket Granting Ticket)는 클라이언트가 서비스를 받을 때마다 발급 받아야 한다.
② 커버로스는 독립성을 증가시키기 위해 키 교환에는 관여하지 않아 별도의 프로토콜을 도입해야 한다.
③ 커버로스 방식에서는 대칭키 암호화 방식을 사용하여 세션 통신을 한다.
④ 공격자가 서비스 티켓을 가로채어 사용하는 공격에는 취약한 방식이다.

♤ **커버로스 시스템 구조**

• 커버로스는 티켓(ticket) 인증 방식의 **대칭키** 기반 키 확립 프로토콜이다.

① TGT(Ticket Granting Ticket)는 클라이언트가 서비스를 받을 때마다 발급 받아야 한다.**(×)**
→ TGT는 클라이언트가 **한번만 발급** 받으면 된다.
② 커버로스는 독립성을 증가시키기 위해 키 교환에는 관여하지 않아 별도의 프로토콜을 도입해야 한다.**(×)** → 커버로스 자체가 키를 분배하는 시스템이다.
④ 공격자가 서비스 티켓을 가로채어 사용하는 공격에는 취약한 방식이다.**(×)**
→ 서비스 티켓(SGT)에는 **타임스탬프**가 포함되어 있다.
→ 이 **타임스탬프**는 공격자의 **재전송 공격을 방지**한다.

정답 : ③

4. 다음에서 설명하는 용어는? [2022년 지방 9급]

○ 한 번의 시스템 인증을 통해 다양한 정보시스템에 재인증 절차 없이 접근할 수 있다.
○ 이 시스템의 가장 큰 약점은 일단 최초 인증 과정을 거치면,
모든 서버나 사이트에 접속할 수 있다는 것이다.

---

① NAC(Network Access Control)　② SSO(Single Sign On)
③ DRM(Digital Right Management)　④ DLP(Data Leak Prevention)

♤ **싱글사인온(SSO, single sign on) – 통합인증**

• SSO는 한 번의 인증으로 여러 컴퓨터의 자원을 이용할 수 있는 인증 방식이다.
• SSO는 통합인증, 단일 계정 로그인, **단일인증**이라고 한다.

정답 : ②

5. 커버로스(Kerberos) 버전 4에 대한 설명으로 옳지 않은 것은? [2022년 지방 9급]

① 사용자를 인증하기 위해 사용자의 패스워드를 중앙집중식 DB에 저장하는 인증 서버를 사용한다.
② 사용자는 인증 서버에게 TGS(Ticket Granting Server)를 이용하기 위한 TGT(Ticket Granting Ticket)를 요청한다.
③ 인증서버가 사용자에게 발급한 TGT는 유효기간 동안 재사용 할 수 있다.
④ 네트워크 기반 인증 시스템으로 비대칭 키를 이용하여 인증을 수행한다.

♤ **커버로스**

• 네트워크 기반 인증 시스템으로 **비대칭 키**를 이용하여 인증을 수행한다.(×)
→ 네트워크 기반 인증 시스템으로 **대칭 키**를 이용하여 인증을 수행한다.

정답 : ④

6. Single-Sign On을 실현하기에 적합한 기술로 가장 옳은 것은? [2021년 서울 7급]

① DTLS ② TLS
③ OCS ④ Kerberos

♤ **Single-Sign On**

• **커버로스**는 **싱글사인온**(Single Sign On) 인증 방식으로 구현된다.
• 사용자는 인증서버와 **한 번 인증**을 성공하면, 또 다시 비밀번호를 입력할 필요가 없다.
• **커버로스**는 네트워크상에서 **사용자 인증** 서비스를 제공하는 대표적인 메커니즘이다.

정답 : ④