ПРОТОКОЛЫ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Лекция 8

Распределение ключей

Два способа распределения ключей

1. Централизованное
2. Прямой обмен сеансовыми ключами

Основные механизмы, используемые для подтверждения подлинности:

- запроса-ответа (используется для аутентификации участников)
- временной штемпель (используется для аутентификации связи)

Достоинства и недостатки

- Достоинство схемы централизованного распределения ключей состоит в том, что ЦРК имеет больше возможностей генерации качественного ключа, нежели отдельный абонент, который может оказаться некрупной организацией или частным лицом, и не обязательно будет обладать таким оборудованием и квалифицированными специалистами, какие имеются в ЦРК.
- Недостатком централизованного распределения ключей является то, что факт компрометации ЦРК вызывает компрометацию всей ключевой информации, переданной через этот центр или хранимой в нем.

СХЕМА АУТЕНТИФИКАЦИ И ЦЕНТРАЛИЗОВАННОГО РАСПРЕДЕЛЕНИЯ СИММЕТРИЧНЫХ КЛЮЧЕЙ

Ключи хранятся в центре распределения ключей (ЦРК).

K_A - общий секретный ключ ЦРК и участника А

K_B - общий секретный ключ ЦРК и участника В

1. А→ЦРК : Id_A , Id_B
2. ЦРК →А: E_{KA} (T, L, K_s, Id_B , E_{KB} (T, L, K_s, Id_A))

   T – временная метка

   L –срок действия сеансового ключа Ks

   E – шифрование симметричное (например, по DES)

   K_s – сеансовый ключ
3. А →В: E_{KB} (T, L, K_s, Id_A), E_{KS} (T’, Id_A)

   E_{KS} (T’, Id_A) – часть, которая аутентифицирует А для В

   T’ – метка времени А
4. В →А: E_{KS} (f(T’)) – по схеме запрос- ответ, f(T’)= T’ -1

Система Kerberos

Система Kerberos разработана в рамках проекта Athena в Массачусетском технологическом институте.

Также как мифологический многоголовый (обычно трехголовый) пес (Кербер или Цербер), охраняющий царство мертвых Аида система Kerberos должна была иметь три компоненты защиты узла сети: аутентификацию, учет и аудит. Последние две «головы» так и не были реализованы.

Версия Kerberos 5 была принята в качестве стандарта IETF. Требования реализации протокола изложены в документе RFC 1510

IETF, IAB

Инженерный совет Интернета (Internet Engineering Task Force, **IETF**) — открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров, созданное IAB (Совет по архитектуре Интернета (Internet Architecture Board)) в 1986 году, которое занимается развитием протоколов и архитектуры Интернета.

Вся техническая работа осуществляется в рабочих группах IETF, занимающихся конкретной тематикой (вопросами маршрутизации, транспорта данных, безопасности и т.д.). Работа ведётся через почтовые рассылки, но трижды в году проводятся собрания IETF.

RFC - Request for Comments

Запрос комментариев (Request for Comments, **RFC**) — документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети.

Название «Request for Comments» ещё можно перевести как «заявка на обсуждение» или «тема для обсуждения». Публикацией документов RFC занимается IETF под эгидой открытой организации Общество Интернета (Internet Society, ISOC). Правами на RFC обладает именно Общество Интернета.

Система Kerberos

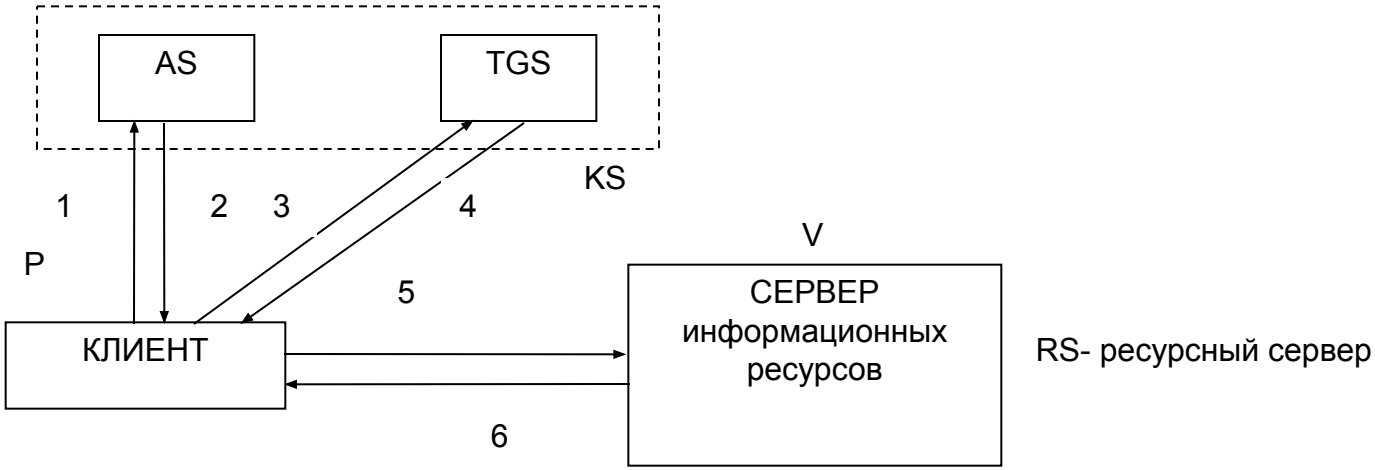
Kerberos в значительной степени основан на протоколе Нидхема-Шредера, но с двумя существенными изменениями:

Первое изменение протокола уменьшало количество сообщений пересылаемых между клиентом и сервером аутентификации.

Второе, более существенное изменение базового протокола, заключается в введении TGT (Ticket Granting Ticket — билет для получения билета) концепции, позволяющей пользователям аутентифицироваться на несколько сервисов используя свои доверительные данные только один раз.

СХЕМА АУТЕНТИФИКАЦИИ KERBEROS

(СИММЕТРИЧНАЯ)



AS – Аутентифицирующий сервер (типа ЦРК)
TGS – сервер выдачи разрешений (мандатов)
KS – сервер KERBEROS
K_{PG} – ключ для взаимодействия P и TGS (сеансовый)
K_{PV} – ключ для взаимодействия P и V

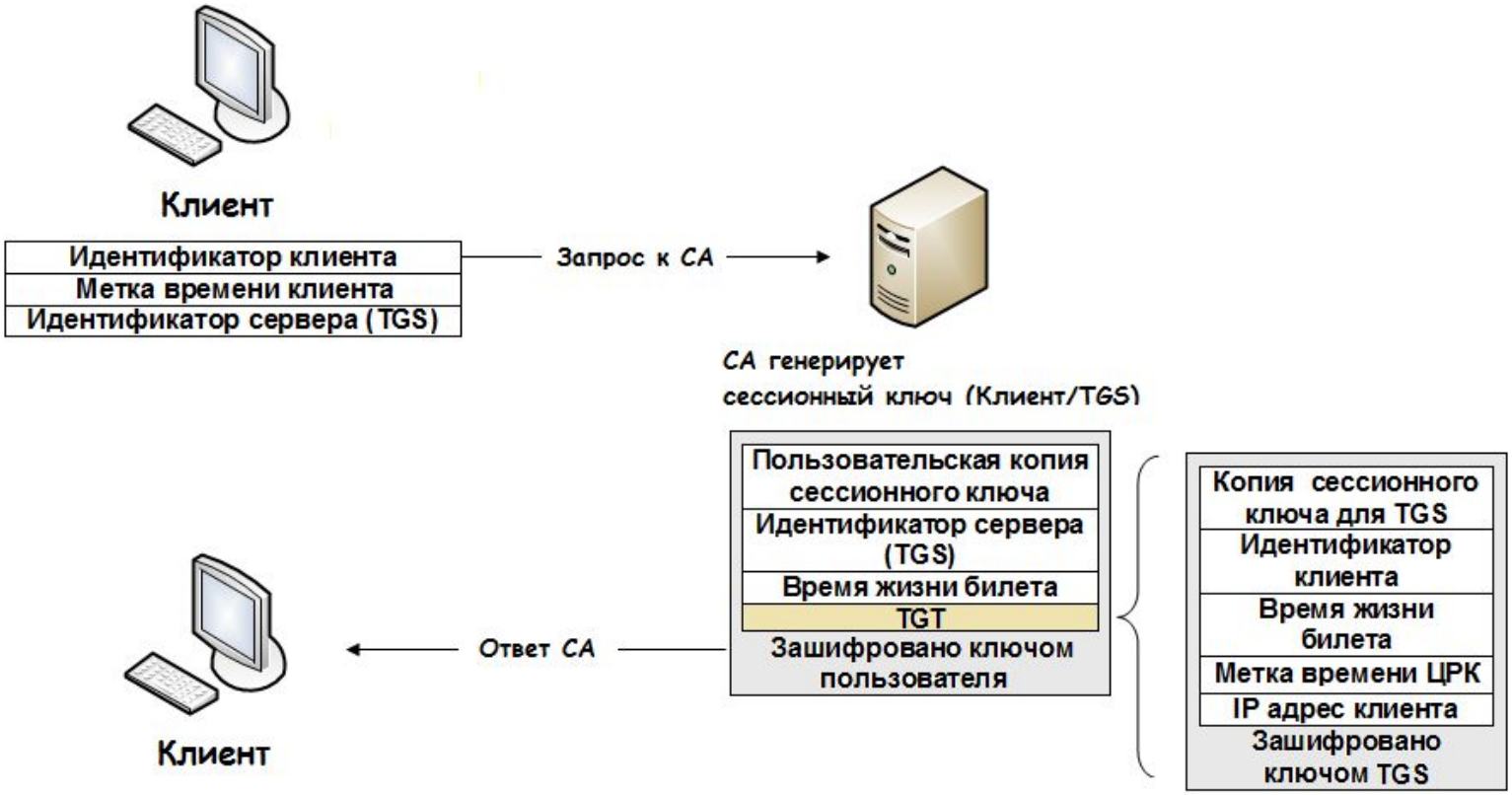
Kerberos 4

Kerberos 4 содержит два логических компонента: **Сервер аутентификации** (CA) и **сервер выдачи билетов** (TGS — Ticket Granting Server). Обычно эти компоненты поставляются как единая программа, которая запускается на центре распределения ключей (ЦРК — содержит базу данных логинов/паролей для пользователей и сервисов использующих Kerberos).

Kerberos 4

Сервер аутентификации выполняет одну функцию: получает запрос, содержащий имя клиента, запрашивающего аутентификацию, и возвращает ему зашифрованный TGT. Затем пользователь может использовать этот TGT для запроса дальнейших билетов на другие сервисы. В большинстве реализаций Kerberos время жизни TGT 8-10 часов. После этого клиент снова должен запросить его у CA.

Этап аутентификации клиента



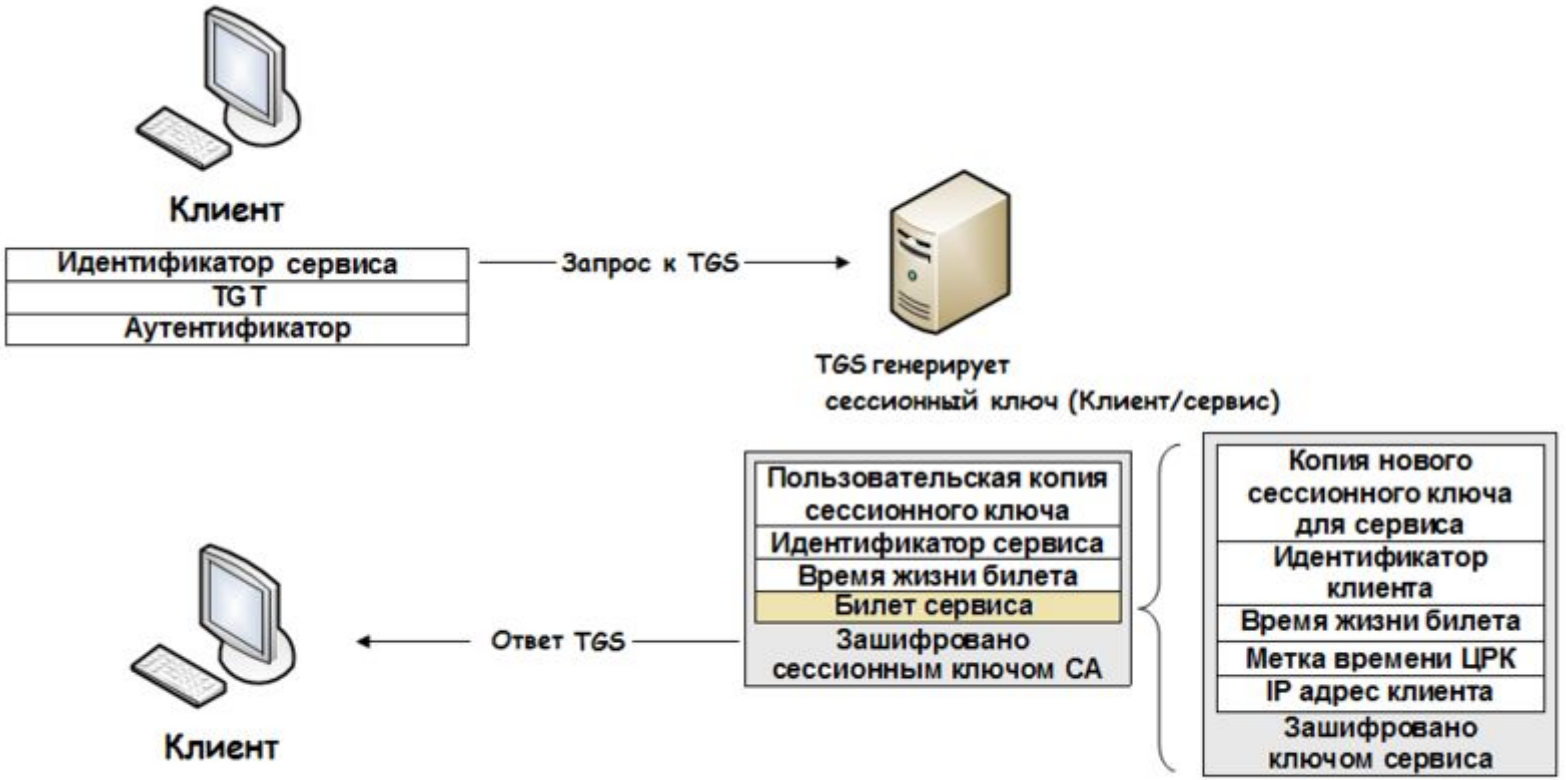
Запрос аутентификации (1)

- Первое сообщение, отправляемое центру распределения ключей — запрос к CA, так же известен как AS_REQ. Это сообщение отправляется открытым текстом и содержит идентификационные данные клиента, метку времени клиента и идентификатор сервера предоставляющего билет (TGS).

Запрос аутентификации (2)

Когда ЦРК получает AS_REQ сообщение, он проверяет, что клиент, от которого пришел запрос, существует, и его метка времени близка к локальному времени ЦРК (обычно ± 5 минут). Данная проверка производится не для защиты от повторов (сообщение посылается открытым текстом), а для проверки соответствия времени. Если хотя бы одна из проверок не проходит, то клиенту отправляется сообщение об ошибке, и он не аутентифицируется.

Запрос авторизации клиента



Авторизация на сервере выдачи разрешений

- В случае удачной проверки CA генерирует случайный сеансовый ключ, который будет совместно использоваться клиентом и TGS (данный ключ защищает дальнейшие запросы билетов у TGS на другие сервисы). ЦРК создает 2 копии сессионного ключа: одну для клиента и одну для TGS.

Авторизация на TGS

- Затем ЦРК отвечает клиенту сообщением сервера аутентификации (AS_REP) зашифрованным долгосрочным ключом клиента. Которое включает TGT зашифрованный TGS ключом (TGT содержит: копию сессионного ключа для TGS, идентификатор клиента, время жизни билета, метку времени ЦРК, IP адрес клиента), копию сессионного ключа для клиента, время жизни билета и идентификатор TGS.

ПРОТОКОЛ СИСТЕМЫ KERBEROS

1. P→AS : P, V-запрос разрешить обратиться к G Примеч.: G обозначает TGS, tkt_{PG} → TGT
2. AS →P: $E_P (T_{PG}, L_{PG}, K_{PG}, G, tkt_{PG})$- разрешение обратиться к TGS
   $tkt_{PG} = E_G (T_{PG}, L_{PG}, K_{PG}, P)$
3. P→ TGS : $E_{PG} (T_{PG}, P)$, V, tkt_{PG}- запрос на допуск к RS
   $E_{PG} (T_{PG}, P)$ – аутентифицирующая информация – удостоверение.
4. TGS →P: $E_{PG} (T_{PV}, L_{PV}, K_{PV}, V, tkt_{PV})$- разрешение на допуск к RS
   $tkt_{PV} = E_V (T_{PV}, L_{PV}, K_{PV}, P)$

ПРОТОКОЛ СИСТЕМЫ KERBEROS

5.P →V: E_{pv} (T_{pv},P), tkt_{pv} – запрос на получение информационного ресурса от RS

6.V→P: E_{pv} (T_{pv}) или E_{pv} (f(T_{pv}))= E_{pv} (T_{pv}-1) подтв. подл.V и получение информационного ресурса

Обозначения

T_{pg} - отметка времени при направлении информации от P к TGS

T_{pv} - отметка времени при направлении информации от P к V

E_V -шифрование на ключе, который знает только V и центр (AS)

E_G -шифрование на ключе, который знает только TGS и центр (AS)

E_P -шифрование на ключе, который знает только P и центр (AS)

L – время жизни ключа

ПРОТОКОЛ СИСТЕМЫ KERBEROS

- Действия 1,2 выполняются один раз для каждого сеанса пользователя.
- Действия 3,4 выполняются один раз для каждого типа сервиса.
- Действия 5,6 выполняются один раз для каждого сеанса сервиса.
- Клиент использует мандат при запросах мандатов многократного доступа к службам.

Сертификаты открытых ключей. Основные понятия

- **X.500** – стандарт службы каталогов.
- Рекомендации **X.509** Международного союза телекоммуникаций (ITU – International Telecommunication Union) – часть рекомендаций серии X.500. Появился в 1988 году. После исправлений – в 1993 году.
- **Обозначения:**
- **Y«X»** - удостоверение пользователя X, выданное центром сертификации Y
- **Y{I}** – подпись I объектом Y. Она состоит из I с добавленным шифрованным хэш-кодом.

СХЕМА ЦЕНТРАЛИЗОВАННОГО РАСПРЕДЕЛЕНИЯ ОТКРЫТЫХ КЛЮЧЕЙ (1)

А – инициатор, запрашивает выдачу сертификатов А и В.

1. А → ЦРК: Id_A, Id_B «Пришлите сертификаты А и В»

2. ЦРК → А: ЦРК передает А два сертификата:

$C_A = E_{K^C_{ЦРК}}(h(L_A, K^O_A, Id_A)), (L_A, K^O_A, Id_A); C_A = C_A\ \{L_A, K^O_A, Id_A\}$

$C_B = E_{K^C_{ЦРК}}(h(L_B, K^O_B, Id_B)), (L_B, K^O_B, Id_B). C_B = C_B\ \{L_B, K^O_B, Id_B\}$

А проверяет подлинность сертификата В и берет себе K^O_B . Свой ОК у него есть. Проверяет сертификат В путем:

- Проверить подпись;
- Проверить сроки L_A, L_B действия сертификатов C_A,C_B.

Успешная проверка подписи говорит о том, что информация подписана ЦРК и что ключ В K^0_B – подлинный.

Проверка сроков L_A, L_B используется для подтверждения актуальности сертификатов.

СХЕМА ЦЕНТРАЛИЗОВАННОГО РАСПРЕДЕЛЕНИЯ ОТКРЫТЫХ КЛЮЧЕЙ (2)

- **3**. A проверяет открытым ключом сертификат B
- $A \rightarrow B: C_A, E_K{}^{C}{}_{A}(T), E_K{}^{O}{}_{B}(r_1)$
- C_A – сертификат открытого ключа A
- $E_K{}^{C}{}_{A}(T)$ –для аутентификации A. $E_K{}^{O}{}_{B}(r_1)$ – для проверки подлинности B.
- r_1 – некоторое случайное число
- **4.** $B \rightarrow A: E_K{}^{O}{}_{A}(f(r_1))$
- $E_K{}^{O}{}_{B}$ - открытый ключ B, $E_K{}^{O}{}_{A}$ - открытый ключ A. Y {I}- подпись I объектом Y. Это I с добавленным шифрованным хэш-кодом