Министерство образования Республики Беларусь
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

ОТЧЁТ
к лабораторной работе №3
на тему

ПРОТОКОЛ KERBEROS

Выполнил: студент гр.253504
Фроленко К.Ю.
Проверил: ассистент кафедры информатики
Герчик А.В.

Минск 2025

СОДЕРЖАНИЕ

1 Формулировака задачи 3
2 Ход работы 4
Заключение 5

1 ФОРМУЛИРОВКА ЗАДАЧИ

В данной работе требуется разработать программное средство, реализующее протокол *Kerberos* для обеспечения безопасной аутентификации в клиент-серверной архитектуре. Программа должна демонстрировать ключевые этапы обмена данными между клиентом и сервером, который объединяет функции сервера аутентификации (*AS*), сервера выдачи билетов (*TGS*) и сервисного сервера. Основной целью является показ принципов работы *Kerberos*, где клиент запрашивает аутентификацию у *AS*, получает зашифрованный *Ticket Granting Ticket* (*TGT*), затем с помощью *TGT* обращается к *TGS* для получения билета для доступа к конкретному сервису, и, наконец, представляется этот билет сервисному серверу для подтверждения своей личности.

Реализация должна включать обмен зашифрованными сообщениями, используя упрощённые алгоритмы симметричного шифрования для демонстрации процессов шифрования и дешифрования данных. Программа должна обеспечивать возможность запуска сервера как отдельного сетевого процесса, который принимает запросы от клиента через сокеты, обрабатывая их в соответствии с этапами протокола. Клиентская часть, в свою очередь, должна последовательно выполнять запросы к различным компонентам сервера, выводя полученные сеансовые ключи и подтверждение аутентификации, а также отображать отладочную информацию для контроля хода выполнения операций.

Таким образом, итоговое решение должно не только демонстрировать корректное выполнение механизма *Kerberos*, но и предоставлять удобный способ отслеживания процесса обмена зашифрованными данными между клиентом и сервером, обеспечивая понимание основных принципов аутентификации в распределённых системах.

2 ХОД РАБОТЫ

При запуске серверного модуля в терминале выводятся отладочные сообщения, демонстрирующие выполнение ключевых этапов протокола *Kerberos*. Сервер, объединяющий функции аутентификации (*AS*), выдачи билетов (*TGS*) и подтверждения доступа сервису, генерирует сеансовые ключи, формирует *Ticket Granting Ticket* (*TGT*) и сервисный билет, а также выводит информацию о каждом из этих этапов.

Запуск клиентской части инициирует последовательную обработку запросов. Вначале клиент отправляет запрос к серверу *AS*, указывая свой идентификатор (например, «*client1*»). Сервер *AS*, используя предопределённый общий секрет, генерирует сеансовый ключ для связи с *TGS* и формирует *TGT*, который шифруется и возвращается клиенту. Клиент расшифровывает полученное сообщение с помощью своего секретного ключа, извлекает сеансовый ключ для дальнейшего обмена с сервером *TGS* и сохраняет полученный *TGT*.

Затем клиент обращается к серверу *TGS*, передавая полученный *TGT* и идентификатор требуемого сервиса (например, «*fileserver*»). Сервер *TGS* дешифрует *TGT*, извлекает идентификатор клиента и исходный сеансовый ключ, генерирует новый сеансовый ключ для связи с сервисным сервером и формирует зашифрованный сервисный билет. Ответ от *TGS* шифруется с использованием сеансового ключа, полученного на предыдущем этапе, и возвращается клиенту. Клиент, расшифровывая сообщение, получает новый сеансовый ключ для сервиса и сервисный билет.

Заключительным этапом является отправка клиентом запроса к сервисному серверу с использованием полученного сервисного билета и нового сеансового ключа. Сервисный сервер, расшифровывая билет, проверяет подлинность клиента и возвращает подтверждение, содержащее идентификатор клиента. Этот результат свидетельствует о корректном выполнении всех этапов обмена зашифрованными сообщениями согласно протоколу *Kerberos*. На рисунке 1 представлен пример работы программы.

```
Kerberos-сервер запущен на localhost:12345
[AS] Для клиента client1:
     session_key = 8832be515bb5efad44bee27771a42897
     TGT_plain    = b'client1::\x882\xbeQ[\xb5\xef\xadD\xbe\xe2wq\xa4(\x97'
[TGS] Извлечён client_id: client1
[TGS] Извлечён session_key (из TGT) = 8832be515bb5efad44bee27771a42897
[TGS] Для сервиса fileserver:
     service_session_key = 52624f23d46438696de6b8919820f339
     service_ticket_plain = b'{"client_id": "client1", "service_session_key": "UmJPI9RkOGlt5riRmCDzOQ=="}'
[SERVICE] Подтверждён client_id: client1
```

Рисунок 1 – Пример работы программы

ЗАКЛЮЧЕНИЕ

В ходе данной работы было разработано программное средство, реализующее протокол *Kerberos* для обеспечения безопасной аутентификации в клиент-серверной архитектуре. Программа продемонстрировала ключевые этапы обмена зашифрованными сообщениями между клиентом и сервером, который объединяет функции сервера аутентификации (*AS*), сервера выдачи билетов (*TGS*) и сервисного сервера.

На начальном этапе была определена архитектура системы, выбран упрощённый алгоритм симметричного шифрования, позволяющий моделировать процессы шифрования и дешифрования данных на каждом из этапов аутентификации. Реализация обеспечила корректный обмен информацией: клиент отправляет запрос к серверу *AS*, получает зашифрованный *Ticket Granting Ticket* (*TGT*) и сеансовый ключ, затем с помощью *TGT* обращается к серверу *TGS* для получения сервисного билета, и, наконец, представляет билет сервисному серверу для проверки подлинности.

Представленный пример работы программы подтверждает, что система корректно формирует сеансовые ключи и билеты, а также выполняет проверку аутентификации клиента. Отладочные сообщения, выводимые сервером, позволяют наглядно проследить процесс формирования *TGT* и сервисного билета, что свидетельствует о надёжности и эффективности реализации протокола *Kerberos*.

Таким образом, поставленная задача была успешно решена. Разработанное средство демонстрирует основные принципы работы *Kerberos* и может служить основой для дальнейших исследований и развития механизмов безопасной аутентификации в распределённых системах.