Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

Факультет безопасности информационных технологий

Дисциплина:

«Теория информационной безопасности и методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

«Разграничение доступа. Идентификация и аутентификация»

Выполнил:

студент группы N3246,

Суханкулиев Мухаммет

(подпись)

Проверила:

Коржук Виктория Михайловна

(отметка о выполнении)

(подпись)

Санкт-Петербург

2024 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель работы – разработка подсистемы идентификации и аутентификации субъектов.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Составить алгоритм для реализации выбранной подсистемы.
2. Составить полную схему компьютерной системы со встроенной в нее подсистемой идентификации и аутентификации.

1 ХОД РАБОТЫ

1.1 Основные принципы реализации протокола Диффи-Хеллмана

Протокол Диффи-Хеллмана (1976 год) позволяет двум сторонам (А и Б) выработать общий секретный ключ, используя открытые каналы связи, что важно для безопасного обмена данными с использованием симметричного шифрования. Протокол основан на математической задаче вычисления дискретных логарифмов в конечных полях, что делает его сложным для взлома.

Основные шаги протокола:

1. **Договоренность о публичных параметрах:** Стороны А и Б договариваются о двух числах:
   - **Модуль N** (большое простое число).
   - **Примитивный элемент g** (число, степень которого образует множество всех чисел от 1 до N-1).
2. **Выбор секретных ключей:** Каждая сторона выбирает свой секретный ключ (случайное число меньше N).
   - $СК_{\boldsymbol{A}}$ (секретный ключ для А)
   - $СК_{\boldsymbol{B}}$ (секретный ключ для Б)
3. **Вычисление открытых ключей:** Стороны вычисляют открытые ключи на основе своих секретных ключей:
   - $ОК_{\boldsymbol{A}} = \boldsymbol{g}^{СК_A} \boldsymbol{mod\ N}$
   - $ОК_{\boldsymbol{B}} = \boldsymbol{g}^{СК_B} \boldsymbol{mod\ N}$
4. **Обмен открытыми ключами:** Стороны обмениваются этими открытыми ключами по незащищенному каналу связи.
5. **Вычисление общего секрета:**
   - Пользователь А вычисляет общий секрет:
     - $\boldsymbol{K} = (ОК_{\boldsymbol{B}})^{СК_A} \boldsymbol{mod\ N}$
   - Пользователь Б вычисляет общий секрет:
     - $\boldsymbol{K} = (ОК_{A})^{СК_B} \boldsymbol{mod\ N}$

Обе стороны получают одинаковый общий секрет K, который может использоваться как сеансовый ключ для симметричного шифрования данных.

Достоинства

- **Безопасность без защищенных каналов:** Протокол позволяет безопасно обмениваться ключами даже через незашифрованные каналы.
- **Отсутствие необходимости в предварительных секретах:** Нет нужды в заранее обмене секретной информацией между сторонами, что упрощает процесс.
- **Широкая применимость:** Протокол используется в различных системах (например, в SSL/TLS для безопасных соединений в интернете).
- **Простота реализации:** Алгоритм достаточно прост для реализации и понимания.

Недостатки и уязвимости

- Протокол сам по себе не обеспечивает аутентификацию сторон, что позволяет злоумышленнику (**MITM**) подменить открытые ключи во время обмена, если не используется дополнительная защита, например, цифровые сертификаты.

Атаке "человек посередине" подвержены не только открытые ключи, но и сам процесс обмена ключами. Злоумышленник может вмешаться и подменить открытые ключи.

- Протокол полагается на сложность вычисления дискретных логарифмов в конечных полях. Хотя это безопасно при больших числах, с развитием вычислительных мощностей и новых методов криптоанализа риск взлома возрастает.
- **Replay attacks:** Протокол не предусматривает встроенные механизмы защиты от повторного использования ранее переданных сообщений.
- Правильный выбор чисел N и g критичен для безопасности. Малые значения этих параметров могут привести к слабости системы.

1.2 Алгоритм реализации протокола Диффи-Хеллмана

Выбор публичных параметров:

- Публичный модуль N (большое простое число).
- Примитивный элемент g (целое число, степень которого образует группу чисел от 1 до N-1).
- Эти параметры являются общими для обеих сторон.

Выбор секретных ключей:

- Сторона А выбирает случайное число $СК_{\boldsymbol{A}}$ (секретный ключ для А).
- Сторона Б выбирает случайное число $СК_{\boldsymbol{B}}$ (секретный ключ для Б).

Вычисление открытых ключей:

- Сторона А вычисляет свой открытый ключ:

$$OK_A = g^{CK_A} \, mod \, N$$

- Сторона Б вычисляет свой открытый ключ:

$$OK_B = g^{CK_B} \; mod \; N$$

Обмен ключами: Стороны обмениваются своими открытыми ключами через незащищённый канал.

Вычисление общего секрета для обеих сторон:

- Сторона А вычисляет общий секрет $\boldsymbol{K_A}$:

$$K_A = (OK_B)^{CK_A} \; mod \; N$$

- Сторона Б вычисляет общий секрет $\boldsymbol{K_B}$:

$$K_B = (OK_A)^{CK_B} \; mod \; N$$

Из-за свойств степеней и модулей результат $\boldsymbol{K_A}$ и $\boldsymbol{K_B}$ будет одинаковым.

Использование общего секрета для симметричного шифрования: Полученный общий секрет может быть использован как ключ для симметричного шифрования для безопасного обмена данными между сторонами.

Важные замечания:

1. Протокол Диффи-Хеллмана не обеспечивает аутентификацию сторон. Для защиты от атак "человек посередине" рекомендуется использовать цифровые сертификаты или дополнительные механизмы аутентификации.
2. Можно добавить этап подписи открытых ключей для подтверждения их подлинности и защиты от подмены.
3. Несмотря на то, что сам протокол безопасен, его безопасность можно улучшить с помощью шифрования канала связи, например, с использованием TLS/SSL.

1.3 Полная схема компьютерной системы

Описание компонентов схемы:

Пользователь (субъект системы) инициирует процесс аутентификации, предоставляя идентификационные данные (например, логин и пароль, биометрические данные или токен). Эти данные передаются в систему для проверки.

Система идентификации и аутентификации (СИА) отвечает за верификацию личности пользователя. Она сверяет предоставленные данные с теми, которые хранятся в **сервере базы данных (БД)**, где находятся учетные данные пользователей. В случае успешной проверки система разрешает доступ пользователю.

Сервер базы данных хранит учетные данные (например, хешированные пароли) и другие данные, связанные с пользователями. Для обеспечения безопасности данные защищаются с помощью криптографических алгоритмов.

Криптографический модуль обеспечивает защиту данных, используя алгоритмы шифрования и протоколы обмена ключами, связанные с протоколом Диффи-Хеллмана. Это гарантирует, что данные, передаваемые между пользователем и сервером, защищены от перехвата или подделки.

Мониторы безопасности контролируют доступ к системным ресурсам и действиям пользователей. Они отслеживают подозрительные активности, такие как несанкционированные попытки доступа, и генерируют уведомления о возможных угрозах. Эти мониторы помогают поддерживать безопасность на уровне объектов и субъектов системы.

Внешний канал обеспечивает передачу данных между пользователем и сервером, при этом важно, чтобы передаваемая информация была защищена с помощью шифрования для предотвращения атак, таких как "человек посередине". Взаимодействие по защищенному каналу делает систему более безопасной.

Для защиты от атак "человек посередине" в компьютерной системе так же можно использовать дополнительные механизмы аутентификации (цифровые сертификаты или подписи).

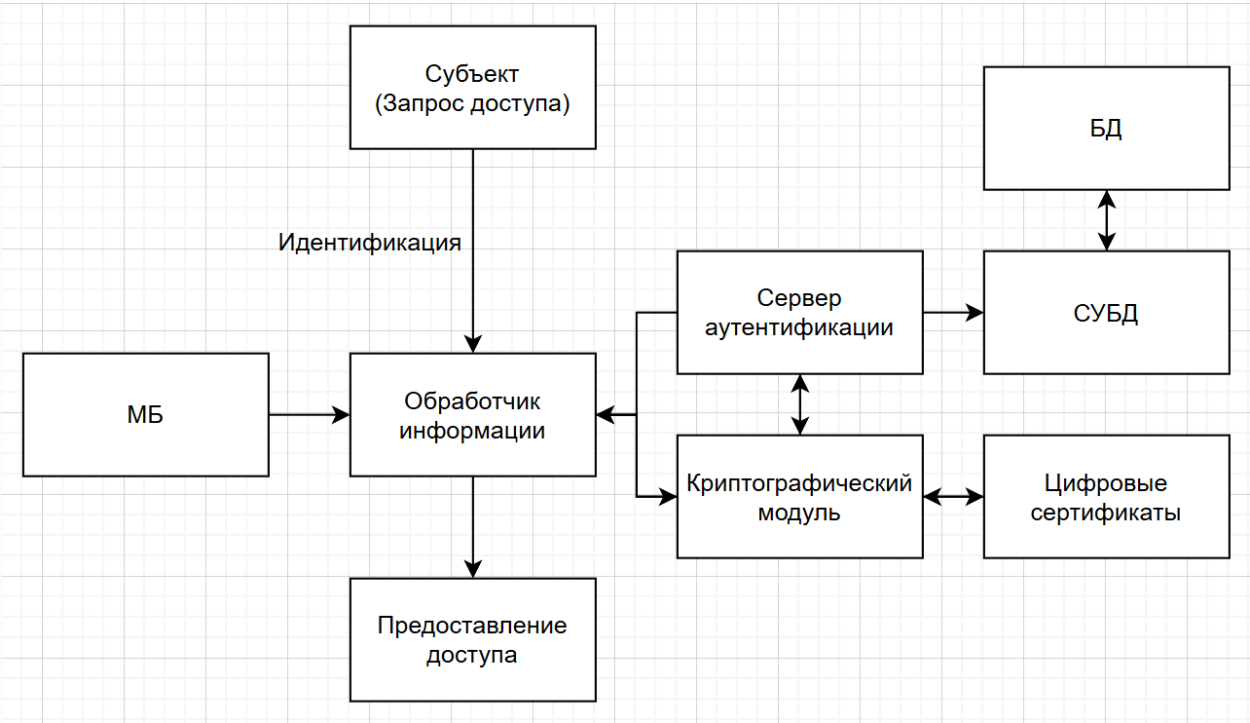

Рисунок 1 – Полная схема системы

Общий вывод:

Несмотря на высокую эффективность, протокол подвержен атакам типа "человек посередине", так как не предоставляет механизмов аутентификации сторон. Для повышения безопасности рекомендуется использовать цифровые сертификаты и другие способы верификации участников обмена. Также важным дополнением является использование защищенных каналов связи, которые могут дополнительно гарантировать безопасность данных.

Внедрение подсистемы идентификации и аутентификации, основанной на протоколе Диффи-Хеллмана, в компьютерные системы позволяет обеспечить надежную защиту от несанкционированного доступа и контролировать безопасность данных. Однако для полноценной защиты необходимо учитывать также механизмы аутентификации сторон, выбор надежных криптографических параметров и защиту от атак с повторным использованием сообщений.

ЗАКЛЮЧЕНИЕ

В ходе лабораторной работы был рассмотрен протокол Диффи-Хеллмана, который является основным инструментом для безопасного обмена ключами в подсистемах идентификации и аутентификации. Он позволяет двум сторонам безопасно договориться о секретном ключе через открытый канал связи, что делает его полезным для обеспечения безопасности обмена данными в современных сетевых протоколах.

Обобщая, протокол Диффи-Хеллмана является важным компонентом систем безопасности, но требует дополнительных мер для защиты от атак и обеспечения целостности данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Лр 6 идентификация .pdf - Google Диск
2. Док к 6 лабе.pdf - Google Диск
3. Алгоритм Diffie-Hellman: Ключ к безопасному общению / Хабр
4. Протокол Диффи — Хеллмана — Википедия
5. Большое руководство по сетям и шифрованию трафика в Linux (часть 1) / Хабр
6. «Криптосистемы-протоколы»: Диффи—Хеллмана, Эль-Гамаля, MTI/A(0), STS / Хабр