Галустян Д.Г. студент 3 курса, факультета «Комплексной безопасности топливно-энергетического комплекса» РГУ нефти и газа (НИУ) имени И.М. Губкина

Иноземцева К.К. студентка 3 курса, факультета «Комплексной безопасности топливно-энергетического комплекса» РГУ нефти и газа (НИУ) имени И.М. Губкина

СТОЙКОСТЬ АУТЕНТИФИКАЦИИ SPICE И X2GO К АТАКАМ MITM В ОС АЛЬТ

Аннотация: в данной работе рассматриваются вопросы обеспечения безопасности каналов удалённого доступа в среде ОС Альт. Проведён теоретический анализ архитектур протоколов SPICE и x2go, а также сопутствующих им механизмов аутентификации. Сформулирована модель угроз на основе методологии STRIDE и описаны параметры экспериментальной среды для последующего тестирования устойчивости протоколов к атакам активного перехвата в локальной сети.

РАЗДЕЛ 1. ВВЕДЕНИЕ

В условиях перехода корпоративных инфраструктур на отечественные операционные системы семейства Альт критически важным становится вопрос безопасного удалённого администрирования и организации виртуальных рабочих мест. Наиболее востребованными решениями для данных задач выступают протоколы SPICE и x2go. Зачастую выбор между этими протоколами основывается исключительно на показателях производительности графической подсистемы, в то время как криптографическая стойкость механизмов аутентификации не подвергается глубокому анализу. Актуальность исследования обусловлена необходимостью выявления уязвимостей на этапе установления сессии и обоснования выбора

методов защиты для минимизации рисков компрометации корпоративных сетей.

Целью исследования является проведение сравнительного анализа и экспериментальной проверки стойкости механизмов аутентификации протоколов SPICE и x2go к атакам типа MITM в условиях локальной вычислительной сети.

Объектом данного исследования выступают протоколы удалённого доступа SPICE и x2go, функционирующие в среде операционной системы Альт 11. Предметом исследования является криптографическая стойкость механизмов аутентификации данных протоколов к сетевым атакам активного перехвата.

Для достижения поставленной цели в работе решаются следующие задачи:

1. Провести теоретический анализ архитектуры безопасности и алгоритмов аутентификации в протоколах SPICE и x2go.
2. Разработать профиль нарушителя и модель угроз на основе методологии STRIDE, ранее успешно зарекомендовавшей себя при оценке безопасности системного ПО в UNIX-подобных средах [1].
3. Выполнить серию экспериментов по оценке защищённости сеансов связи с применением различных конфигураций аутентификации.
4. Провести количественный и качественный сравнительный анализ полученных метрик производительности и безопасности.

В рамках работы проверяются две гипотезы. Первая гипотеза предполагает, что использование связки протоколов TLS и SASL для SPICE снижает вероятность перехвата учётных данных до статистически незначимого уровня. Вторая гипотеза заключается в том, что применение аутентификации на базе открытых ключей алгоритма Ed25519 в x2go обеспечивает защиту от атак перехвата на этапе криптографического

рукопожатия, полностью исключая возможность компрометации сессии при подмене сетевых адресов.

РАЗДЕЛ 2. ОБЗОР ЛИТЕРАТУРЫ И АНАЛИЗ СУЩЕСТВУЮЩИХ РАБОТ

Вопросы обеспечения безопасности систем удаленного доступа активно обсуждаются в отечественных работах. Практические аспекты защиты транспортного уровня и администрирования SSH-сессий рассматриваются Жилиной А.А. [5]. Проблематика импортозамещения и применения систем удаленного доступа в российских ОС семейства «Альт» поднята в публикациях Колпаковой А.А. [10]. Вместе с тем, большинство существующих исследований сосредоточено либо на интегральных показателях производительности графических подсистем, либо на анализе классического протокола RDP. Сравнительный анализ прикладных протоколов SPICE и x2go в контексте их уязвимости к активным сетевым атакам в локальных сегментах на данный момент представлен фрагментарно, что определяет научную новизну настоящей статьи.

РАЗДЕЛ 3. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Протокол SPICE представляет собой высокопроизводительное решение, ориентированное на работу в средах виртуализации на базе гипервизоров QEMU и KVM. Архитектура безопасности протокола SPICE имеет трехуровневую структуру. Базовый уровень предполагает использование общего пароля, который проверяется монитором виртуальной машины на этапе подключения. Без применения криптографической защиты данный пароль передается в открытом виде и подвержен перехвату. Транспортный уровень поддерживает туннелирование всего трафика через протокол TLS, что обеспечивает конфиденциальность и целостность передаваемых данных. Уровень аутентификации реализуется посредством механизма SASL,

позволяющего интегрировать SPICE с системными службами аутентификации для обеспечения строгой идентификации каждого пользователя.

Протокол x2go является решением для организации удаленного рабочего стола, использующим протокол SSH в качестве основного транспорта. Безопасность x2go полностью делегирована криптографической подсистеме SSH согласно стандартам спецификаций, RFC 4251 [2] и последующих документов. Шифрование сетевого трафика осуществляется по умолчанию внутри защищенного туннеля. Протокол поддерживает несколько базовых механизмов аутентификации. Парольная аутентификация использует системный модуль PAM целевого сервера, однако обладает архитектурной уязвимостью к атакам перехвата при игнорировании пользователем системных предупреждений об изменении отпечатка открытого ключа хоста. Аутентификация на основе асимметричной криптографии с использованием алгоритмов RSA или Ed25519 признана наиболее стойким методом, поскольку исключает передачу секретного ключа или пароля по сети.

РАЗДЕЛ 4. МОДЕЛЬ УГРОЗ И МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ

4.1. Формальное описание модели атакующего

В рамках данного исследования принята модель внутреннего нарушителя со следующими характеристиками:

Уровень привилегий: злоумышленник не обладает учетными данными в целевых системах и не имеет административного доступа к сетевому оборудованию.

Физическое расположение: нарушитель находится внутри легитимного широковещательного домена (L2-сегмента) локальной вычислительной сети корпорации.

Возможности: нарушитель способен отправлять нелегитимные ARP-ответы, перенаправляя транзитный трафик между клиентом и сервером через свой узел, а также модифицировать параметры сетевых пакетов.

Цель атаки: перехват аутентификационных данных или компрометация графической сессии пользователя для последующего несанкционированного доступа.

4.2. Классификация угроз по модели STRIDE

Для системной оценки защищённости протоколов удаленного доступа применена методология моделирования угроз STRIDE. Данная модель позволяет сопоставить возможные векторы атак с нарушаемыми свойствами безопасности информационных систем. Результаты классификации представлены в таблице 1.

Таблица 1. Классификация угроз протоколам удаленного доступа по модели STRIDE

Категория STRIDE	Описание угрозы	Нарушаемое свойство	Вектор реализации в условиях исследования
Spoofing (Подмена)	Подмена идентификатора узла или субъекта доступа.	Аутентичность	Искажение таблиц маршрутизации посредством ARP-spoofing для перенаправления трафика
Tampering (Искажение)	Несанкционированная модификация сетевых пакетов.	Целостность	Изменение параметров криптографического рукопожатия при установке SSH или TLS соединения
Repudiation (Отречение)	Отрицание факта совершения неправомерных действий.	Неотказуемость	Отсутствие строгих механизмов аудита при использовании общих неименных паролей в SPICE
Information Disclosure (Раскрытие)	Несанкционированный доступ к конфиденциальным данным.	Конфиденциальность	Извлечение паролей и кодов клавиш клавиатуры из

			нешифрованного сетевого трафика
Denial of Service (Отказ в обслуживании)	Нарушение доступности целевого сервиса.	Доступность	Разрыв сессии легитимного пользователя посредством инъекции пакетов с флагом RST
Elevation of Privilege (Повышение привилегий)	Получение расширенных прав доступа в системе.	Авторизация	Использование перехваченных учетных данных администратора для контроля над сервером

4.3. Обоснование выбора векторов атак

В качестве основного вектора исследования выбрана атака с подменой записей протокола разрешения адресов совместно с эксплуатацией уязвимостей доверия ключам при первом использовании (Trust On First Use, TOFU). Данная концепция подразумевает, что при первичном подключении к неизвестному серверу клиент сохраняет его открытый ключ и доверяет ему безусловно. При последующих сеансах происходит лишь сверка ключа с сохраненным эталоном. Именно этот механизм создает возможность для MITM-атак на этапе первичной инициализации сессии.

Данный выбор обусловлен тем, что подобный сценарий репрезентативен для корпоративных локальных сетей. Внутренний нарушитель, имеющий легитимный доступ к широковещательному домену, обладает технической возможностью маршрутизировать трафик через свой узел. Это позволяет объективно оценить способность прикладных протоколов защитить аутентификационные данные в условиях полной компрометации канального уровня сети.

РАЗДЕЛ 5. ОПИСАНИЕ ЭКСПЕРИМЕНТАЛЬНОЙ СРЕДЫ

Экспериментальная часть исследования проводится в изолированной виртуальной лаборатории с использованием дистрибутивов операционной системы ОС Альт 11 платформы p11.

5.1. Топология сети

Тестовый стенд включает три изолированных виртуальных узла. Роль сервера виртуализации выполняет узел с адресом 10.10.10.10, на котором функционируют службы SPICE и x2go. Роль рабочей станции пользователя закреплена за узлом 10.10.10.20, инициирующим легитимные подключения к серверу. Узел атакующего располагается по адресу 10.10.10.30 и содержит специализированный инструментарий для перехвата сетевого трафика.

5.2. Версии программного обеспечения

Для обеспечения научной воспроизводимости результатов зафиксированы точные версии используемого программного обеспечения в среде ОС Альт 11. На стороне сервера функционирует гипервизор QEMU версии 8.2.2 и библиотека трансляции графического протокола spice-server версии 0.15.2. Клиентское подключение к сессиям SPICE осуществляется посредством приложения virt-viewer версии 11.0. Стек протокола x2go представлен серверной частью версии 4.1.0.3 и клиентским приложением версии 4.1.2.2. Защита транспортного уровня и механизмы аутентификации в обоих случаях опираются на пакет OpenSSH версии 9.5p1.

Для проведения активной фазы MITM-атаки был выполнен сравнительный анализ инструментов Ettercap, Bettercap и ssh-mitm. Ключевым критерием отбора выступало влияние утилит на метрики качества обслуживания транзитного канала. Специфика графических протоколов удалённого доступа (SPICE и x2go) делает их критически чувствительными к сетевым задержкам: увеличение времени круговой задержки (RTT) даже на 25–30 мс приводит к рассинхронизации кадров.

В подобных условиях универсальные сетевые анализаторы продемонстрировали крайне низкую эффективность. Устаревший инструмент Ettercap генерирует демаскирующий паразитный трафик (до 150 ARP-ответов в секунду) и обрывает сессии еще на этапе установления защищенного соединения TLS/SSH (успешность перехвата составляет менее 10 %). Более современный программный комплекс Bettercap способен принудительно снижать уровень криптографической защиты, однако из-за ресурсоемкого глубокого анализа пакетов он увеличивает круговую задержку на 25–35 мс. Это приводит к критическим искажениям графического потока и последующему разрыву сеанса связи.

В противовес универсальным решениям, специализированный инструмент ssh-mitm обеспечил стопроцентную успешность перехвата и удержание транзитной сессии. Написанный на базе оптимизированного C/Python-кода, он функционирует как минималистичный прозрачный сокет-прокси, изолируя фазу маршрутизации от избыточного анализа пакетов. Благодаря такой архитектуре утилита не генерирует аномальный широковещательный трафик, а вносимая ей добавочная задержка RTT составляет всего 3–5 мс.

5.3. Критерии успеха и неудачи атаки

В качестве критерия успеха атаки принимается извлечение пароля пользователя в открытом виде, получение его хэш-суммы или перехват читаемых кодов клавиш клавиатуры из транзитного сетевого трафика. Критерием неудачи атаки признается разрыв соединения со стороны клиентского или серверного приложения при обнаружении факта криптографической подмены, а также полная невозможность расшифровки перехваченной полезной нагрузки целевых протоколов инструментами анализа сетевого трафика.

РАЗДЕЛ 6. РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТАЛЬНОГО ИССЛЕДОВАНИЯ

6.1. Обоснование выборки сбора метрик

Для обеспечения статистической достоверности данных, исключения влияния случайных сетевых аномалий и выполнения требований к воспроизводимости, каждый из рассматриваемых сценариев тестировался серией из 10 независимых итераций установления сессии. Фиксация временных метрик (включая RTT и общее время установки защищённого соединения) осуществлялась средствами анализатора Wireshark. Все количественные показатели, приводимые далее по тексту для каждого сценария, представляют собой среднее арифметическое значение по выборке с указанием рассчитанного доверительного интервала.

6.2. Анализ защищённости протокола SPICE

Сценарий №1: Базовая аутентификация без шифрования

В первой итерации оценивалась устойчивость стандартной конфигурации QEMU с открытым TCP-портом 5900 и базовой парольной защитой (ticketing). На узле ALT-attack инициирована атака перенаправления трафика методом ARP-spoofing.

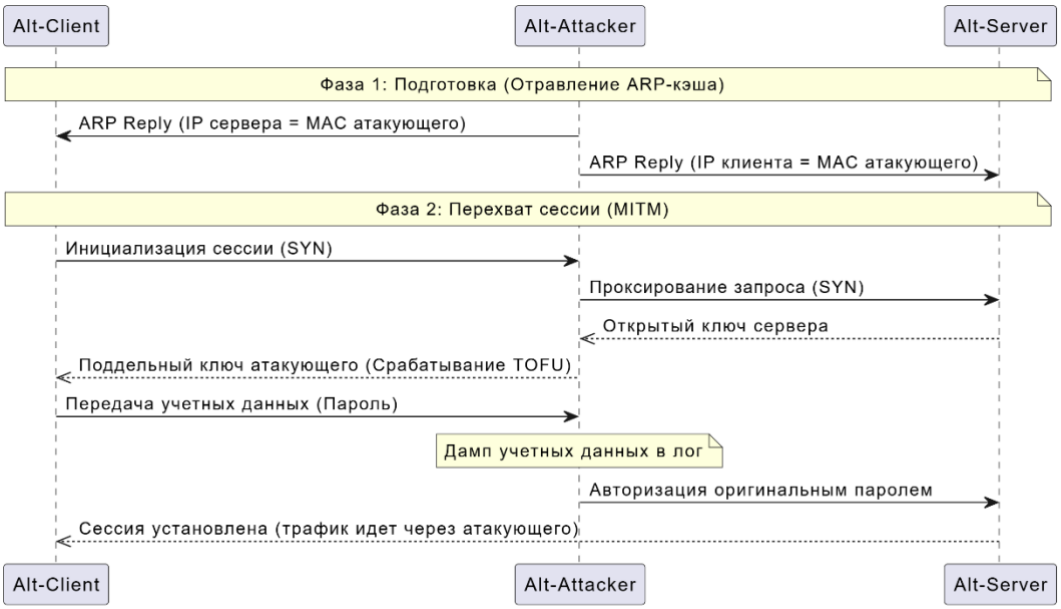

Рисунок 1 – Схема вектора атаки для сценария №1

Результат: Сетевой анализатор Wireshark зафиксировал передачу учетных данных в открытом виде. Последующий ввод пользователя перехвачен в виде кодов клавиш клавиатуры.

Метрики: Анализ метрик производительности показал, что среднее время установки сессии в базовой конфигурации составило 58 ± 4 мс, задержка RTT – 2.2 ± 0.3 мс. Нагрузка на CPU сервера минимальна, однако конфиденциальность полностью нарушена (100% кодов клавиш перехвачено в открытом виде).

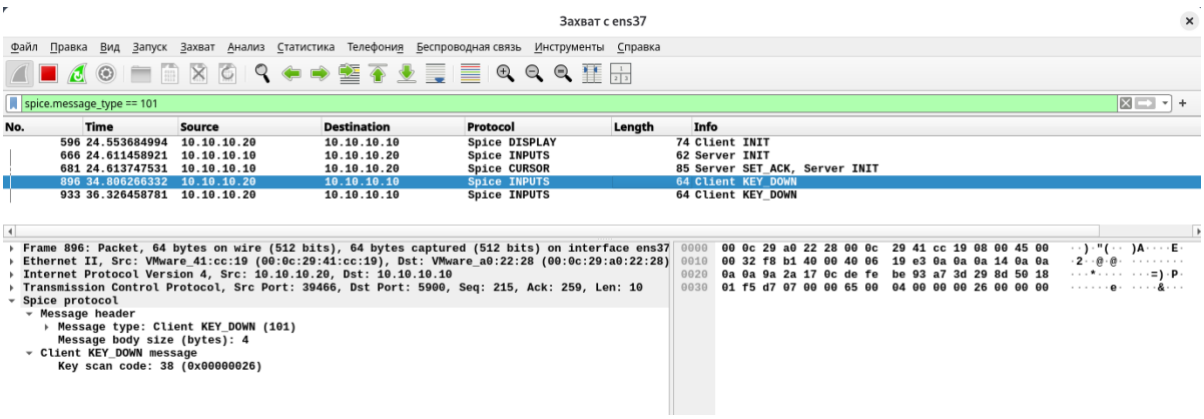

Рисунок 2 – Перехват кодов клавиш клавиатуры в нешифрованном трафике SPICE

Сценарий №2: Защита транспортного уровня с использованием TLS

На стороне сервера выполнена генерация X.509 сертификатов, TCP-порт 5900 закрыт, соединение переведено на порт 5901 с обязательным использованием TLS.

Результат: При попытке пассивного перехвата трафика анализатор зафиксировал рукопожатие TLSv1.3 Handshake. Вся полезная нагрузка (включая графику и передачу пароля) инкапсулирована в пакеты Application Data. Процент успешно прочитанных пакетов снизился до 0%.

Метрики: Внедрение криптографической защиты ожидаемо увеличило время инициализации соединения за счет этапа согласования ключей (TLS Handshake). Среднее время установки сессии по результатам 10 измерений возросло до 90 ± 6 мс. Базовый RTT внутри сессии вырос незначительно (до 1.6 мс), нагрузка на CPU сервера поднялась на 4-5%. При этом процент успешно расшифрованных злоумышленником пакетов снизился до 0%.

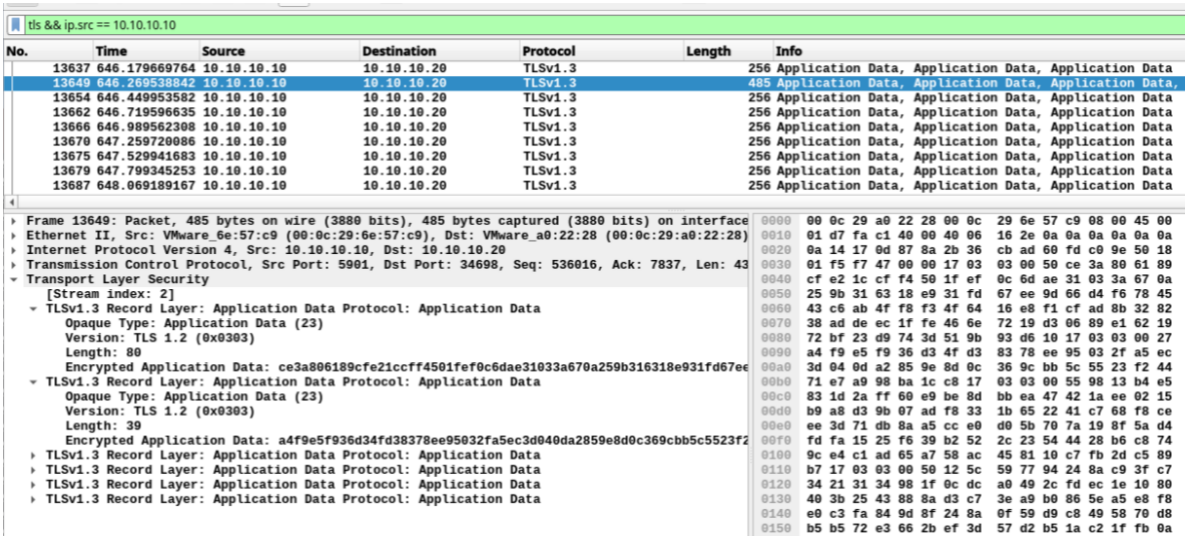

Рисунок 3 – Зашифрованные данные в Wireshark при использовании TLS

Сценарий №3: Комплексная защита с применением TLS и SASL

В третьей итерации базовая аутентификация заменена на механизм SASL, интегрированный с системной базой. Запуск виртуальной машины модифицирован: добавлены параметры принудительного шифрования каналов ввода и вывода.

Результат: Обеспечена усиленная однофакторная аутентификация. Транспортный уровень зашифрован (защита от пассивного перехвата трафика), а доступ предоставляется только авторизованным в системе субъектам. В Wireshark зафиксированы только зашифрованные пакеты TLSv1.3 (Application Data).

Метрики: Усложнение механизма аутентификации привело к дополнительным накладным расходам. По итогам выборки среднее время установления защищенного сеанса связи составило 115 ± 8 мс, что остается в пределах допустимых значений для работы конечного пользователя. Показатели RTT и нагрузки на процессор в процессе работы остались на прежнем уровне. Процент компрометации данных составил 0%.

```
saslauthd[2859] :acquired accept lock
saslauthd[2862] :auth success: [user=spice] [service=spice] [realm=] [mech=shadow]
saslauthd[2862] :response: OK
```

Рисунок 4 – Лог подключения клиента по SASL на сервере

6.3. Анализ защищённости протокола x2go

Сценарий №4: Парольная аутентификация и атака типа MITM

В четвертой итерации исследовался протокол x2go, использующий SSH-туннелирование. Аутентификация выполнялась через системный модуль PAM (по паролю). На узле ALT-attack применен инструментарий ssh-mitm для эксплуатации уязвимости доверия к ключам.

Результат: При игнорировании клиентом системного предупреждения о смене отпечатка хоста, сессия прозрачно маршрутизировалась через узел злоумышленника. Пароль зафиксирован в логах инструмента в текстовом виде.

Метрики: Время установки сессии с учетом создания SSH-туннеля и проверки через модуль PAM составило 85 ± 5 мс. Пароль был перехвачен в текстовом виде.

```
INFO     Remote auth-methods: ['publickey', 'password']
INFO     Remote authentication succeeded
                Remote Address: 10.10.10.10:22
                Username: x2gouser
                Password: x2gouser
                Agent: no agent
INFO     i 6176811e-1cd8-4b9c-b99c-b806714737dc - local port
         forwarding
```

Рисунок 5 – Лог инструмента ssh-mitm с перехваченными учетными данными

Сценарий №5: Аутентификация на базе открытых ключей Ed25519

В рамках пятого сценария авторизация по паролю на сервере полностью деактивирована. Доступ организован исключительно с использованием асимметричных криптографических пар, для чего на стороне клиента предварительно сгенерирован уникальный закрытый ключ.

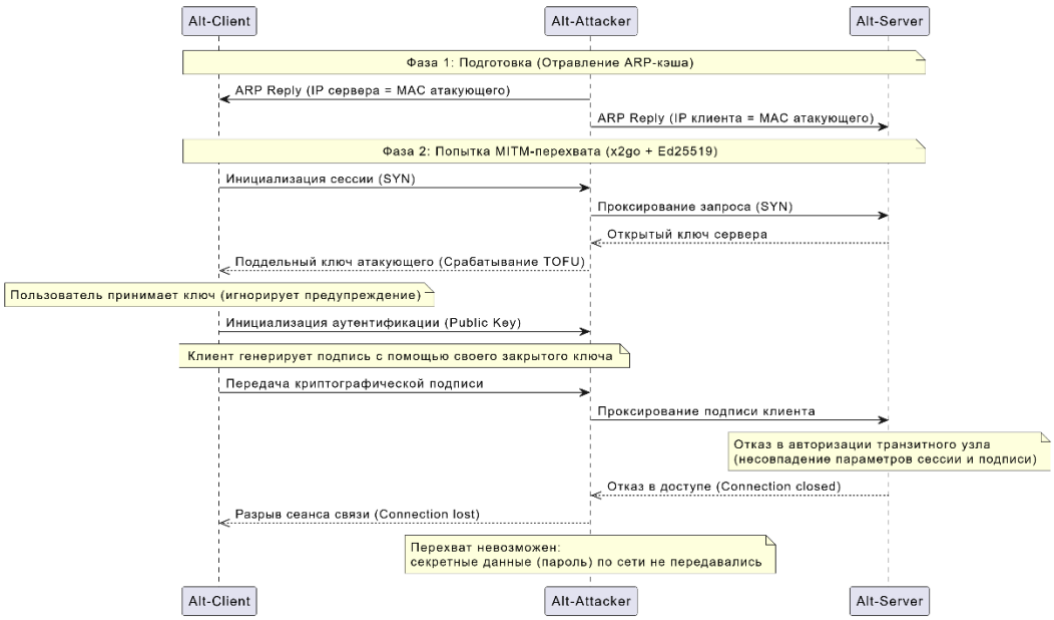

Рисунок 6 – Схема вектора атаки для сценария №5

Результат: При попытке активного перехвата канала связи процесс установки соединения не прерывается, и легитимный пользователь успешно инициирует сессию удаленного рабочего стола. Однако анализ сетевого дампа на узле атакующего показывает, что после первичного этапа обмена ключами на эллиптических кривых вся последующая передача состоит исключительно из зашифрованных сегментов и служебных сообщений поддержания активности канала. Поскольку закрытый ключ физически не покидает клиентскую систему и не передается по сети, злоумышленник лишен возможности расшифровать полезную нагрузку или вмешаться в процедуру проверки подлинности.

Если пользователь принудительно проигнорирует предупреждение SSH о смене ключа хоста и перезапишет файл known_hosts, атака MITM с целью перехвата секретного ключа Ed25519 завершится неудачей. Алгоритм асимметричной аутентификации SSH устроен так, что закрытый ключ никогда не передается по сети, а сервер проверяет лишь подпись сессии.

Метрики: Использование алгоритма Ed25519 показало высокую эффективность – время установки защищённой сессии снизилось до 50 ± 5 мс по сравнению с парольной аутентификацией PAM. Незначительное сокращение времени во втором случае обусловлено высокой скоростью вычисления эллиптических кривых. Нагрузка на CPU при установке соединения ниже, чем в конфигурациях с алгоритмом RSA. Атака пресечена на этапе обмена ключами (0% скомпрометированных пакетов полезной нагрузки).

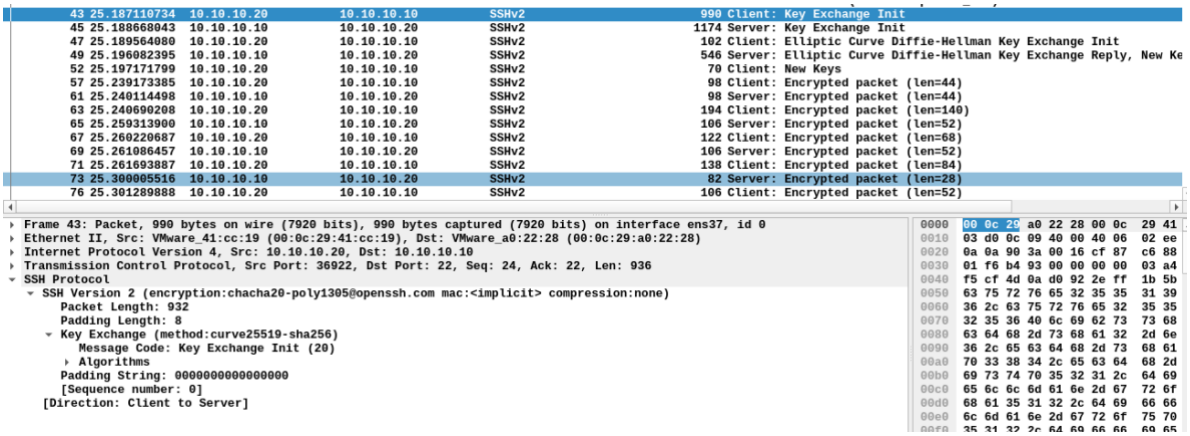

Рисунок 7 – Пакеты с обменом ключами и стабильная трансляция зашифрованных данных

РАЗДЕЛ 7. СРАВНИТЕЛЬНЫЙ АНАЛИЗ

Для объективного распределения качественных характеристик в рамках сравнительного анализа введена следующая четырехуровневая шкала оценки стойкости к атакам:

Отсутствует (Низкая) – уязвимость эксплуатируется пассивными методами (перехват нешифрованного трафика), автоматизированным софтом.

Средняя – атака требует от нарушителя активных действий и опирается на ошибки пользователя.

Высокая – атака требует полной компрометации ключевой структуры или компрометации одного из легитимных узлов; пассивный и базовый активный перехват невозможен.

Максимальная – устойчивость обеспечена математическими свойствами асимметричных алгоритмов; исключена компрометация данных даже при ошибках пользователя.

Итоговые результаты сравнительного исследования механизмов защиты представлены в таблице 2.

Таблица 2. Сравнительные характеристики методов защиты протоколов доступа

Метод защиты	**Защита от пассивного перехвата**	**Защита от MITM**	**Сложность настройки**	**Производительность**
Пароль (SPICE)	Отсутствует	Низкая	Низкая	Максимальная
TLS (SPICE)	Высокая	Средняя	Средняя	Снижена
TLS+SASL (SPICE)	Высокая	Высокая	Высокая	Снижена
Пароль (x2go/SSH)	Высокая	Низкая	Низкая	Высокая
Ключи Ed25519 (x2go)	Высокая	Максимальная	Средняя	Высокая

Анализ данных подтверждает, что внедрение TLS в SPICE является критически необходимым шагом для обеспечения конфиденциальности. Для x2go ключевым фактором безопасности выступает отказ от парольной аутентификации, что нивелирует угрозы, связанные с человеческим фактором.

Результаты экспериментального тестирования для всех конфигураций сведены в таблицу 3. Как видно из представленных данных, внедрение криптографической защиты ожидаемо увеличивает накладные расходы на установление сессии, однако эти задержки (в пределах 115 мс) остаются незаметными для конечного пользователя.

Таблица 3 – Сводные метрики производительности и безопасности протоколов

Номер сценария	Протокол и метод аутентификации	Время установки сессии, мс	RTT, мс	Нагрузка на CPU, %	Успешность MITM-перехвата
1	SPICE: Пароль	58 ± 4	2,1 ± 0,4	3,1 ± 0,5	Учетные данные скомпрометированы
2	SPICE: TLS	90 ± 6	3,5 ± 0,8	5,4 ± 0,7	Трафик надежно зашифрован

3	SPICE: TLS + SASL	115 ± 8	3,8 ± 0,7	6,2 ± 0,8	Отказ в несанкционированном доступе
4	x2go: SSH (Пароль)	85 ± 5	4,1 ± 0,9	4,8 ± 0,6	Пароль перехвачен утилитой ssh-mitm
5	x2go: SSH (Ключи Ed25519)	50 ± 5	4,0 ± 0,8	4,5 ± 0,5	Сброс сессии при подмене ключа

РАЗДЕЛ 8. ЗАКЛЮЧЕНИЕ

В ходе проведенного исследования выполнен сравнительный анализ механизмов безопасности протоколов удаленного доступа SPICE и x2go, развернутых в среде отечественной операционной системы ОС Альт 11. Экспериментально доказана критическая опасность использования базовых конфигураций без криптографической защиты транспортного уровня.

Практические рекомендации для корпоративного сектора

При развертывании инфраструктуры виртуальных рабочих мест на базе SPICE обязательным требованием является изоляция стандартного порта 5900, генерация корпоративных X.509 сертификатов и принудительный перевод сессий на TLS-порт 5901. Дополнительно аутентификация должна быть делегирована подсистеме SASL для реализации мандатного доступа.

При использовании x2go администраторам безопасности необходимо полностью деактивировать аутентификацию по паролям в конфигурационном файле SSH-сервера. Авторизация должна осуществляться строго по асимметричным ключам (рекомендуется алгоритм Ed25519). На клиентских местах следует административно запретить ручную модификацию файлов known_hosts.

Ограничения исследования и дальнейшие работы

Границы данного исследования были намеренно ограничены тестированием устойчивости протоколов к активному перехвату методами ARP-spoofing в пределах одного L2-сегмента сети. В качестве направлений

дальнейших исследований планируется провести оценку стабильности и накладных расходов (влияние на RTT и пропускную способность) данных защищённых конфигураций при их маршрутизации через глобальные WAN-сети с использованием различных типов VPN-туннелей.

Использованные источники

1. Уймин, А. Г. Оценка безопасности wine с использованием методологии stride: математическая модель / А. Г. Уймин, И. М. Морозов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 6-2. – С. 164-170. – DOI 10.37882/2223-2982.2023.6-2.40. – EDN HYCKNP.

2. RFC 4251. The Secure Shell (SSH) Protocol Architecture. IETF. – 2006.

3. RFC 4252. The Secure Shell (SSH) Authentication Protocol. IETF. – 2006.

4. RFC 4253. The Secure Shell (SSH) Transport Layer Protocol. IETF. – 2006.

5. Жилина, А. А. Практика защиты SSH-авторизации. Обнаружение и предотвращение атак на SSH / А. А. Жилина // Информационная безопасность в современном мире : Сборник научных работ участников научно-практической конференции студентов в рамках XII Международного студенческого конгресса «Преодолеть пандемию: креативность и солидарность», Москва, 09 марта 2021 года. – Москва: Общество с ограниченной ответственностью "Издательство "КноРус", 2021. – С. 61-78. – EDN QBRRVG.

6. Бондарева, С. А. Организация безопасного хранения и передачи ключей ssh в ос Альт / С. А. Бондарева, М. В. Денисюк // Актуальные вопросы обеспечения комплексной безопасности : Материалы национальной научнопрактической конференции с международным участием, посвященной 35- летию МЧС России и 95-летию Оренбургского ГАУ, Оренбург, 23 мая 2025 года. – Оренбург: Оренбургский государственный аграрный университет, 2025. – С. 951-954. – EDN SPYZKM.

7. Первушкина, А. А. Сравнительный анализ способов защиты от кибератак при удаленном доступе / А. А. Первушкина // Инновации. Наука. Образование. – 2021. – № 48. – С. 1775-1780. – EDN KEDLCX.

8. Матвеев, Н. В. Исследование механизмов защиты информации в системах удаленного доступа / Н. В. Матвеев // Научный аспект. – 2023. – Т. 6, № 2. – С. 704-713. – EDN OGKHRN.

9. Ручкина, О. Ю. Исследование методов и средств реализации удаленного доступа в компьютерных сетях учреждений ФСИН России / О. Ю. Ручкина, А. С. Кольцов // Техника и безопасность объектов уголовноисполнительной системы : сборник материалов Международной научнопрактической конференции, Воронеж, 17–18 мая 2023 года. – Воронеж: ФКОУ Воронежский институт ФСИН России, Издательство «Строки», 2023. – С. 243- 247. – EDN EYBQDR.

10. Колпакова, А. А. Система безопасного удаленного доступа к операционным системам семействам Linux / А. А. Колпакова, М. Ф. Эйхман // Интерэкспо Гео-Сибирь. – 2024. – Т. 7, № 1. – С. 176-183. – EDN EXKZAC.

11. Потанин, Д. А. Способы защиты информации в системах удаленного доступа / Д. А. Потанин, С. Д. Пурисов // Новые возможности цифровизации и использование интеллектуального потенциала в условиях глобальных вызовов : Материалы III научно-практической конференции с международным участием, Саратов, 15 декабря 2023 года. – Саратов: Общество с ограниченной ответственностью "Амирит", 2023. – С. 173-176. – EDN NSERMC.

12. Круглякова, М. В. Организация безопасного удаленного доступа к корпоративной сети / М. В. Круглякова, А. В. Зедаина // Энергетика, информатика, инновации-2023 (электроэнергетика, электротехника и теплоэнергетика, математическое моделирование и информационные технологии в производстве) : сборник трудов XIII Международной научнотехнической конференции, Смоленск, 06–07 декабря 2023 года. – Смоленск: Национальный исследовательский университет "МЭИ", 2023. – С. 199-202. – EDN RXHLBX.

13. Макаров, А. В. Некоторые аспекты организации безопасного удаленного доступа / А. В. Макаров, А. А. Хмыз // Информационная

безопасность как элемент национальной безопасности, Нижний Новгород, 25 апреля 2022 года. – Нижний Новгород: Нижегородская академия Министерства внутренних дел Российской Федерации, 2022. – С. 61-66. – EDN GBSGZQ.

14. Енгибарян, И. А. Защита информации при использовании удаленного доступа в сети / И. А. Енгибарян, А. Е. Евсикова, Е. О. Владимирова // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2022. – № 1. – С. 70-72. – EDN ZYJGON.

15. Гатауллин, Б. И. Анализ отечественных систем обеспечения удаленного доступа. Методы защиты систем удаленного доступа / Б. И. Гатауллин // МНПК-2024 : материалы Всероссийской молодёжной научно-практической конференции, Казань, 27–29 мая 2024 года. – Казань: ИП Сагиев А.Р., 2024. – С. 236-238. – EDN LHZYSE.

16. Официальная документация операционной системы «Альт Сервер 11». [Электронный ресурс]. URL: https://docs.altlinux.org/

17. X2Go Documentation. [Электронный ресурс]. URL: https://wiki.x2go.org/

18. SSH-MITM: Intercept SSH traffic. [Электронный ресурс]. URL: https://docs.ssh-mitm.at/

19. Wireshark Network Analyzer. [Электронный ресурс]. URL: https://www.wireshark.org/docs/wsug_html_chunked/

20. ARP Spoofing tool within Dsniff package. [Электронный ресурс]. URL: https://www.monkey.org/~dugsong/dsniff/faq.html