ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.056.53

АНАЛИЗ МЕТОДОВ СОЗДАНИЯ ЗАЩИЩЕННЫХ СОЕДИНЕНИЙ В ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ

Баулин Егор Игоревич
Студент магистратуры
2 курс, факультет «Сети и системы связи»
Кафедра «Сети связи и системы коммутации»
Московский технический университет связи и информатики
e-mail: egor38ka@mail.ru

Зунуни Умарджони Толибджон
Студент магистратуры
2 курс, факультет «Сети и системы связи»
Кафедра «Сети связи и системы коммутации»
Московский технический университет связи и информатики
e-mail: bigby.w99@gmail.com

Чванов Владислав Вячеславович
Студент, магистратура 2 курс
Факультет «Сети и системы связи»
Кафедра «Сети связи и системы коммутации»
Московский технический университет связи и информатики
e-mail: fyndell@yandex.ru

Аннотация

В статье рассматриваются основные аспекты создания защищённых соединений в инфокоммуникационных сетях. Обсуждаются ключевые технологии и протоколы, такие как SSL/TLS, IPSec и SSH, а также методы шифрования данных, включая симметричные и асимметричные алгоритмы. Особое внимание уделяется анализу уязвимостей и стратегиям защиты данных от современных угроз, а также предлагается комплексный подход к обеспечению информационной безопасности, необходимый для защиты данных в условиях постоянно растущих киберугроз.

Ключевые слова: инфокоммуникационные сети, защищённые соединения, шифрование, аутентификация, SSL/TLS, IPSec, SSH, кибербезопасность.

ANALYSIS OF METHODS FOR CREATING SECURE CONNECTIONS IN INFOCOMMUNICATION NETWORKS

Egor I. Baulin
Master's degree student

2nd year, Faculty of Networks and Communication Systems
Department of Communication Networks and Switching Systems
Moscow Technical University of Communications and Informatics

Umardzhoni T. Zununi
Master's degree student
2nd year, Faculty of Networks and Communication Systems
Department of Communication Networks and Switching Systems
Moscow Technical University of Communications and Informatics

Vladislav V. Chvanov
Master's degree student
2nd year, Faculty of Networks and Communication Systems
Department of Communication Networks and Switching Systems
Moscow Technical University of Communications and Informatics

ABSTRACT

The article discusses the main aspects of creating secure connections in information and communication networks. Key technologies and protocols such as SSL/TLS, IPsec and SSH are discussed, as well as data encryption methods, including symmetric and asymmetric algorithms. Particular attention is paid to vulnerability analysis and data protection strategies against modern threats, and an integrated approach to information security is proposed, which is necessary to protect data in the face of ever-growing cyber threats.

Keywords: infocommunication networks, secure connections, encryption, authentication, SSL/TLS, IPSec, SSH, cybersecurity

Введение

С развитием информационных технологий и увеличением объема обрабатываемых и передаваемых данных в инфокоммуникационных сетях, значимость обеспечения надежности и безопасности этих данных становится критически важной. Защищенные соединения являются фундаментальным элементом современных информационных систем, поскольку они обеспечивают конфиденциальность, целостность и доступность данных при их передаче между узлами сети. Это особенно актуально в условиях постоянно растущих угроз кибербезопасности, когда атаки становятся все более изощренными и целенаправленными. [1]

В основе важности защищенных соединений лежат требования к защите персональных данных, корпоративной информации, а также государственных секретов, которые требуют строгой конфиденциальности и защиты от несанкционированного доступа. [2] При этом, защищенные соединения предотвращают возможные атаки на сетевую инфраструктуру, такие как «Человек посередине», где злоумышленник может перехватывать и модифицировать передаваемую информацию, или атаки типа отказ в обслуживании (Denial of Service, DoS), направленные на нарушение доступности ресурсов. [3]

Одной из основных проблем в обеспечении безопасности данных в инфокоммуникационных сетях является разнообразие и постоянное обновление методов кибератак. Это требует от систем безопасности гибкости и способности адаптироваться к новым угрозам. Второй значительной проблемой является необходимость обеспечения баланса между уровнем безопасности и производительностью системы. Чрезмерное увеличение сложности шифрования может привести к замедлению работы сети, что недопустимо в условиях требований к высокой скорости передачи данных. [4]

Кроме того, существует проблема совместимости различных систем и протоколов безопасности. В идеальном случае, защищенные соединения должны быть универсальными и поддерживать возможность интеграции с различными платформами и устройствами. Это становится особенно актуальным в контексте развития Интернета вещей (Internet of Things, IoT), где количество устройств и типов соединений постоянно растет.

Стандарты и протоколы

SSL/TLS, IPSec и SSH – это протоколы, обеспечивающие безопасную передачу данных. SSL/TLS шифрует информацию между веб-сервером и браузером для конфиденциальности и защиты от атак. IPSec защищает информацию в IP-сетях с помощью шифрования и аутентификации на сетевом уровне, обеспечивая безопасность во всей сетевой архитектуре. SSH обеспечивает безопасный удаленный доступ и передачу данных через защищенный канал, используя надежное шифрование и аутентификацию.

Таблица 1. Сравнение протоколов защищенных соединений

Протокол	Уровень безопасности	Метод шифрования	Использование	Особенности
SSL/TLS	Транспортный	Симметричное и асимметричное	Браузеры, онлайн-торговля	Защищает передачу данных в интернете
IPSec	Сетевой	Симметричное	VPN, обмен информацией между устройствами	Обеспечивает шифрование и аутентификацию на IP уровне
SSH	Прикладной	Симметричное	Дистанционное управление, передача файлов	Предоставляет безопасный канал для удаленной работы

В таблице 1 показывается, что каждый из представленных протоколов имеет свои уникальные особенности и области применения. SSL/TLS обычно используется для защиты соединений в интернете, тогда как IPSec применяется для установления защищенных сетевых соединений на IP-уровне. SSH отлично подходит для обеспечения безопасности при удаленном доступе и передаче файлов. Выбор конкретного протокола следует основывать на требованиях к безопасности, производительности и совместимости в соответствующей операционной среде.

Методы шифрования

Шифрование – это важный элемент защиты данных в информационных системах. Оно подразумевает преобразование информации в формат, который может быть прочитан только теми, кто обладает ключом дешифрования. Существуют два основных вида шифрования: симметричное и асимметричное, каждый из которых имеет свои особенности, преимущества и недостатки.

Симметричное шифрование предполагает использование одного и того же ключа для шифрования и дешифрования данных. Этот метод отличается высокой скоростью и эффективностью с точки зрения использования вычислительных ресурсов, что делает его оптимальным для приложений, требующих быстрой обработки больших объемов информации. К примерам алгоритмов симметричного шифрования можно отнести AES, DES, 3DES и другие. Симметричное шифрование широко применяется для защиты данных на уровне файлов и дисков, а также в сетевых протоколах, таких как Wi-Fi Protected Access (WPA), обеспечивающих безопасность беспроводных сетей.

Асимметричное шифрование, также известное как шифрование с использованием пар ключей, использует два ключа: один для шифрования (открытый ключ) и другой для дешифрования (закрытый ключ). Этот метод решает проблему безопасной передачи ключей, присутствующую в симметричном шифровании, позволяя безопасно обмениваться зашифрованной информацией даже в случае, если стороны ранее не встречались и не обменивались ключами. К примерам алгоритмов асимметричного шифрования можно отнести RSA, ECC, DSA и другие. Асимметричное шифрование часто используется в цифровых подписях и SSL/TLS-сессиях для обеспечения аутентификации и безопасного обмена ключами. Оно также применяется в системах электронной почты для защиты конфиденциальности и целостности сообщений.

В защищенных соединениях оба метода шифрования играют ключевую роль. Протоколы безопасности, такие как SSL/TLS, используют асимметричное шифрование для начального обмена ключами, чтобы безопасно передать симметричный ключ, который затем применяется для шифрования всего сеанса передачи данных. Такое сочетание методов позволяет объединить преимущества асимметричного шифрования с высокой производительностью симметричного шифрования.

Протоколы защищенных соединений

SSL и его улучшенная версия TLS – это протоколы, которые обеспечивают безопасность данных, передаваемых через интернет и другие сети, сочетая асимметричное и симметричное шифрование. Механизм работы таков:

Соединение начинается с «рукопожатия», в ходе которого клиент и сервер обмениваются информацией о версиях протокола, алгоритмах шифрования и методах аутентификации.

Сервер предоставляет свой сертификат с открытым ключом, который клиент использует для создания предварительного мастер-ключа, зашифрованного открытым ключом сервера.

Затем данные шифруются симметричным сессионным ключом, который генерируется из предварительного мастер-ключа.

IPSec – это набор протоколов для защиты данных на уровне сетевого интерфейса, работающий в двух режимах: транспортном и туннельном.

Механизм работы IPSec:

Протокол Authentication Header (AH) подтверждает подлинность и защищает от изменений в IP-пакетах.

Протокол Encapsulating Security Payload (ESP) обеспечивает конфиденциальность передаваемых данных посредством шифрования.

Для установления ключей используется Internet Key Exchange (IKE), который сочетает асимметричное шифрование для безопасного обмена ключами.

Таблица 2. Примеры использования протоколов в различных типах сетей

Протокол	Корпоративные сети	Облачные сети	Мобильные сети

SSL/TLS	Защита корпоративных веб-сервисов и внутренних порталов	Шифрование данных, передаваемых между облачными сервисами и клиентами	Шифрование данных мобильных приложений, особенно в банковских и коммерческих приложениях
IPSec	Защита данных между филиалами компании через VPN	Создание защищённых соединений между облачными провайдерами и корпоративными центрами данных	Защита VoIP звонков и других чувствительных данных, передаваемых на мобильных устройствах

В таблице 2 подчеркиваются особенности применения каждого из рассмотренных протоколов в зависимости от типа сети. SSL/TLS чаще всего используется в приложениях, требующих защиты веб-трафика, что делает его оптимальным для корпоративных веб-сервисов и мобильных приложений. В то время как IPSec лучше подходит для защиты данных на сетевом уровне, обеспечивая надежное шифрование для корпоративных VPN и мобильной телефонии. Выбор между этими протоколами определяется требованиями к безопасности, конфигурацией сети и характером трафика.

Анализ уязвимостей и угроз

Анализ уязвимостей и угроз, связанных с протоколами шифрования и защиты данных, играет важную роль в обеспечении безопасности инфокоммуникационных систем. Уязвимости в этих протоколах могут поставить под угрозу конфиденциальность, целостность и доступность данных. В этом разделе мы рассмотрим известные уязвимости и методы их предотвращения.

Известные уязвимости:

Heartbleed (SSL/TLS) – это ошибка в реализации OpenSSL, позволяющая злоумышленникам считывать память сервера, что может привести к утечке конфиденциальной информации, включая приватные ключи и пользовательские данные.

POODLE (SSL 3.0) – уязвимость в протоколе SSL 3.0, позволяющая злоумышленникам расшифровывать зашифрованные данные из-за уязвимости в механизме «padding».

KRACK (Wi-Fi WPA2) – уязвимость в протоколе WPA2, используемом для защиты Wi-Fi сетей, позволяющая атакующим восстанавливать ключи шифрования и подслушивать передаваемые данные.

Методы защиты и снижения рисков включают:

Регулярное обновление программного обеспечения для устранения известных уязвимостей в протоколах и библиотеках.

Использование современных версий протоколов, таких как переход на TLS 1.3, который устраняет многие уязвимости предыдущих версий SSL/TLS.

Применение многофакторной аутентификации для повышения уровня защиты, затрудняя несанкционированный доступ даже в случае возможной утечки данных.

Таблица 3. Уязвимости и методы защиты

Уязвимость	Протокол	Описание уязвимости	Методы защиты

Heartbleed	SSL/TLS	Доступ к памяти сервера и возможность утечки данных	Обновление OpenSSL до последней версии
POODLE	SSL 3.0	Небезопасное использование padding, позволяющее расшифровку данных	Отключение SSL 3.0, использование TLS 1.2 и выше
KRACK	Wi-Fi WPA2	Возможность восстановления ключей шифрования	Обновление прошивки устройств, использование WPA3

Анализ уязвимостей и соответствующие методы защиты подчеркивают важность постоянного обновления и контроля систем безопасности. Уязвимости в протоколах шифрования могут серьезно повлиять на конфиденциальность и целостность данных, однако их можно успешно уменьшить, внедряя рекомендованные методы защиты. Переход на современные технологии и стандарты, такие как TLS 1.3 и WPA3, а также регулярное обновление программного и аппаратного обеспечения, являются ключевыми стратегиями для обеспечения безопасности данных в современных инфокоммуникационных сетях.

Заключение

Исходя из проведенного анализа, можно сделать вывод о необходимости комплексного подхода к защите данных. Это включает в себя не только применение передовых технологий шифрования и использование актуальных версий протоколов, но и создание многоуровневой системы защиты, способной адаптироваться к изменяющимся условиям и угрозам. Важно подчеркнуть, что безопасность данных в инфокоммуникационных сетях – это непрерывный процесс, требующий регулярного пересмотра защитных мер и обновления систем в ответ на новые вызовы в области кибербезопасности.

Список литературы:

1. Биячуев, Т.А. Безопасность корпоративных сетей / Т.А. Биячуев. - СПб: СПб ГУ ИТМО, 2004.- 161 с. Источник: https://www.bibliofond.ru/view.aspx?id=785494 © Библиофонд.
2. Волчков, А. Современная криптография / А.Волчков // Открытые системы.- 2002. - №07-08. -С.48. Источник: https://www.bibliofond.ru/view.aspx?id=785494 © Библиофонд.
3. Гмурман, А.И. Информационная безопасность/ А.И. Гмурман - М.: «БИТ-М», 2004.- 387с. Источник: https://www.bibliofond.ru/view.aspx?id=785494 © Библиофонд.
4. Зима, В. Безопасность глобальных сетевых технологий / В.Зима, А. Молдовян, Н. Молдовян - СПб.: BHV, 2000. - 320 с. Источник: https://www.bibliofond.ru/view.aspx?id=785494 © Библиофонд.

References:

1. Biyachuev, T.A. Security of corporate networks / T.A. Biyachuev. - St. Petersburg: St. Petersburg State University ITMO, 2004.- 161 p. Source: https://www.bibliofond.ru/view.aspx?id=785494 © Bibliofond.

2. Volchkov, A. Modern cryptography / A. Volchkov // Open Systems. - 2002. - No. 07-08. - P.48. Source: https://www.bibliofond.ru/view.aspx?id=785494 © Bibliofond.
3. Gmurman, A.I. Information security/ A.I. Gmurman - M.: “BIT-M”, 2004.-387p. Source: https://www.bibliofond.ru/view.aspx?id=785494 © Bibliofond.
4. Zima, V. Security of global network technologies / V. Zima, A. Moldovyan, N. Moldovyan - St. Petersburg: BHV, 2000. - 320 p. Source: https://www.bibliofond.ru/view.aspx?id=785494 © Bibliofond.