DOI 10.23859/1994-0637-2018-4-85-4
УДК 004.056.52

Смирнов Денис Вадимович
Инженер, Череповецкое высшее военное инженерное училище радиоэлектроники (Череповец, Россия)
E-mail: deanwalters@yandex.ru

Smirnov Denis Vadimovich
Engineer, Cherepovets Higher Military Engineering College of Radio Electronics (Cherepovets, Russia)
E-mail: deanwalters@yandex.ru

Сотников Александр Иванович
Преподаватель, Череповецкое высшее военное инженерное училище радиоэлектроники (Череповец, Россия)
E-mail: vokintos@rambler.ru

Sotnikov Aleksandr Ivanovich
Teacher, Cherepovets Higher Military Engineering College of Radio Electronics (Cherepovets, Russia)
E-mail: vokintos@rambler.ru

Асеев Алексей Юрьевич
Кандидат технических наук, доцент, Череповецкий государственный университет (Череповец, Россия)
E-mail: passionarij@rambler.ru

Aseev Aleksey Yurievich
PhD in Technical Sciences, Associate professor, Cherepovets State University (Cherepovets, Russia)
E-mail: passionarij@rambler.ru

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМЫ ЭЛЕКТРОННОЙ ПОЧТЫ ОТ ТИПА АТАК «ЧЕЛОВЕК ПОСЕРЕДИНЕ» НА ОСНОВЕ БЛОКЧЕЙНА

E-MAIL SECURITY MAINTENANCE USING BLOCKCHAIN AGAINST "MAN-IN-THE-MIDDLE" TYPE ATTACK

Аннотация. В данной статье рассмотрена проблема и предложено решение обеспечения безопасности системы электронной почты от атак типа «Человек посередине». Решение основано на внедрении в существующие системы защиты дополнительного модуля для предоставления пользователям контрольной суммы и организации блокчейна на клиентской стороне. Результатом реализации данной системы защиты является специальное программное обеспечение "ChainMail".

Ключевые слова: защита информации, безопасность, e-mail, человек посередине, блокчейн, несанкционированное изменение, дерево Меркла

Abstract. This article discusses how to protect E-mail system against "Man in the middle" attack. The solution is based on the introduction of an additional module into existing security systems to provide checksum to users and making a blockchain on the client side. The result of this protection system implementation is the special software "ChainMail".

Keywords: data protection, security, E-mail, Man in the middle, blockchain, unauthorized modification, Merkle tree

Введение

В настоящее время особую значимость представляют вопросы обеспечения конфиденциальности информации, передаваемой через сеть Интернет. В качестве подтверждения можно привести следующие примеры: размещение на сайте “WikiLeaks” скомпрометированной переписки директора ЦРУ, взлом базы данных сайта знакомств “Ashley Madison”, повлекший за собой шантаж участников данного проекта [4].

Одним из распространенных способов передачи информации между корреспондентами является использование электронной почты. Посредством почтовых сообщений осуществляется доставка различной информации, представляющей интерес для злоумышленников. В качестве таких данных могут выступать: личная информация (почтовые переписки, фотографии), информация об электронных платежах и банковские реквизиты, информация об аккаунтах пользователя в различных сервисах и т.д. Таким образом, защита конфиденциальных данных, передаваемых с использованием электронной почты, является задачей актуальной и имеет, ввиду широкого использования данного сервиса в современных информационных системах, большую практическую значимость.

Основная часть

Особенностью эксплуатации электронной почты с точки зрения информационной безопасности является архитектура, состоящая из наборов трех основных компонентов: почтовые сервера, почтовые клиенты и каналы связи.

На рис. 1 представлена обобщенная модель почтового сервиса, которая показывает, что сообщение в процессе передачи может быть перехвачено минимум 7 раз:

1. На персональном компьютере отправителя.
2. При передаче сообщения от отправителя почтовому серверу.
3. На почтовом сервере отправителя.
4. При передаче сообщения между почтовыми серверами.
5. На почтовом сервере получателя.
6. При передаче сообщения почтовым сервером получателю.
7. На персональном компьютере получателя [2].

На основе анализа процесса передачи почтового сообщения можно выделить 3 основных вектора атак на систему электронной почты:

1. Атака на пользователей.
2. Атака на сервер.
3. Атака на канал связи.

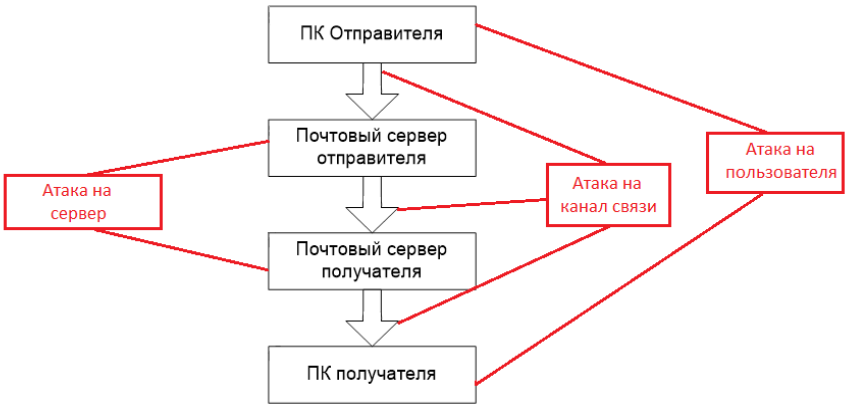

Рис. 1. Векторы атак на электронную почту

В ходе реализации данных угроз целями злоумышленников, в основном, являются перехват и подмена сообщений. В настоящее время защита системы почтовых сообщений организована на базе использования криптографической защиты, которая использует асимметричную систему шифрования. Данная система основана на обратимой функции и двух взаимосвязанных ключах (открытом и закрытом), при этом шифрование сообщения осуществляется на основе открытого ключа, обратный процесс проходит при использовании закрытого ключа. Открытый ключ является публичным, хранится на выделенном сервере и доступен всем пользователям, а закрытый ключ является секретным и хранится только у легитимного пользователя [1].

Но такие системы не гарантируют защиту, если кто-либо получит доступ к серверу и осуществит подмену открытых ключей. В этом случае злоумышленник, подключившись к каналу связи между пользователями, может осуществить вмешательство в протокол передачи, считывая, удаляя или искажая информацию. Такой вид угрозы называется «Человек посередине» (англ. *Man in the middle (MitM)*). Это вид атаки, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом (рис. 2).

Для повышения защищенности таких систем предлагается использовать проверку открытых ключей на стороне клиента на основе блокчейна, который позволяет уникально идентифицировать легитимность пользователей. Данная проверка будет основана на взаимосвязанном хешировании базы данных открытых ключей при помощи дерева Меркла [3].

Рис. 2. Реализация MitM-атаки

Для создания такой проверки предлагается встроить в существующую систему защиты почтовых коммуникаций отдельный модуль, позволяющий проверить легитимность открытых ключей, а также пользователей, участвующих в переписке (рис. 3).

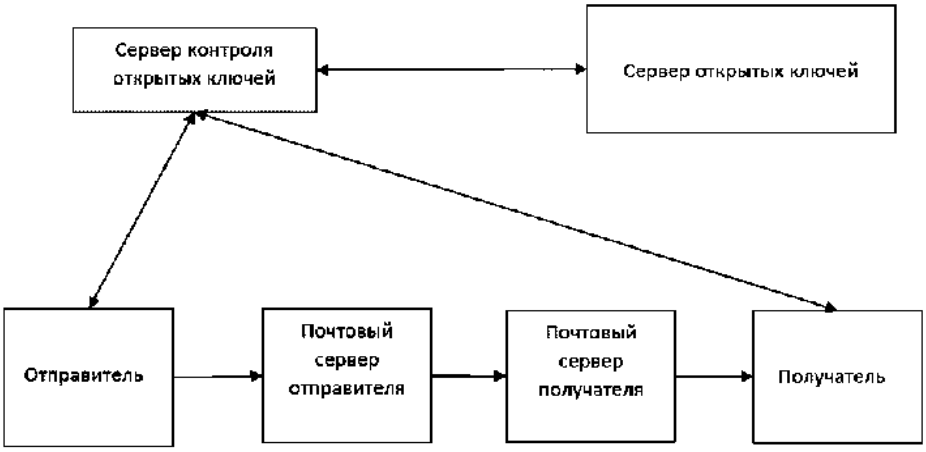

Рис. 3. Архитектура предлагаемой системы защиты

Суть дерева Меркла состоит в том, что каждый лист бинарного дерева (который в нашем случае является записями соответствующего адреса электронной почты и связанного с ним открытым ключом из базы данных) хешируется, а затем из каждой пары хешей поочередно вычисляется следующий хеш. Данная процедура повторяется до тех пор, пока не останется единственный хеш, который и будет являться корнем этого дерева (рис. 4) [5].

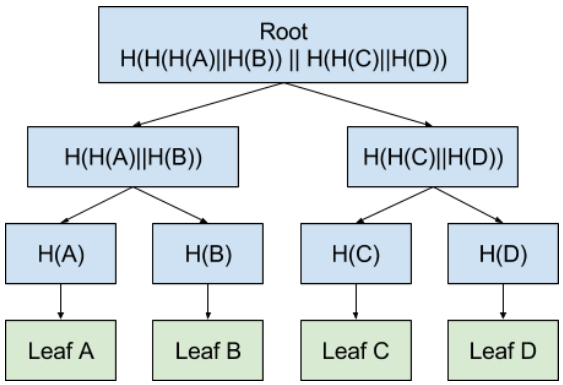

Рис. 4. Формирование хеша при помощи дерева Меркла

Существует три типа узлов, которые хешируются с использованием стойкой к коллизиям функции $H(x)$:

1. Внутренние – узлы, существующие для любого префикса дерева, которые разделяются более чем одним его индексом, присутствующим в дереве. Внутренний узел хеширован следующим образом, подчиняясь двум его детям:

$$H_{interior} = H(H_{child.0} \,||\, H_{child.1}).$$

2. Пустые – узлы, представляющие собой префикс i длины l (глубина l в дереве), который не является префиксом какого-либо пользователя, включенного в дерево (Необходимы для поддержания четного количества листов, а также генерации произвольного количества фиктивных пользователей для усложнения криптоанализа системы). Пустые узлы хешированы как:

$$H_{bmpty} = H(k_{bmpty} \,||\, k_n \,||\, i \,||\, l).$$

3. Листовые узлы представляют индекс i определенного пользователя. Он присутствует в дереве на глубине l (это означает первые l бит из уникального префикса). Узлы листа хешируются следующим образом:

$$H_{lbaf(i)} = H(H(k_{lbaf} \,||\, k_n \,||\, i \,||\, L) \,||\, H(\text{name}_i \,||\, \text{keys}_i)),$$

k_{lbaf} и k_{bmpty} – константы для отличия листовых и пустых узлов; k_n – нумерация ветви; name_i – электронная почта пользователя; keys_i – открытый ключ пользователя.

Результирующий хеш будет основой для проверки пользователями открытых ключей.

Рассмотрим работу данной проверки:

1. При отправке письма пользователь получает из базы данных открытый ключ получателя.

2. После получения открытого ключа пользователь запрашивает проверочную информацию у сервера контроля открытых ключей.

3. Сервер контроля открытых ключей производит генерацию обрезанного дерева Меркла следующим образом:

- производится поиск ячейки в листьях дерева Меркла, содержащей имя пользователя (ячейка 4 на рис. 5);
- производится запись каждого смежного узла на каждом уровне дерева (ячейки (3), (1,2), ((5,6)(7,8)) на рис. 5);

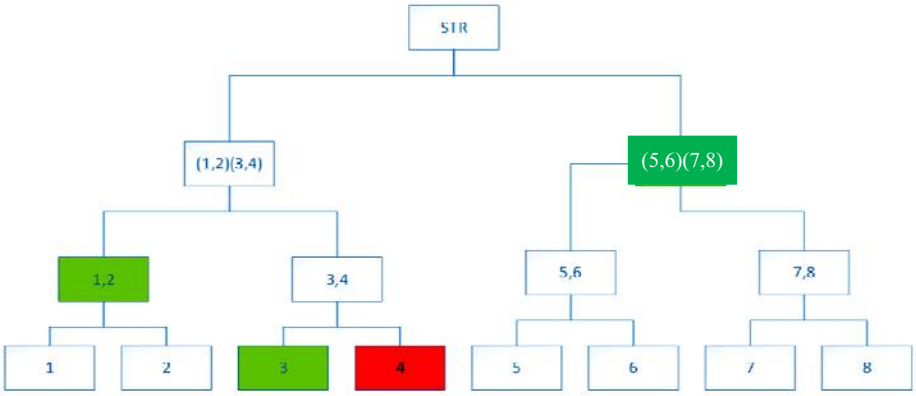

Рис. 5. Определение необходимых записей в дереве

- построение структуры данных из этих блоков, где первый блок – это недостающая информация для хеширования листа дерева Меркла (рис. 6).

Рис. 6. Формирование блокчейна

4. После генерации такой структуры данных сервер контроля открытых ключей подписывает, шифрует эту информацию и отправляет ее пользователю.

5. Пользователь подставляет в первый блок информацию, полученную из базы данных открытых ключей, и хеширует этот блок. После этого последовательно хешируется каждый последующий блок с предыдущим и получается «суммарный» хеш STR’ (рис. 7).

6. Полученное значение пользователь сравнивает с корнем дерева Меркла. Если они равны, значит открытый ключ легитимный, в противном случае можно сделать вывод о том, что сервер скомпрометирован и открытый ключ не принадлежит получателю.

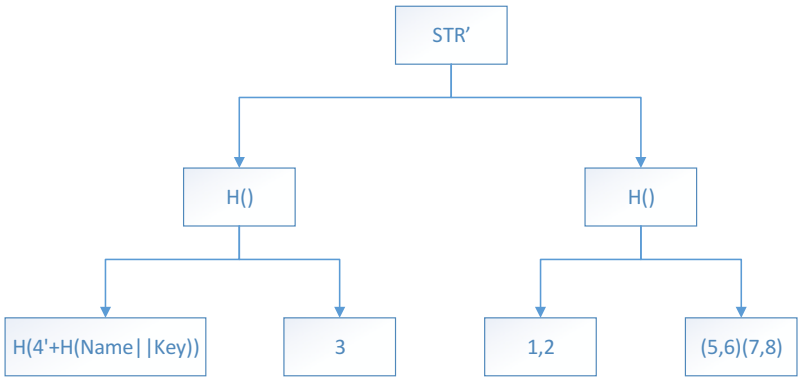

Рис. 7. Вычисление STR’

С таким построением системы приложение позволяет проверять принадлежность определенного открытого ключа к части хеша: когда один пользователь передает сообщение другому, то он проверяет его личность перед отправкой сообщения. Следовательно, пользователь может быть уверен, что прямо сейчас открытые ключи получателя соответствуют именно его аккаунту.

Для обновления базы в системе с заданной периодичностью строится новое дерево и вычисляется новый хеш. Чтобы исключить подмену данных, корень устаревшего дерева Меркла включается в новое и производится перерасчет нового дерева. Дерево заполняется слева направо, а в его структуре содержится доказательство, что каждая новая версия является измененным состоянием предыдущего (рис. 8).

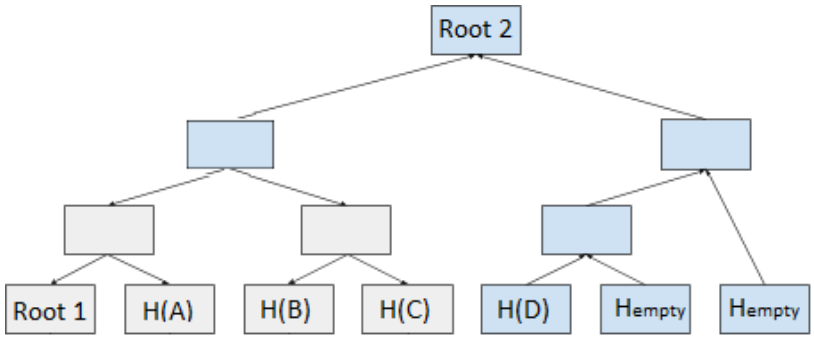

Рис. 8. Построение следующего дерева Меркла

Достоинства использования такой системы:

1. Неопределенность. Действующий в данный момент публичный ключ невозможно обнаружить, так как пользователи оперируют связанными снимками хешей, а проверка ликвидности открытого ключа проверяется на принимающей стороне.

2. Невозможность подмены ключей. Если злоумышленник попытается вставить свой открытый ключ, то клиентское программное обеспечение обнаружит это и предупредит пользователя.

3. Конфиденциальность. Серверам не нужно предоставлять какую-либо конфиденциальную информацию.

4. Скрытое количество пользователей. Такое строение системы позволяет вставлять произвольное количество фиктивных записей в дерево (пустых узлов), которые будут неразличимы от реальных пользователей.

Выводы

В данной работе была рассмотрена проблема возможности несанкционированного просмотра и изменения почтовой переписки при помощи атаки «Человек посередине» и предложено ее решение. Решение основано на проверке открытых ключей на стороне пользователя при помощи связанных цепочек хеш-блоков, которые построены при помощи дерева Меркла. Данный механизм защиты был реализован в прототипе СПО “ChainMail”. Тестирование данного прототипа в реальных условиях показало высокий уровень защиты от рассмотренной угрозы.

Литература

1. Джонсон Дж., Калиски Б. RFC 3447 Стандарты криптографии на основе открытых ключей. 2003.

2. Истлэйк Д. Расширения систем защиты электронной почты. 2014.

3. Мелара М.С. CONIKS. 2014.

4. Habrahabr // URL: https://habrahabr.ru.

5. Sahai A. Fully secure accountableauthority identity-based encryption // Public Key Cryptography–PKC 2011. 2011.

References

1. Jonsson J. and Kaliski B. *RFC 3447 Public-Key Cryptography Standards (PKCS) #1:Cryptography Specifications Version 2.1*, 2003.

2. Eastlake D. *E-mail Security Extensions*. 2009.

3. Melara M.S. *CONIKS: Preserving Secure Communication with Untrusted Identity Providers*. 2014.

4. *Habrahabr* [On-line magazine habrahabr]. Available at: https://habrahabr.ru.

5. Sahai A. Fully secure accountableauthority identity-based encryption. In *Public Key Cryptography–PKC 2011*.

Для цитирования: Смирнов Д.В., Сотников А.И., Асеев А.Ю. Обеспечение безопасности системы электронной почты от типа атак «человек посередине» на основе блокчейна // Вестник Череповецкого государственного университета. 2018. №4(85). С. 31–38. DOI: 10.23859/1994-0637-2018-4-85-4

For citation: Smirnov D.V., Sotnikov A.I., Aseev A.Y. E-mail security maintenance using blockchain against “man-in-the-middle” type attack. *Bulletin of the Cherepovets State University*, 2018, no. 4 (85), pp. 31–38. DOI: 10.23859/1994-0637-2018-4-85-4