СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ ГЕНЕРАЦИИ ОДНОРАЗОВЫХ ПАРОЛЕЙ

Каршакевич В.М., студент гр.567001

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бойправ О.В. – канд. тех. наук, доцент,
заведующий кафедрой защиты информации

Аннотация. Статья посвящена комплексному исследованию современных технологий генерации одноразовых паролей (One-Time Password), которые в настоящее время широко используются для повышения эффективности процесса аутентификации пользователей в информационных системах. В рамках этого исследования проведен анализ алгоритмов HOTP (HMAC-Based One-Time Password Algorithm), TOTP (Time-based One-Time Password), а также методов, используемых для передачи одноразовых паролей. Представлены рекомендации по совершенствованию систем генерации одноразовых паролей, разработанные с учетом результатов проведенного исследования.

Ключевые слова. одноразовый пароль, HOTP, TOTP, аутентификация, информационная безопасность, двухфакторная аутентификация.

Информационные системы на данный момент используют повсеместно: они помогают хранить данные, автоматизировать рутину в бизнесе, налаживать электронный документооборот, управлять ресурсами компании, а также оказывать услуги онлайн. Одним из ключевых методов защиты информации, обрабатываемой в информационных системах, является аутентификация их пользователей.

Многие устоявшиеся методы аутентификации, использующие статические пароли, имеют ряд недостатков, такие как уязвимости каналов передачи одноразовых паролей, возможность реализации атак перехвата и воспроизведения, зависимость некоторых алгоритмов от синхронизации времени, а также необходимость хранения секретных ключей на серверной стороне. Кроме того, существенную угрозу представляют атаки социальной инженерии, при которых пользователь может самостоятельно передать одноразовый пароль злоумышленнику. Такого рода исследования позволяют не только определить проблемные участки, но также найти метод для улучшения.

Цель работы – выполнить анализ уязвимостей современных систем генерации одноразовых паролей и по результатам этого анализа предложить пути усовершенствования таких систем.

Для достижения поставленной цели были поставлены следующие задачи:

– анализ современных алгоритмов генерации одноразовых паролей;

– исследование основных угроз и атак на системы генерации одноразовых паролей;

– оценка криптографической стойкости одноразовых паролей;

– сравнительный анализ методов генерации одноразовых паролей;

– разработка рекомендаций по совершенствованию систем генерации одноразовых паролей.

Характеристики атак на системы генерации одноразовых паролей представлены ниже.

Атаки перехвата (eavesdropping) направлены на получение одноразового пароля в процессе его передачи по каналу связи. Несмотря на ограниченный срок действия одноразового пароля, злоумышленник может использовать его в реальном времени, особенно при реализации атаки типа «man-in-the-middle». В этом случае безопасность системы зависит не только от алгоритма генерации одноразового пароля, но и от защищенности канала передачи [1].

Атаки воспроизведения (replay attacks) заключаются в повторном использовании перехваченного пароля. Большинство систем генерации одноразовых паролей защищены от данного типа атак благодаря одноразовому характеру паролей, однако при наличии временного окна (например, в алгоритме TOTP) существует вероятность успешного повторного использования в пределах допустимого интервала. Дополнительную угрозу создают атаки с опережением по времени (time-shift attacks), когда злоумышленник искусственно рассинхронизирует время на устройстве жертвы и сервере [2].

Существенную угрозу представляют атаки на серверную сторону. В случае компрометации базы данных злоумышленник может получить доступ к секретным ключам (в алгоритмах HOTP и TOTP), что позволяет ему генерировать валидные одноразовые пароли. Это является одним из наиболее критичных недостатков классических систем генерации одноразовых паролей, так как делает скомпрометированным весь будущий сеанс аутентификации [3].

Отдельную категорию составляют атаки социальной инженерии, включая фишинг. Даже при использовании одноразового пароля пользователь может быть обманут и самостоятельно передать одноразовый пароль злоумышленнику. Особенно опасны фишинговые сайты, которые в реальном времени проксируют трафик между жертвой и легитимным сервисом (атака «человек посередине» с перехватом сессии), что позволяет злоумышленнику использовать полученный одноразовый пароль мгновенно, до его истечения.

Большинство одноразовых паролей передаются через SMS, мессенджеры или электронную почту. Протокол SS7 (Signaling System № 7), используемый в сотовой связи, имеет фундаментальные уязвимости, позволяющие злоумышленникам перенаправлять SMS с одноразовыми паролями на свои устройства без физического доступа к SIM-карте жертвы. Таким образом, даже криптографически стойкий алгоритм генерации пароля теряет свою эффективность при использовании небезопасного канала доставки [4].

Таким образом, анализ модели угроз показывает, что повышение безопасности систем генерации одноразовых паролей требует комплексного подхода, включающего как совершенствование алгоритмов генерации, так и защиту каналов передачи и пользовательских сценариев.

Криптографическая стойкость систем генерации одноразовых паролей во многом определяется длиной пароля и используемыми алгоритмами. Как правило, одноразовые пароли представляют собой числовые значения длиной от 6 до 8 символов. Общее количество возможных комбинаций можно оценить как:

$$N = 10^d, \tag{1}$$

где d – количество цифр в пароле.

Для шестизначного одноразового пароля количество возможных значений составляет 10^2 = 1000000. При отсутствии ограничений на количество попыток это делает систему уязвимой к перебору (brute force). Однако на практике применяются механизмы ограничения числа попыток и временные задержки, что существенно снижает вероятность успешной атаки.

Вероятность угадывания одноразового пароля за одну попытку определяется как:

$$P = \frac{1}{10^d} \tag{2}$$

При наличии ограничения на число попыток k, вероятность успешной атаки может быть оценена как:

$$P_k = \frac{k}{10^d} \tag{3}$$

Однако современные распределенные атаки (например, с использованием ботнетов) позволяют злоумышленникам обходить ограничения на количество попыток, распределяя запросы между различными IP-адресами. В связи с этим увеличение длины одноразового пароля (например, до 8-10 символов) становится необходимой, но не достаточной мерой.

Дополнительным фактором является энтропия секретного ключа. В алгоритмах HOTP и TOTP безопасность напрямую зависит от стойкости ключа K и используемой хеш-функции (например, SHA-1, SHA-256). При использовании современных криптографических примитивов вероятность подбора ключа остается пренебрежимо малой [3].

В случае хеш-цепочек безопасность определяется стойкостью хеш-функции к предобразованию (preimage resistance) и коллизиям. Использование современных функций (например, SHA-256) обеспечивает высокий уровень защиты при условии корректной реализации [5].

Сравнение рассмотренных методов позволяет выделить их ключевые характеристики с точки зрения безопасности и практической применимости.

Алгоритмы HOTP и TOTP отличаются простотой реализации и широким распространением, однако требуют хранения секретного ключа на сервере. Это делает их уязвимыми при компрометации серверной базы данных. Кроме того, алгоритм TOTP критически зависит от точности синхронизации времени. При расхождении часов сервера и клиента более чем на допустимый интервал (обычно 30–60 секунд) аутентификация становится невозможной без ручного вмешательства.

Методы на основе хеш-цепочек, напротив, минимизируют необходимость хранения секретных данных на сервере, что повышает устойчивость к утечкам. Однако они уступают по удобству использования из-за необходимости управления цепочками и их ограниченной длины. После исчерпания цепочки требуется повторная инициализация, что снижает удобство для пользователя.

С точки зрения устойчивости к атакам можно отметить, что: алгоритм HOTP уязвим к рассинхронизации счетчика; алгоритм TOTP зависит от точности времени и подвержен атакам с использованием временных окон; хеш-цепочки ограничены по ресурсу использования и требуют сложного механизма восстановления; все методы подвержены атакам перехвата при отсутствии защищенного канала.

Таким образом, ни один из подходов не является универсальным решением, что подтверждает необходимость разработки комбинированных моделей, компенсирующих недостатки друг друга.

Реализация комбинированной системы генерации одноразовых паролей требует учета ряда практических аспектов.

Безопасная инициализация. Во-первых, необходимо обеспечить безопасную инициализацию системы, включая генерацию исходного секретного значения и начального элемента хеш-цепочки. Инициализация должна происходить в защищенной среде (например, с использованием протокола

TLS 1.3) с проверкой подлинности сервера, чтобы исключить возможность внедрения злоумышленником собственных параметров в процессе первоначальной настройки [6].

Выбор функции вывода ключей (KDF). Во-вторых, важным является выбор функции вывода ключей. Она должна обладать свойствами устойчивости к атакам перебора (brute-force) и обеспечивать равномерное распределение выходных значений. В качестве таких функций могут использоваться PBKDF2, HKDF или Argon2. Argon2 рекомендуется к использованию в новых системах благодаря устойчивости к атакам с использованием GPU и ASIC [4].

Производительность и масштабируемость. В-третьих, необходимо учитывать производительность системы. Добавление нескольких факторов (хеш-цепочка, время, идентификатор сессии) в процесс генерации одноразового пароля увеличивает вычислительную нагрузку. Для высоконагруженных систем критически важно использовать эффективные алгоритмы или распределение вычислений.

Защита от атак повторного воспроизведения. Также следует уделить внимание защите от атак повторного воспроизведения. Для этого одноразовый пароль должен быть привязан не только к времени, но и к конкретной сессии или контексту аутентификации. Это может быть реализовано путем включения дополнительного параметра (например, идентификатора сессии или уникального nonce) в функцию генерации. Такой подход делает перехваченный пароль бесполезным для злоумышленника.

На основе проведенного анализа предлагаются следующие рекомендации по усовершенствованию системы генерации одноразовых паролей.

1. Отказ от SMS как канала доставки. В случае высоких требований к безопасности (финансовый сектор, государственные информационные системы) следует использовать push-уведомления в защищенных приложениях или аппаратные токены, исключающие перехват через уязвимости SS7.

2. Многофакторность генерации. Генерировать одноразовый пароль на основе комбинации трех факторов: секретного ключа (хранящегося в защищенном элементе TPM на устройстве пользователя), временной метки (ограниченной окном в 15-30 секунд) и идентификатора сессии.

3. Защита серверной стороны. Секретные ключи на сервере не должны храниться в открытом виде. Использование аппаратных модулей безопасности (HSM) или методов разделения секрета (threshold cryptography) позволяет исключить компрометацию всей системы при взломе одной из баз данных [3].

4. Адаптивная политика ограничений. Внедрение адаптивных механизмов блокировки, которые увеличивают задержку при неудачных попытках не линейно, а экспоненциально, а также учитывают геолокацию и поведенческие факторы пользователя.

Дальнейшие исследования могут развиты по следующим направлениям.

1. Интеграция с биометрией. Одним из перспективных направлений является интеграция одноразовый пароль с биометрическими факторами аутентификации, что позволяет создать многоуровневые системы защиты. Биометрические данные могут выступать в роли фактора владения (после первичной регистрации) или использоваться для динамической генерации ключа.

2. Аппаратные средства безопасности. Другим направлением является использование аппаратных средств, таких как токены безопасности (U2F/WebAuthn) и Trusted Platform Module (TPM), для хранения секретных данных и выполнения криптографических операций. В отличие от программных одноразовых паролей-генераторов, аппаратные средства исключают возможность извлечения ключа даже при заражении устройства пользователя вредоносным ПО.

3. Применение машинного обучения. Кроме того, интерес представляет применение методов машинного обучения для выявления аномалий в процессе аутентификации. Это позволяет дополнительно повысить уровень безопасности за счет анализа поведения пользователя (тайминг нажатия клавиш, характерные местоположения, типичные устройства).

4. Постквантовая криптография. Наконец, развитие постквантовой криптографии может оказать влияние на алгоритмы генерации одноразовых паролей. Алгоритмы, основанные на цепочках хешей (которые устойчивы к квантовым атакам в большей степени, чем асимметричные схемы), могут стать основой для будущих стандартов аутентификации в постквантовый период [5].

Список использованных источников:

1. HOTP: An HMAC-Based One-Time Password Algorithm / D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen // RFC 4226. – 2005. – 34 p.

2. TOTP: Time-Based One-Time Password Algorithm / D. M'Raihi, S. Machani, M. Pei, J. Rydell // RFC 6238. – 2011. – 14 p.

3. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes / J. Bonneau, C. Herley, P. C. van Oorschot, F. Stajano // Proceedings of the IEEE Symposium on Security and Privacy. – 2012. – P. 553–567.

4. Digital Identity Guidelines: Authentication and Lifecycle Management / P. A. Grassi, M. E. Garcia, J. L. Fenton // NIST Special Publication 800-63B. – 2017. – 77 p.

5. Post-quantum cryptography / D. J. Bernstein, T. Lange // Nature. – 2017. – Vol. 549, No. 7671. – P. 188–194.

6. The Transport Layer Security (TLS) Protocol Version 1.3 / E. Rescorla // RFC 8446. – 2018. – 160 p.