УДК 004.056.55

МЕХАНИЗМ АДАПТИВНОГО ФОРМИРОВАНИЯ ЭПОХ MERKLE-ДЕРЕВА ДЛЯ ПРЕДОТВРАЩЕНИЯ МАНИПУЛЯЦИЙ С ДАННЫМИ В IOT-СИСТЕМАХ

Белокобыльский И.В.[1]
Научный руководитель – канд. техн. наук, доцент Харитонов А. Ю.[1]
[1]Университет ИТМО
ilya.belokobylsky@gmail.com

Работа выполнена в рамках темы НИР №2 «Проектирование механизма адаптивного формирования эпох Merkle-дерева для предотвращения манипуляций с данными в IoT-системах».

Введение

IoT-системы применяются в критически важных сферах, где необходимо обеспечить целостность и защиту от манипуляций с данными [1]. Поскольку вычислительные ресурсы устройств ограничены [2], используются агрегирующие решения. Одними из них стали Merkle-деревья [3]. Однако в их реализации есть ограничение – механизм накапливания данных в эпохи, для которых вычисляется корневой хэш [3]. Размер эпохи, задающийся статически в большинстве систем, напрямую влияет на задержку фиксации, вычислительную нагрузку и размер доказательства вхождения данных. При увеличении размера повышается риск атак подмены или потери данных, а при уменьшении – риск чрезмерного использования ресурсов. Существующие адаптивные подходы фокусируются на структуре дерева для масштабируемости, но не затрагивают динамику управления размером эпохи [4]. Поэтому в работе приведен механизм адаптивного формирования эпох, а также проведено его экспериментальное тестирование.

Основная часть

В рассматриваемой модели IoT-устройства аутентифицируются с использованием HMAC. Шлюз считается доверенным компонентом. Вводится понятие окна уязвимости – интервала между поступлением события на шлюз и фиксацией корня Merkle-дерева во внешнем хранилище. В течение этого интервала данные существуют только на шлюзе. Чем он длиннее, тем выше риски: потери данных при сбое шлюза, невозможности аудита и проверки целостности до момента фиксации, а в случае недоверенного брокера сообщений – возможности манипуляции при передаче [5]. Для окна уязвимости управляющим параметром является размер эпохи. Малая эпоха сокращает окно, но порождает частые операции фиксации и нагружает шлюз. Большая – снижает нагрузку, но оставляет данные незащищёнными дольше.

Предлагается механизм определения размера эпохи пропорционально текущей интенсивности данных и целевому интервалу задержки фиксации. Это обеспечивает приближенную инвариантность среднего окна уязвимости при изменении нагрузки. Корректировка происходит за счет следующих факторов: 1) длины очереди необработанных событий; 2) задержки подтверждения записи во внешнее хранилище; 3) загрузки вычислительных ресурсов шлюза; 4) интенсивности поступающих данных. Каждый фактор выполняет отдельную роль. Размер эпохи пропорционален интенсивности потока, чтобы окно уязвимости оставалось постоянным. Увеличение задержки фиксации увеличивает эпоху для снижения частоты обращений к хранилищу. Высокая загрузка CPU аналогично увеличивает эпоху для экономии вычислительных ресурсов. При заполнении очереди необработанных событий эпоха, напротив, сокращается для предотвращения переполнения буфера. Также вводятся ограничения на размер эпохи для обеспечения устойчивости. Помимо штатной корректировки предусмотрен механизм досрочного закрытия эпохи при обнаружении аномалий. Для

каждого параметра телеметрии вычисляется скользящее среднее в пределах окна фиксированного размера. Предусмотрен также параметр критичности данных, который свидетельствует о необходимости немедленного завершения эпохи.

Решение оценено экспериментально в виртуализированной среде. Моделировался поток телеметрии с переменной интенсивностью, включая повышенную нагрузку и деградацию канала связи между шлюзом и хранилищем. В качестве метрик использовались размер окна уязвимости максимально и в среднем, частота операций фиксации и длина очереди при пиковой нагрузке. Адаптивный механизм удержал окно уязвимости в заданных рамках во всех сценариях. Фиксированный размер эпохи при тех же условиях приводил либо к росту задержки фиксации при большом значении, либо к перегрузке шлюза. Таким образом, предложенный подход обеспечивает предсказуемое поведение IoT-системы без ручного вмешательства за счет адаптивного управления размером эпохи Merkle-дерева.

Выводы

В работе рассмотрена проблема статического задания размера эпохи Merkle-дерева. Предложен адаптивный механизм, опирающийся на понятие окна уязвимости – времени от поступления события до записи корневого хэша в хранилище. Решение подстраивает размер эпохи под уровень загрузки CPU, стабильность сети, интенсивность и очередь из входящего потока данных. Экспериментальное сравнение с фиксированной политикой формирование эпох показало работоспособность подхода. Окно уязвимости удерживалось в допустимых рамках в различных условиях нагрузки и деградации канала связи без ручной настройки параметров. Полученные результаты могут быть использованы при проектировании IoT-систем в условиях ограниченных вычислительных ресурсов и изменяющегося потока телеметрии, где требуется высокая пропускная способность и предсказуемая защита целостности данных.

Литература

1. Alaba F. A., Othman M., Hashem I. A. T., Alotaibi F. Internet of Things security: A survey // Journal of Network and Computer Applications. 2017. Vol. 88. P. 10–28. DOI: 10.1016/j.jnca.2017.04.002
2. Kumar S., Kumar D., Dangi R., Choudhary G., Dragoni N., You I. A Review of Lightweight Security and Privacy for Resource-Constrained IoT Devices // Computers, Materials & Continua. 2024. Vol. 78, No. 1. P. 31–63. DOI: 10.32604/cmc.2023.047084
3. Crosby S. A., Wallach D. S. Efficient Data Structures for Tamper-Evident Logging // Proceedings of the 18th USENIX Security Symposium. Berkeley, CA: USENIX Association, 2009. P. 317–334.
4. Kuznetsov O., Chepurnoy A., Yezhov A. Adaptive Restructuring of Merkle and Verkle Trees for Enhanced Blockchain Scalability // Internet of Things. 2024. Art. 101315. DOI: 10.1016/j.iot.2024.101315.
5. Zhao R. et al. Rethinking tamper-evident logging: A high-performance, co-designed auditing system //Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security. – 2025. – С. 2624-2638.