Математические структуры и моделирование 2024. № 1 (69). С. 117–126

УДК 004.056
DOI 10.24147/2222-8772.2024.1.117-126

РАЗЛИЧНЫЕ СХЕМЫ И ПОДХОДЫ К ПРОЦЕССАМ ЖУРНАЛИРОВАНИЯ

В.Н. Семенихин
аспирант, e-mail: svladimir-99@mail.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Вычислительная среда требует надёжного и комплексного процесса для отслеживания и документирования действий пользователей для поддержания доверия к системе. Для этой цели используется журналирование. Однако журналы, которые создаются в процессе жизненного цикла информационной системы, уязвимы для множества атак, в том числе модификации журналов, возможности стирания журналов и раскрытия конфиденциальности пользователя. Для решения этих проблем создано множество схем. Каждая из них имеет свои особенности и свои взгляды на процессы журналирования. Даётся обзор различных схем для защиты журналов, подходов к процессу журналирования.

Ключевые слова: схемы журналирования, схемы логирования, логирование.

Введение

Вычислительная среда требует надёжного и комплексного процесса для отслеживания и документирования действий пользователей, внутренних и сторонних сервисов для поддержания доверия к системе. Для этой цели используется журналирование. Требуется уточнить, что логирование и журналирование очень близкие понятия, которые описывают один и тот же процесс. Однако главное отличие этих процессов в их документированности. В случае журналирования все процессы и алгоритмы описаны в руководстве пользователя, тогда как в случае процесса логирования некоторый функционал может оставаться сокрытым. Далее будем говорить про подходы, которые имеют чётко описанную структуру, соответствующую понятию «журналирование». Благодаря данному процессу мы можем установить наблюдение за системой, действиями администраторов и пользователей. Однако в современном мире журналы уязвимы для множества атак, таких как подделка, модификация, возможность стирания журналов или раскрытие конфиденциальности пользователя. К этому следует добавить и действия администраторов, поскольку они имеют неограниченный доступ к журналам, могут создавать, модифицировать и даже удалять их. Защита журналов от вредоносных действий является крайне важной задачей их ведения. Существующие схемы имеют ряд ограничений, включая изменяемость, трудоёмкость вычислений, отсутствие семантики, также остро стоит вопрос верифицируемости. Целью этой статьи является знакомство с различными схемами для защиты журналов, с подходами к процессу журналирования.

1. Связанные проблемы и критерии оценки

В наши дни информационные технологии не перестают развиваться и совершенствоваться. Системы становятся всё более комплексными, усложняя как свою структуру, так и функционал. Данные, циркулирующие в таких системах, тоже выходят на новый уровень. Их объём стремительно растёт с развитием информационных систем, появляется неоднородность из-за различий между платформами, появляется больше работы, связанной с их безопасностью. Подобное целостное видение вызывает некоторые опасения, например какой уровень безопасности эти системы могут обеспечить? И как они обеспечивают и защищают конфиденциальность своих пользователей? Могут ли они в достаточной степени обеспечить целостность данных пользователей? Для удовлетворения нужд клиентов и заинтересованных сторон в информационных системах необходимы комплексные механизмы безопасности. Функциональность и производительность информационных систем, включая их устройства, можно отслеживать и исследовать путём анализа журналов, генерируемых взаимосвязанными устройствами, и обеспечивать централизованный мониторинг в информационных системах. Подотчётные журналы аудита могут обеспечить более высокий уровень доверия для поставщиков услуг и арендаторов. Доверие и управление доверием очень важно для сервиса, инфраструктуры, надёжности предоставляемых услуг и всей информационной системы в целом.

Также, говоря о журналировании, нельзя забывать о компьютерной криминалистике. Для успешного расследования инцидентов требуется защита журналов от несанкционированного доступа. В критериях оценки доверенных вычислительных систем [1] требования безопасности журналов аудита описываются следующим образом: «информация аудита должна выборочно храниться и защищаться, чтобы действия, влияющие на безопасность, можно было отследить до ответственной за них стороны» и «данные аудита должны быть защищены от изменения и несанкционированного уничтожения, а также позволять обнаруживать и расследовать нарушения безопасности». Здесь важно отметить, что результаты экспертизы любых сервисов зависят от состояния исходных журналов [2].

Администраторы в режиме непосредственного и удалённого доступа и поставщики услуг имеют полный доступ к соответствующим ресурсам и могут представлять серьёзную угрозу информационной безопасности. Защита ресурсов информационной системы является ключевым требованием для надёжной среды. Журналы аудита используются для мониторинга производительности, ресурсов, действий администраторов и пользователей. Журналирование помогает устранять проблемы в информационной системе. Эти журналы неоднородны в силу отсутствия требований к их реализации, поэтому часто структуры данных бывают непонятны вычислительным системам, поскольку им не хватает данных о семантике. Чтобы воспользоваться преимуществами журналирования и получить неизменяемую систему хранения с поддержкой гетерогенности, семантически обогащённую, и при этом иметь встроенную функция обмена статистикой для заинтересованных сторон, необходимо решить следующие проблемы:

1. Обеспечение конфиденциальности, целостности, доступности.
2. Неоднородность журналов.

3. Проблема угроз злонамеренных пользователей.
4. Вопрос семантики.
5. Вопрос энергозависимости хранилищ журналов.

Для защиты целостности журналов уже проделана большая работа и до сих пор продолжаются поиски наилучшего решения. В этой статье мы упомянем такие решения, как: BAF, BAFi и Fi-BAF, FssAgg, SecLaaS, SecLaaS-RW, BBox, SLOPPI, D-CAM, EmLog, Flogger, smartFIX, а также подходы на аппаратном уровне. Обеспечение безопасности (конфиденциальность, целостность, доступность), неизменяемости, семантики является критически важным вопросом схем журналирования.

2. Классические подходы и схемы

Для журналирования доступно множество различных решений. Решения для управления информацией о безопасности и событиях (SIEM) с открытым исходным кодом, такие как GFI Events Manager, Syslog-ng, Manage-Engine Log Storage and Analyser, LOGalyze, Splunk Enterprise и т. д., – вот несколько примеров таких решений. Стоит упомянуть различные DLP системы, которые тесно взаимодействуют с журналами и данными внутри информационной системы, а также помогают в расследовании инцидентов. Стоит также сказать про решения для анализа и поиска данных, такие как OpenSearch [3] или его отечественный аналог Arenadata LogSearch [4]. Они представляют собой легкомасштабируемую систему для обеспечения быстрого доступа и реагирования на большие объёмы данных, независимо от их формата. Все эти решения способны хранить и анализировать журналы различных устройств. Системные администраторы имеют полный контроль над журналами в таких системах, и целостность хранилищ таких журналов объективно не может быть гарантирована. Обратим внимание на такой параметр, как неизменяемость данных. Для поддержания целостности журналов даже после компрометации системы исследователи предлагаются разные решения. Рассмотрим некоторые из них.

2.1. Подходы на основе криптографии

В первом из примеров обеспечения безопасности данных используются асимметричные схемы шифрования. LogCrypt7 – асимметричная схема шифрования для обеспечения безопасности журналов, где журналы защищены шифрованием и доступны для публичной проверки. В этой схеме существуют дополнительные накладные расходы на шифрование, процессы дешифрования и сохранение ключей для этих типов шифрования.

Схемы на основе подписей с использованием шифрования, такие как BAF, BAFi, Fi-BAF и т. д., были предложены в [5–7]. Проблема данного решения в том, что журнал будет накапливать записи в течение длительного периода, а количество подписей, сохраняемых для проверки журнала, будет пропорционально расти. Это привело к новому решению на основе агрегирования. Схема FssAgg [8] была предложена для безопасной аутентификации на основе агрегирования этих подписей, чтобы защитить только ранее вошедшие в систему длинные сеансы. В схеме аутентификации FssAgg подписи с прямой защитой (MAC), сгенерированные одним и тем же под-

писывающим лицом, последовательно объединяются в одну совокупную подпись. Успешная проверка совокупной подписи эквивалентна проверке каждой подписи компонента. Неудачная проверка совокупности подписей подразумевает, что подпись хотя бы одной компоненты недействительна [9].

2.2. Подходы на основе облачных вычислений

В сценарии облачных вычислений для пользователей облака также предлагается ведение журнала как услуги. Эта схема также зависит от надёжности и добросовестности поставщиков облачных услуг, где арендаторы системы имеют возможность манипулировать этими журналами. Схема получения, хранения и анализа этих журналов через использование центрального сервера журналов SecLaaS предложена в [10] через использование облачных функций для хранения журналов. Но это дискуссионное решение, так как администраторы облака все ещё могут представлять угрозу. Эта система хранит данные виртуальных машин и предоставляет доступ криминалистам, обеспечивая конфиденциальность пользователей облака. Кроме того, SeclaaS защищает целостность журналов от нечестных следователей или поставщиков облачных услуг. К тому же реализация SecLaaS выполнена в OpenStack – популярной облачной платформе с открытым исходным кодом. Однако у этой схемы всё ещё остаётся проблема вседозволенности администраторов, что ставит целостность данных под сомнение.

В [11] авторы предложили Seclaas-RW, используя «двустороннее нанесение водяных» знаков, где журналы хранятся в облаке в течение более длительного времени и аутентификация контента осуществляется при помощи нанесения обратимых водяных знаков. При таком подходе возможна только криминалистическая проверка подлинности контента, тогда как другие параметры безопасности отсутствуют.

Цифровой чёрный ящик (BBox) [12], обеспечивающий аутентичное архивирование в распределённых системах, создан для обеспечения подлинности и конфиденциальности журналов. Он основан на криптографии с открытым ключом. BBox использует стандартные примитивы для обеспечения подлинности записей во время передачи от устройств к источнику данных, а также во время хранения на источнике и извлечения аудиторами. В этом решении появляется дополнительная сущность, которая по сути становится единой точкой отказа всей системы.

Схема SLOPPI [13] сделана на основе шифрования для обеспечения целостности журналов и их соответствия заданной политике. В этом решении на журналирование обращают внимание с позиции администрирования и расследования инцидентов. Схема направлена на то, чтобы защитить журналы от злоумышленников, при этом оставив возможность администраторам выполнять свои базовые задачи. В этом решении обеспечение неизменности и семантики журналов отсутствует, нет защиты и от недобросовестности администраторов.

Анонимизация данных журнала путём переноса всей инфраструктуры в облачные хранилища, как предложено в [14], помогает обеспечить конфиденциальность данных, но другие требования безопасности данных при таком подходе отсутствуют.

Хенце с соавторами предложили структуру D-CAM [15] для безопасного журналирования в IoT. Предлагаемая структура позволяет осуществлять контроль и

управление из центра для защиты сети IoT от поставщика облачных услуг со злыми намерениями. Система определяет и регистрирует управляющие сообщения в резервных местах для проверки через различные шлюзы. Сообщения журнала проверки используются для выявления злонамеренного поведения, что помогает защитить облачный IoT от блокировки, вставки, удержания и изменения порядка сообщений.

2.3. Подходы на аппаратном уровне

Некоторые исследователи предложили аппаратные схемы безопасного ведения журнала. В [16] авторы представили хранение журналов в рамках концепции обеспечения целостности и неизменяемости с использованием сценариев однократной записи и многократного чтения (WORM). В качестве дополнения, блок управления чтением/записью отключает операции стирания в секторах, содержащих поля с уникальным форматированием, но разрешает такие операции в секторах, которые не содержат таких полей, чтобы разрешить тестирование калибровки и ведение списков дефектов носителей.

Защищённое от несанкционированного доступа хранение журналов с использованием Trusted Platform Module 2.0 (TPM) описано в [17]. Это обеспечивает решение практических проблем, в том числе обработку частого обновления журналов, экономию дискового пространства и эффективную проверку произвольного подмножества журналов. Для обеспечения гарантии защиты от несанкционированного доступа создан безопасный протокол регистрации.

Система EmLog [18] создана для защищённого хранения от несанкционированного доступа и защиты от модификаций. Данная схема разработана для ограниченных устройств с доверенной средой выполнения. Доверенная среда выполнения (TEE) – безопасная область главного процессора. Она помогает защитить код и данные, загруженные в него, с точки зрения конфиденциальности и целостности. Целостность данных предотвращает изменение данных неавторизованными объектами за пределами TEE, а целостность кода предотвращает замену или изменение кода в TEE неавторизованными объектами.

Все рассмотренные выше аппаратные схемы ограничены с точки зрения ресурсов и обработки. Их мощность, стоимость и доступность не подходят для более крупных сетей с множеством вычислительных блоков. Аналогично, другие неаппаратные схемы не могут в полной мере обеспечить неизменность, семантику и распределение статистики журналов.

2.4. Подходы на основе файловых систем

Flogger [19] передаёт информацию из пространств ядра как виртуальных машин (VM), так и физических машин (PM) в облаке, обеспечивая тем самым полную прозрачность всего ландшафта данных в облаке. С помощью Flogger над ним можно построить сервисы, чтобы предоставить облачным провайдерам, конечным пользователям и регулирующим органам соответствующую информацию о происхождении данных. Схема позволяет конечному пользователю отслеживать, был ли «тронут» его файл неавторизованным пользователем.

Защищённая пересылка журнала и подпись только для добавления (LogFAS) [20] достигает наиболее желательных свойств как симметричных схем, так и схем на основе РКС. LogFAS может создавать публично проверяемые подписи с прямой защитой и ограниченной возможностью добавления без необходимости какой-либо онлайн-поддержки доверенного сервера или фактора времени.

2.5. Другие подходы к журналированию

Также стоит отметить использование структур данных «только для добавления», представленных в схеме Balloons [21]. Данная схема хранения записей журнала заключается в подходе, когда изначально доверенный автор хранит данные на недоверенном сервере или хранилище, а пользователи могут запрашивать доступ к ней или различным её версиям. Описанная структура называется аутентифицируемой, в том смысле, что каждая операция, совершаемая с данными, будет зафиксирована (через механизм снимков) и доступна для публичной проверки. Данная схема предназначена для смягчения предположения о доверии для обеспечения прозрачности изменений, а также сохраняет конфиденциальность ведения журнала.

Интересный подход к журналированию на основе семантики smartFIX был предложен в ссылках [22, 23]. В этом решении документы классифицируются автоматически на основе методов свободной формы и форм-анализа. Соответствующие данные извлекаются с использованием разных методов для каждого типа документа, который проверяется и оценивается через базу данных сопоставления и другие сложные методы, основанные на предыдущих знаниях. Качество данных обеспечивается за счёт математических и логических проверок. Данные, которые точно распознаны, публикуются для прямого экспорта. Иные, неуверенно распознанные данные пересылаются для ручной проверки. По своей сути это решение, которое создано для того, чтобы получить данные независимо от источника и формата, в котором они представлены. Это решение полностью закрывает вопросы гетерогенности и семантики. К сожалению, безопасность, неизменяемость и другие базовые требования остаются вне поля этого решения.

Также следует упомянуть решения на основе блокчейна. В Scytl [24] используется технология, называемая неизменяемыми журналами, которая используется в решениях для электронного голосования. Это обеспечивает целостность, подлинность и неотказуемость созданных журналов, поэтому в случае каких-либо событий аудиторы могут использовать их для расследования инцидентов.

На основании этого исследования были выделены некоторые схемы, их сравнение представлено в табл. 1 и 2.

Заключение

Проблемы организации журналирования, связанные с обеспечением безопасности, целостности, конфиденциальности, гетерогенности, неизменяемости, существуют уже много лет. За это время проблемы были рассмотрены по-разному и с использованием разных технологий. Важно помнить, что угрозы по отношения к системе аудита никуда не исчезают, а компании всё больше оцифровывают свой

Таблица 1. Сравнение схем журналирования

Схема	Краткое описание и сильные стороны	Вопросы
LogCrypt	Публично верифицируемые журналы	Проблемы с производительностью
FssAgg	Последовательная агрегация подписей, основанная на длинных сессиях	Только для активных сессий
BAF	Система, основанная на подписях(MAC)	Проблемы с производительностью, проблемы с излишним потреблением памяти
Balloons	Структура данных для хранения на недоверенном хранилище	Вопросы в отношении потребления памяти
BBox	Решение в рамках распределённых вычислительных систем, сохраняется публичная верифицируемость	Проблемы с производительностью, единая точка отказа
LogFAS	Публичная верифицируемость	Проблемы с производительностью
smartFIX	Взгляд на процесс журналирования на основе семантики	Не уделено внимание остальным параметрам безопасности
BAF / FI-BAF	Агрегирование, уменьшение затрат на вычисление	Проблемы с производительностью в области криптографии, вопросы по распределению логов
SLOPPI	Централизованный центр журналирования	Отсутствует безопасность журналов
SecLaaS	Централизованный центр журналирования, дополнительный уровень защиты от злоумышленников, ориентирование на заданную политику	Вопросы целостности и неизменяемости остаются закрытыми не полностью, данные из журналов могут быть модифицированы или удалены администраторами
SecLaaS-RW	Добавление проверки подлинности, сильный механизм аутентификации	Не продумана работа в режиме реального времени и работа с хранилищами
D-CAM	Система основанная на технологии распределенного реестра (DLT)	Описана только конфигурация хранилища журналов

Таблица 2. Сравнение схем журналирования (продолжение). К – конфиденциальность, Ц – целостность, Д – доступность, Н – неизменяемость, Г – гетерогенность, С – семантика

Схема	К	Ц	Д	Н	Г	С
LogCrypt	+	+	–	+	–	–
FssAgg	–	+	–	+	–	–
BAF	–	+	-	+	–	–
BBox	+	+	–	+	–	–
LogFAS	–	+	–	+	–	–
smartFIX	–	–	–	–	+	+
BAF / FI-BAF	–	+	–	+	–	–
SLOPPI	–	+	–	+	–	–
SecLaaS	–	+	+	–	–	–
SecLaaS-RW	+	+	–	+	–	–
D-CAM	+	+	+	+	–	–

бизнес. Именно поэтому стоит обращать внимание на то, какие риски имеются у организации, какие методы и какие технологии стоит применять для того, чтобы избавиться от рисков или сделать их приемлемыми.

Литература

1. Qiu L., Zhang Y., Wang F., Kyung M., Mahajan H.R. Trusted Computer System Evaluation Criteria. National Computer Security Cente, 1985.
2. Ye F., Zheng Y., Fu X., Luo B., Du X., Guizani M. TamForen: a tamper-proof cloud forensic framework // Transactions on Emerging Telecommunications Technologies. 2020. Vol. 33, Iss. 4.
3. Opensearch. URL: `https://opensearch.org` (дата обращения: 05.01.2024).
4. Arenadata LogSearch. URL: `https://docs.arenadata.io/adls/index.html` (дата обращения: 05.01.2024).
5. Yavuz A.A., Ning P. Baf: an efficient publicly verifiable secure audit logging scheme for distributed systems // 2009 Annual Computer Security Applications Conference. 2009. P. 219–228.
6. Yavuz A.A., Ning P., Reiter M.K. BAF and FI-BAF: efficient and publicly verifiable cryptographic schemes for secure logging in resource-constrained systems // ACM Transactions on Information and System Security. Vol. 15, Iss. 2. Art. 9, P. 1–28.
7. Kampanakis P, Yavuz A.A. BAFi: a practical cryptographic secure audit logging scheme for digital forensics // Secure Community Network. 2015. Vol. 8, Iss. 17. P. 3180–3190.
8. Ma Di, Tsudik G. Forward-secure sequential aggregate authentication // IEEE. 2007. URL: `https://eprint.iacr.org/2007/052` (дата обращения: 02.01.2024).

9. Ma Di, Tsudik G. A New Approach to Secure Logging // Data and Applications Security XXII, 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security, London, UK, July 13-16, 2008, Proceedings. Vol. 5094. P. 48–63.
10. Zawoad S, Dutta AK, Hasan R. SecLaaS: secure logging-as-a-service for cloud forensics // ASIA CCS '13. 2013. P. 219–230.
11. Khan A, Yaqoob A, Sarwar K, Tahir M, Ahmed M. Secure logging as a service using reversible watermarking // Procedia Computer Science. 2017. Vol. 110. P. 336–343.
12. Accorsi R. BBox: a distributed secure log architecture // EuroPKI. Public Key Infrastructures, Services and Applications. 2010. P. 109–124.
13. Von Eye F., Schmitz D., Hommel W. SLOPPI-A Framework for Secure Logging with Privacy Protection and Integrity // ICIMP. 2013.
14. Rajalakshmi J.R., Rathinraj M., Braveen M. Anonymizing log management process for secure logging in the cloud // International Conference on Circuits, Power and Computing Technologies. 2014. P. 1559–1564.
15. Henze M., Wolters B., Matzutt R., Zimmermann T., Wehrle K. Distributed configuration, authorization and management in the cloud-based internet of things // 2017 IEEE Trustcom/BigDataSE/ICESS. 2017. P. 185–192.
16. Jaquette G.A., Jesionowski L.G., Kulakowski J.E., McDowell J.A. Low cost tamper-resistant method for write-once read many (WORM) storage. US Patent. 2001. US6272086B1.
17. Sinha A., Jia L., England P., Lorch J.R. Continuous tamper-proof logging using TPM 2.0 // Trust and Trustworthy Computing. 2014. Lecture Notes in Computer Science. Vol. 8564.
18. Shepherd C., Akram R.N., Markantonakis K. EmLog: tamper-resistant system logging for constrained devices with TEEs // Information Security Theory and Practice. 2017. Vol. 10741. P. 75–92.
19. Ko R.K., Jagadpramana P., Lee B.S. Flogger: a file-centric logger for monitoring file access and transfers within cloud computing environments // 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. 2011. P. 765–771.
20. Yavuz A.A., Ning P., Reiter M.K. Efficient, compromise resilient and append-only cryptographic schemes for secure audit logging // Financial Cryptography and Data Security. 2012. Vol. 7397. P. 148–163.
21. Pulls T., Peeters R. Balloon: a forward-secure append-only persistent authenticated data structure // Computer Security ESORICS. 2015. Vol. 9327. P. 622–641.
22. Forcher B., Agne S., Dengel A., Gillmann M., Roth-Berghofer T. Semantic logging: towards explanation-aware das // International Conference on Document Analysis and Recognition. 2011. P. 1140–1144.
23. Shafiq M.O. Semantically Formalized Logging and Advanced Analytics for Enhanced Monitoring and Management of Large-scale Applications: Doctoral thesis. Calgary, Canada: University of Calgary, 2015.
24. Cucurull J., Puiggali J. Distributed immutabilization of secure logs // Security and Trust Management. 2016. Vol. 9871. P. 122–137.

VARIOUS SCHEMES AND APPROACHES TO LOGGING PROCESSES

V.N. Semenikhin
Ph.D. Student, e-mail: svladimir-99@mail.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The computing environment requires a reliable and comprehensive process for tracking and documenting user activity to maintain trust in the system. Logging is used for this purpose. However, logs that are created during the life cycle of an information system are vulnerable to a variety of attacks, including modification of logs, the possibility of erasing logs, and exposing user privacy. Many schemes have been created to solve these problems. Each of them has its own characteristics and its own views on logging processes. An overview of various schemes for protecting logs and approaches to the logging process is given.

Keywords: auditing, logging schemes, logging.

Дата поступления в редакцию: 14.05.2023