УДК 004.75

Юрченков Владислав Олегович, магистрант, Московский институт электронной техники, г. Москва

ПРИМЕНЕНИЕ СХЕМ РАЗДЕЛЕНИЯ СЕКРЕТА ДЛЯ ЗАЩИТЫ РАСПРЕДЕЛЁННЫХ СИСТЕМ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Аннотация

В статье рассматриваются вопросы обеспечения информационной безопасности распределённых систем управления базами данных (РаСУБД). Особое внимание уделяется уязвимостям, возникающим вследствие распределённой архитектуры таких систем, а также методам их устранения с использованием криптографических схем разделения секрета. Проведён анализ принципов работы пороговых схем разделения секрета и обоснована целесообразность их применения для повышения уровня защиты данных от несанкционированного доступа. Показано, что интеграция схем разделения секрета в механизмы управления доступом и защиты криптографических ключей позволяет повысить устойчивость РаСУБД к компрометации отдельных узлов и снизить риски утечки конфиденциальной информации.

Annotation

The article considers the issues of information security in distributed database management systems. Particular attention is paid to vulnerabilities caused by the distributed architecture of such systems, as well as to methods for their mitigation using cryptographic secret sharing schemes. The basic principles of threshold secret sharing schemes are analyzed, and the feasibility of their application for protecting cryptographic keys and implementing multi-level access control is substantiated. It is shown that the use of secret sharing schemes increases the resistance of distributed database management systems to unauthorized access and compromise of individual nodes.

Ключевые слова: распределённые базы данных, информационная безопасность, несанкционированный доступ, схемы разделения секрета, криптография, контроль доступа.

Keywords: distributed databases, information security, unauthorized access, secret sharing schemes, cryptographic protection, access control.

Современные информационные системы характеризуются постоянным ростом объёмов обрабатываемых данных и усложнением архитектуры их хранения. В условиях цифровизации и развития распределённых вычислений всё более широкое распространение получают распределённые системы управления базами данных, обеспечивающие высокую доступность, масштабируемость и производительность. Вместе с тем распределённый характер таких систем приводит к возникновению дополнительных угроз информационной безопасности, связанных с увеличением числа узлов, каналов передачи данных и точек возможной компрометации.

В отличие от централизованных систем управления базами данных, распределённые решения предполагают размещение данных и управляющих компонентов на нескольких территориально разнесённых узлах, взаимодействующих между собой посредством сетевых соединений. Это существенно усложняет реализацию механизмов аутентификации,

авторизации и контроля доступа, а также повышает требования к защите информации при передаче по сети. Компрометация одного или нескольких узлов может привести к несанкционированному доступу к данным, их утечке либо нарушению целостности всей системы.

Одной из наиболее значимых проблем безопасности распределённых СУБД является защита криптографических ключей, используемых для шифрования данных. Традиционные подходы, основанные на хранении ключевой информации на одном сервере или в централизованном хранилище, не в полной мере соответствуют требованиям распределённой архитектуры. В случае успешной атаки на такой узел злоумышленник получает возможность расшифровки всего массива защищённых данных, что сводит эффективность криптографической защиты к минимуму.

Дополнительную сложность представляет обеспечение отказоустойчивости механизмов защиты. В распределённых системах отказ или компрометация отдельного компонента не должны приводить к полной потере доступа к данным или снижению уровня безопасности. Это обуславливает необходимость применения методов защиты, которые изначально ориентированы на распределённую среду и учитывают возможность частичного выхода узлов из строя.

Перспективным подходом к решению указанных проблем является применение криптографических схем разделения секрета. Данные схемы предназначены для распределения секретной информации между несколькими участниками таким образом, что ни одна отдельная часть не раскрывает сам секрет. Восстановление исходной информации становится возможным только при объединении заранее определённого числа долей, что позволяет реализовать пороговый механизм доступа.

Наиболее известной и широко применяемой является пороговая схема разделения секрета Шамира, основанная на использовании полиномиальной интерполяции в конечных полях. Данная схема обладает свойством совершенности, при котором получение количества долей, меньшего

порогового значения, не позволяет извлечь какую-либо информацию о секрете. Кроме того, размеры долей соизмеримы с размером самого секрета, что упрощает практическую реализацию схемы. Наряду с этим существуют и другие схемы разделения секрета, отличающиеся используемыми математическими аппаратами и вычислительной сложностью, однако все они направлены на решение задачи надёжного распределённого хранения конфиденциальной информации.

Применение схем разделения секрета в распределённых системах управления базами данных позволяет существенно повысить уровень их защищённости. В первую очередь такие схемы могут использоваться для защиты криптографических ключей. Вместо хранения ключа в явном виде на одном узле он разделяется на несколько долей, которые распределяются между различными компонентами системы. Для восстановления ключа требуется совместное участие нескольких узлов, что значительно снижает вероятность его компрометации.

Даже в случае успешной атаки на отдельный узел злоумышленник не получает достаточной информации для восстановления ключа и расшифровки данных. Таким образом, повышается устойчивость системы к внутренним и внешним угрозам, а также снижаются риски утечки конфиденциальной информации. Кроме того, использование пороговых схем позволяет реализовать гибкие механизмы многоуровневого контроля доступа, при которых выполнение критически важных операций возможно только при соблюдении заданных условий доступа.

Применение схем разделения секрета также положительно сказывается на отказоустойчивости распределённых СУБД. Потеря или недоступность одной или нескольких долей секрета не приводит к утрате доступа к данным при условии, что пороговое значение остаётся достижимым. Это особенно важно для систем, функционирующих в условиях нестабильных сетевых соединений или повышенных требований к надёжности. Дополнительным преимуществом применения схем разделения секрета в

распределённых системах управления базами данных является возможность снижения доверия к отдельным узлам системы. В классических архитектурах часто предполагается, что серверы хранения или узлы управления являются доверенными, что не всегда соответствует реальным условиям эксплуатации. Использование пороговых криптографических схем позволяет перейти к модели частичного доверия, при которой безопасность системы не зависит от надёжности каждого отдельного компонента, а определяется выполнением заданных криптографических условий.

Таким образом, использование схем разделения секрета является эффективным инструментом повышения уровня информационной безопасности распределённых систем управления базами данных. Данный подход позволяет учитывать особенности распределённой архитектуры, обеспечивать защиту криптографических ключей, повышать устойчивость к компрометации отдельных узлов и реализовывать гибкие механизмы управления доступом. Интеграция схем разделения секрета в современные РаСУБД представляет собой перспективное направление развития средств защиты информации и может быть использована при проектировании систем, предъявляющих повышенные требования к безопасности и надёжности.

Литература

1. Аширова, М. Б. Понятие и архитектура распределенной БД / М. Б. Аширова // Внедрение результатов инновационных разработок: проблемы и перспективы : сборник статей международной научно-практической конференции, Екатеринбург, 18 ноября 2016 года. Часть 3. – Екатеринбург: ООО "ОМЕГА САЙНС", 2016. – С. 49-51.
2. Аждер, Т. Б. О распределенных системах баз данных / Т. Б. Аждер // Новая наука: Проблемы и перспективы. – 2016. – № 115-2. – С. 154-156.
3. Чипчагов М.С., Вербицкий А.С., Титов В.А. Защищенность информации в распределённых информационных системах // Вестник УМЦ. 2018. №2

4. Носиров З.А., Щербинина О.В. Анализ криптографических схем разделения секрета для резервного хранения ключевой информации // Прикаспийский журнал: управление и высокие технологии. 2019. №2.
5. Лавриненко А. Н., Червяков Н. И. Некоторые элементы концепции активной безопасности в современной криптографии // Экономика. Информатика. 2014.

Literature

1. Ashirova, M. B. Concept and architecture of distributed databases / M. B. Ashirova // Implementation of Innovative Development Results: Problems and Prospects: Proceedings of the International Scientific and Practical Conference, Yekaterinburg, November 18, 2016. Part 3. – Yekaterinburg: OMEGA SCIENCE LLC, 2016. – Pp. 49–51.
2. Azhder, T. B. On distributed database systems / T. B. Azhder // New Science: Problems and Prospects. – 2016. – No. 115-2. – Pp. 154–156.
3. Chipchagov, M. S., Verbitsky, A. S., Titov, V. A. Information security in distributed information systems // Bulletin of the Training and Methodological Center. – 2018. – No. 2.
4. Nosirov, Z. A., Shcherbinina, O. V. Analysis of cryptographic secret sharing schemes for backup storage of key information // Caspian Journal: Management and High Technologies. – 2019. – No. 2.
5. Lavrinenko, A. N., Chervyakov, N. I. Some elements of the active security concept in modern cryptography // Economics. Informatics. – 2014.