ЗАЩИТА ДАННЫХ В СИСТЕМАХ МОНИТОРИНГА БЕЗОПАСНОСТИ КРУПНОМАСШТАБНЫХ ОБЪЕКТОВ

Полтавцева М.А., Калинин М.О.

Санкт – Петербургский политехнический университет Петра Великого,
Россия, г. Санкт-Петербург ул. Политехническая д.29
poltavtseva@ibks.spbstu.ru

Аннотация: В работе рассматриваются особенности систем управления данными при мониторинге безопасности крупномасштабных объектов. Выделены особенности угроз и возможностей нарушителя. На основе принципов построения защищенных систем управления большими данными авторами предложены решения по концептуальному описанию данных и операций системы мониторинга, обеспечению технологической и архитектурной полноты защиты. Проведена классификация узлов – обработчиков в соответствии с принципом минимизации доверия. Предложена новая архитектура типового звена управления данными системы мониторинга безопасности в защищенном исполнении.

Ключевые слова: Большие данные, информационная безопасность, мониторинг безопасности крупномасштабных объектов.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-03102

Введение

Современные тенденции в области цифрового управления и производства приводят к широкому применению информационных систем для автоматизированного мониторинга, в том числе – мониторинга крупномасштабных объектов промышленного характера. Характерные черты таких систем: распределенность; взаимодействие через публичные сети; связь с реальными физическими объектами - делают их привлекательными для нарушителя. Это порождает необходимость не только мониторинга событий безопасности в крупномасштабных системах, но и защиты самой системы обеспечения устойчивого функционирования от злоумышленника.

Эффективность задач мониторинга безопасности сегодня зависит от обработки больших объемов данных, корректность и конфиденциальность которых достаточно важны. Однако, системы управления Большими данными на сегодняшний день имеют ряд проблем с защитой информации [1], связанных с технологическим развитием самих решений и изменением в модели угроз[2]. Таким образом, задача защиты информации в этом классе систем является сейчас высоко актуальной. Настоящая работа описывает новый подход и соответствующие практические решения для построения защищенных систем управления Большими данными в информационных системах мониторинга безопасности крупномасштабных объектов.

1 Подход к обеспечению безопасности систем управления данными мониторинга

Новые угрозы в системах управления большими данными связаны со сложным жизненным циклом фрагментов обрабатываемой информации и снижением степени доверия к узлам - обработчикам. Основными целями нарушителя могут быть дискредитация и нарушения в системе работы мониторинга безопасности (что открывает возможности для прочих нарушений); получение злоумышленником данных об объекте, его организации (географической и структурной), системе защиты; возможность получения доступа к данным о функционировании физического объекта. Если система мониторинга безопасности совмещена с системой общего мониторинга (как правило, используется общая архитектура данных), это возможность, в конечном итоге, влиять на функционирование объекта в обход систем защиты.

Основными задачами безопасности при построении системы управления данными становятся: отслеживание взаимосвязей и соблюдение политики доступа к данным на протяжении всего жизненного цикла обработки; защита данных на протяжении всего жизненного цикла при передаче, хранении и обработке с учетом низкой степени доверия к узлам – обработчикам. Большинство современных решений по защите Больших данных [1,2] не предлагает комплексного решения проблемы, за исключением согласованных подходов на основе одного программного стека и частных облаков. Для систем этого класса в работе [3] предложен консистентный подход к обеспечению защищенности, основанный на принципах консистентности описания данных и процессов, полноты и минимизации доверия.

2 Консистентное представление данных и процессов мониторинга безопасности

Согласно работам [4-6], данные мониторинга в различных областях представляют собой наборы временных рядов параметров. Важными являются, во-первых, набор фактических данных вида <Paremeter, {Timestamp, Value}>, где Parameter – фиксируемое значение, {Timestamp, Value} – набор

значений, где каждому значению сопоставлено время его формирования. Во вторых, это справочники метаданных. Для унификации представления данных и операций по их обработке в системе безопасности, сформируем схему данных в концептуальной агрегатной модели [3]. В качестве базового агрегата предлагается использовать пару <Key, Value> где в качестве ключа выступает кортеж <P_Class, P_Time,Timestamp>, где P_Class - параметр, P_Time – идентификатор временного ряда, Timestamp – временная метка значения, а значение агрегата представляет собой <Value> временного ряда. При необходимости могут быть добавлены уровни вложенности, связанные с иерархической агрегацией географически распределенной системы: идентификатор источника данных или другие мета - параметры.

Операции над данными в системе мониторинга можно разделить на две группы. Первая группа – это операции оперативного управления информацией, включая ее запись, выборку и пересылку. Основными ключами выборки данных являются: параметры и идентификаторы временных рядов. Вторая группа – операции аналитической обработки, которые можно разделить на операции формирования временного ряда большей размерности и сложные вычислительные операции над компонентами ряда. Так как доступ различных участников (поставщиков данных, аналитиков) к системе мониторинга регламентируется характером требуемых (поставляемых) им данных или подключения, разграничение доступа предлагается регламентировать на основе ABAC [7]. В этом случае основными атрибутами, определяющими права доступа, будут: параметр; время поступления данных; точка (географическое положение или узел) поступления данных; источник данных. При необходимости могут использоваться дополнительные атрибуты.

Все эти характеристики получаются в момент поступления кортежа автоматически. Использование идентификатора источника позволяет дополнительно проводить его верификацию. Права доступа пользователя и, следовательно, для конечного пользователя также определяются в терминах кортежа <Parameter, Time_in, Incoming_node/Source> При этом временная характеристика Time_in задается диапазоном, внося в ABAC элементы интеллектуализации [7]. Источник данных обладает единственным правом на запись информации в систему, то есть вызов функций: $Include(< P\_Class \cdot P\_Time, \{\} >, Create(< Timestamp, Value >))$ строго в указанном формате с учетом атрибутов соединения. В свою очередь, потребитель данных, не смотря на то, что получает на выходе итоговый кортеж, имеет потенциальный доступ ко всей информации, которая использовалась при его порождении. Политика безопасности должна распространяются на все агрегаты, участвовавшие в порождении доступных для пользователя (человека или программного компонента) данных. Для достижения этого свойства права доступа конечного потребителя определяются кортежем <*Parameter, Time_in, Incoming_node/Source*> над входными агрегатами. Пава доступа к производным агрегатам определяются на основании входящих в них исходных. Указанные решения позволяют обеспечить выполнение политики безопасности на всем протяжении обработки данных и снизить вероятность эксплуатации уязвимости логического вывода.

3 Полнота защиты и минимизация доверия

Обеспечение полноты защиты связано с последовательным построением системы защиты «снизу вверх» и полнотой отображения структур логического уровня обработки данных на концептуальный уровень проверки безопасности [3]. При обработке данных мониторинга безопасности используются хранилища данных в памяти для оперативного хранения, долговременные хранилища на диске сырых и исторических данных [4-6]. Основные типы используемых СУБД относятся к системам с низкой структуризацией данных, ориентированным на быструю выборку и запись информации.

Безопасность данных на нижнем технологическом уровне (сети передачи данных, физическое хранение) обеспечивается шифрованием. Требованиями к системе шифрования являются: безопасность, высокая скорость операций с данными (что означает выполнение операций над данными без расшифрования), небольшое увеличение объема данных. Современными подходами к шифрованию в этой области являются: полностью гомоморфное шифрование (FHE - Fully Homomorphic Encryption); линейное разделение секрета (LSS - Linear Secret Sharing); Garbled Circuits (GB). Сегодня характеристиками, пригодными для промышленного применения обладают алгоритмы гомоморфного шифрования, относящиеся к категории OPE (Order – Preserving Encryption). Они обеспечивают шифрование с сохранением порядка и позволяют выполнять над зашифрованными данными операции сравнения. Анализ OPE – схем показывает наибольшую потенциальную эффективность R-OPE [8] шифрования, предложенного Шатиловым. Использование этой схемы позволяет выполнять над зашифрованными данными операции сравнения на равенство и сравнения порядка, достаточные для простых NoSQL СУБД в системе управления Большими данными.

Принцип минимизации доверия в системе управления большими данными [3] определяет классификацию узлов системы на доверенные и не доверенные для распределения между ними операций. Иерархическая система мониторинга состоит из географически распределенных «типовых» подсистем (звеньев), объединенных в общую структуру. Для классификации узлов типового звена по принципу секретности используется классификация операций над данными и отображение их на узлы - исполнители. Предложенная Шатиловым К.А. схема шифрования OPE позволяет выполнять операции сравнения на равенство и на порядок. Для выполнения операций NoSQL СУБД типа ключ – значение и семейство столбцов, как и базовых операций Map_reduce, достаточно иметь возможность сравнения данных на точное совпадение и на равенство.

Узлы, связанные с доверенной обработкой данных, должны быть снабжены фреймворками шифрования, осуществляющими дешифровка и шифрование данных. Они должны быть доверенными. Узлы, выполняющие хранение, выборку и фильтрацию данных (обработку данных без учета семантики) могут выполнять свои функции над зашифрованными данными в не доверенном режиме.

Заключение

Системы мониторинга крупномасштабных объектов имеют иерархическую, географически распределенную организацию и сложный жизненный цикл данных. Это приводит к повышению вероятности реализации различных угроз, результатом реализации которых может стать возможность для злоумышленника получить данные о физическом процессе и режиме функционирования объектов, дискредитировать системы защиты, влиять на целевую систему.

Использование единого представления данных и процессов в концептуальной агрегатной модели позволяет задавать согласованную политику безопасности и контролировать ее выполнение на протяжении всего жизненного цикла данных. Предложенная авторами схема разделения узлов ориентирована на современную систему шифрования OPE. Предложенные решения для обеспечения технологической полноты и минимизации доверия разработаны с учетом современных методов защиты информации, управления данными и специфики систем мониторинга безопасности.

Литература

1. Akeel F. Y. Secure data integration systems // Thesis for the degree of Doctor of Philosophy, 2017. https://eprints.soton.ac.uk/415716/1/Final_thesis.pdf

2. Alshboul Y., Wang Y., Nepali R. K. Big Data LifeCycle:Threats and Security Model. // Proceedings of the 21st Americas Conference on Information Systems (AMCIS 2015). 2015, - P. 1 – 7

3. Полтавцева М.А. Консистентный подход к построению защищенных систем обработки и хранения больших данных // Проблемы информационной безопасности. Компьютерные системы. № 2. 2019, - С. 29-44

4. Pavlenko E., Zegzhda D. Sustainability of cyber-physical systems in the context of targeted destructive influences // Proceedings - 2018 IEEE Industrial Cyber-Physical Systems, ICPS. 2018, - P. 830-834 DOI: 10.1109/ICPHYS.2018.8390814

5. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access, 2018, Vol.6. 10 p. DOI: 10.1109/ACCESS.2018.2881998

6. Adiba N., Li Y., Gupta A. US20110153603A1 Time series storage for large-scale monitoring system // https://patents.google.com/patent/US20110153603A1/en

7. Haourani L.E., Elkalam A.A., Ouahman A.A. Knowledge Based Access Control a model for security and privacy in the Big Data // Proceedings of the 3rd International Conference on Smart City Applications (SCA '18). - ACM, New York, USA. 2018, - P. 1-8 DOI: 10.1145/3286606.3286793

8. Shatilov, K., Boiko, V., Krendelev, S., Anisutina, D., Sumaneev, A. Solution for secure private data storage in a cloud // Proceedings of the 2014 Federated Conference on Computer Science and Information Systems. 2014. – P. 885- 889