МОНИТОРИНГ БЕЗОПАСНОСТИ В IOT-СЕТЯХ

SECURITY MONITORING IN IOT-NETWORKS

УДК 004.056.53

Баев Дмитрий Александрович, Студент кафедры Кибербезопасность информационных систем, Донской государственный технический университет, г. Ростов-на-Дону

Волков Роман Олегович, Студент кафедры Кибербезопасность информационных систем, Донской государственный технический университет, г. Ростов-на-Дону

Зонов Александр Дмитриевич, Студент кафедры Кибербезопасность информационных систем, Донской государственный технический университет, г. Ростов-на-Дону

Baev D.A. fantom-sj@yandex.ru

Volkov R.O. volf.rain@yandex.ru

Zonov A.D. zaffar.edu@gmail.com

Аннотация

В данной статье рассматривается вопросы мониторинга в сетях интернета вещей, а именно вопросы применения мониторинга для контроля процессов, происходящих внутри IoT-сетей. Были рассмотрены преимущества мониторинга сетей IoT по сравнению с традиционными методами контроля. В частности, были рассмотрены возможности применения систем мониторинга IoT для обеспечения безопасности данных сетей.

Annotation

This article discusses the issues of monitoring in the Internet of Things networks, namely, the issues of using monitoring to control the processes occurring within IoT

networks. The benefits of monitoring IoT networks over traditional monitoring methods were discussed. In particular, the possibilities of using IoT monitoring systems to ensure the security of these networks were considered.

Ключевые слова: Интернет вещей, IoT-сети, мониторинг, системы мониторинга, безопасность.

Keywords: Internet of Things, IoT-networks, monitoring, monitoring systems, security.

«Интернет вещей» или «Internet of Things» (далее сокращённо IoT) – это концепция сети передачи данных между физическими объектами, оснащёнными различными модулями для взаимодействия друг с другом посредством использования сетей передачи данных [1].

Среди большого количества устройств умного дома (в том числе охранных систем) наблюдается ряд серьезных проблем с безопасностью. Статистика показывает, что 65% девайсов Интернета Вещей имеют легко реализовываемые уязвимости [2]. Для предотвращения реализации данных уязвимостей предлагается использовать концепцию мониторинга сетей интернета вещей.

Мониторинг сети начинается со сбора данных из соответствующей сети, что в последствии позволит контролировать удаленные устройства и оборудование [3]. Все представленные «умные» подключенные устройства объединяются и работают вместе для автоматизации и управления другим оборудованием из центра обработки данных.

Чтобы быть действительно эффективной, система мониторинга интернета вещей должна обладать определенной функциональностью. Эти функции должны быть в состоянии обеспечить сбор и обработку значительной информации о сети. К подобной функциональности можно отнести мгновенное оповещение и фильтрация сигналов тревоги [4].

Мгновенное оповещение означает своевременное получение уведомлений о важном изменении статуса или условий. Они должны быть

достаточно информативными, для верной и быстрой реакции, чтобы угрозу нарушения безопасности [4].

Существует два основных способа сбора данных: метода push-based («на основе толчка») или опрос [4]. Для систем мониторинга интернета вещей метод push-based может быть более удобным, однако стоит учитывать некоторые компромиссы. Эти компромиссы обычно связаны с существующим протоколом связи.

Важно убедиться, что протокол, поддерживаемый устройствами сети, имеет эффективные способы сбора данных. Но также важно использовать открытые протоколы для обеспечения совместимости между многими устройствами. Современный протокол обеспечит эффективный сбор данных и полную видимость сети [4].

Мониторинг безопасности Интернета вещей отличается от мониторинга общей ИТ-безопасности. Фактически, он полагается на другое программное и аппаратное обеспечение, а также на другие компоненты и протоколы связи, таким образом делаю подход к безопасности на устройствах IoT кардинально отличающимся от обычных устройств [5].

Системы обнаружения вторжений (IDS) - одно из самых распространенных решений для поддержки мониторинга безопасности [6].

В работе [7] предлагается концепция устройства, представляющего из себя небольшой модуль, встраиваемы как в обширную сеть IoT, так и в сеть с ограниченными ресурсами, становясь тем самым системой мониторинга и позволяющий организовать бесперебойную проверку сети интернета вещей на наличие попыток реализации атаки на данную сеть.

Данный модуль состоит из четырёх элементов, которые позволяют ему, захватывая трафик внутри сети IoT, фильтровать и выдавать вердикт о попытке реализации той или иной атаки на устройства данной сети. К основным его компонентам относятся следующие элементы:

– устройство хранения данных – хранит на постоянной основе шаблоны сигнатур атак, использующиеся при анализе данных.

– устройство анализа данных – позволяет обнаружить подозрительный, аномальный трафик внутри сети.

– устройство предварительной обработки и фильтрации данных – получает данные из разных доступных агентов мониторинга и обеспечивает начальную предварительную обработку и агрегирование данных.

– детектор инцидентов – собирает и анализирует обработанные данные, вызывая оповещения при обнаружении инцидента нарушения безопасности.

Схематичное устройство данного модуля изображено на рисунке 1.



Рисунок 3. Модуль мониторинга сети IoT

При этом компонент анализа данных может быть представлен как система обнаружения вторжений на основе аномалий. Данный инструмент создает профиль или модель, которая считается как модель «нормального» поведения, используя статистические или неконтролируемые методы машинного обучения [7]. Любые отклонения от этой модели могут быть расценены как потенциальные угрозы и помечены соответствующем образом.

Обеспечение безопасности в IoT очень сложно, так как во многом ограничение вычислительных ресурсов и мощности препятствует принятию надлежащих контрмер. Подобные ограничения делают традиционные IDS не подходящими для полного мониторинга инфраструктуры интернета вещей.

Тем не менее в результате проведённого исследования были выявлены способы предотвращения атак на подобные системы, посредством использования системы мониторинга интернета вещей. При этом в работе был рассмотрен модуль мониторинга трафика внутри сети интернета вещей, позволяющий выявлять попытке осуществления атак на устройства данной сети в том числе с применением машинного обучения.

Литература:

1. Росляков А.В. Интернет вещей / А.В. Росляков, С. В. Ваняшин, А. Ю. Гребешков, М. Ю. Самсонов; // Самара: ПГУТИ, ООО «Издательство Ас Гард», – 2014. – 340 с.;
2. Соколов М.Н. Проблемы безопасности Интернет вещей: обзор / М.Н. Соколов К.А. Смолянинова, Н.А. Якушева // Вопросы кибербезопасности, – 2015, – №5, – 13 с.;
3. Siggins M. How IoT Makes Your Remote Monitoring System More Efficient/ / M. Siggins – Текст: электронный // DPS Telecom: Network Monitoring Solutions Company: [сайт]. – URL: https://www.dpstele.com/ blog/how-iot-makes-remote-monitoring-more-efficient.php (дата обращения: 03.05.2021);
4. Moulat M.E. Monitoring System Using Internet of Things For Potential Landslides / M.E. Moulat O. Debauche, S. Mahmoudi, L.A. Brahim, P. Manneback, F. Lebeau, // Procedia Computer Science, – vol. 134, – 2018, – P. 26-34, DOI: 10.1016/j.procs.2018.07.140;
5. Котенко И.В. Архитектура системы параллельной обработки больших данных для мониторинга безопасности сетей Интернета вещей / И.В. Котенко, И.Б. Саенко, А.Г. Кушнеревич, // Труды СПИИРАН, – 2018, – №4, – вып. 59, С. 5-30, DOI: 10.15622/sp.59.1;
6. Валиев, А. А. Обработка и сбор данных в сети "Интернет вещей" Система обнаружения вторжений в сети IoT устройств / А.А. Валиев // Научно-практические исследования. – 2017. – №3, – вып. 3, – С. 44-52;

7. Casola V. A security monitoring system for internet of things / V. Casola, A.D. Benedictis, A. Riccio, D. Rivera, W. Mallouli, E.M. Oca // Internet of Things, – 2019, – vol. 7, – 20 p., DOI: 10.1016/j.iot.2019.100080

Literature

1. Roslyakov A.V. Internet of Things / A.V. Roslyakov, S.V. Vanyashin, A. Yu. Grebeshkov, M. Yu. Samsonov; // Samara: PSUTI, As Guard Publishing House, - 2014. - 340 p.;
2. Sokolov M.N. Security problems of the Internet of Things: an overview / M.N. Sokolov K.A. Smolyaninova, N.A. Yakusheva // Issues of cybersecurity, - 2015, - №5, - 13 p.;
3. Siggins M. How IoT Makes Your Remote Monitoring System More Efficient // M. Siggins - Text: electronic // DPS Telecom: Network Monitoring Solutions Company: [site]. - URL: https://www.dpstele.com/blog/how-iot-makes-remote-monitoring-more-efficient.php (date accessed: 05/03/2021);
4. Moulat M.E. Monitoring System Using Internet of Things For Potential Landslides / M.E. Moulat O. Debauche, S. Mahmoudi, L.A. Brahim, P. Manneback, F. Lebeau, // Procedia Computer Science, - vol. 134, - 2018, - P. 26-34, DOI: 10.1016 / j.procs.2018.07.140;
5. Igor Kotenko The architecture of a system for parallel processing of big data for monitoring the security of IoT networks. Kotenko, I.B. Saenko, A.G. Kushnerevich, // Proceedings of SPIIRAS, - 2018, - №4, - issue. 59, S. 5-30, DOI: 10.15622 / sp. 59.1;
6. Valiev, A. A. Processing and collection of data in the Internet of Things. Intrusion detection system in the IoT device network. Valiev // Scientific and practical research. - 2017. - No. 3, - issue. 3, - S. 44-52;
7. Casola V. A security monitoring system for internet of things / V. Casola, A.D. Benedictis, A. Riccio, D. Rivera, W. Mallouli, E.M. Oca // Internet of Things, - 2019, - vol. 7, - 20 p., DOI: 10.1016 / j.iot.2019.100080