Международный журнал прикладных наук и технологий "Integral"

Научная статья
Original article
УДК 004.4

УЯЗВИМОСТИ ИНТЕРНЕТА ВЕЩЕЙ (IOT)

VULNERABILITIES IN THE INTERNET OF THINGS (IOT)

Убеев Валерий Геннадьевич, Студент, 5 курс, факультет «Инфокоммуникационных сетей и систем», СПБГУТ им. проф. М.А. Бонч-Бруевича, Россия, г. Санкт-Петербург

Гельфанд Артем Максимович, старший преподаватель кафедры ЗСС, заместитель декана факультета ИКСС, СПБГУТ им. проф. М.А. Бонч-Бруевича, Россия, г. Санкт-Петербург

Ubeev Valery Gennad'evich, Student, 5th year student, Faculty of Infocommunication Networks and Systems, SPBSUT named after. prof. M.A. Bonch-Bruevich, Russia, St. Petersburg

Gelfand Artem Maksimovich, senior lecturer of the ZSS department, deputy dean of the ICSS faculty, SPBSUT named after. prof. M.A. Bonch-Bruevich, Russia, St. Petersburg

Аннотации

В данной статье описано влияние Интернета вещей (IoT) на повседневную жизнь, рассматриваются наиболее распространенные уязвимости IOT, то к чему эти уязвимости могут привести, способы борьбы с ними и способы обеспечения безопасности данных. Названы виды атак представляющих

угрозу для IoT. Приведены примеры способов защиты данных от злоумышленников.

Summary

This article describes the impact of the Internet of Things (IoT) on everyday life, examines the most common IoT vulnerabilities, what these vulnerabilities can lead to, how to combat them, and how to ensure data security. The types of attacks that pose a threat to IoT are named. Examples of ways to protect data from intruders are given.

Ключевые слова: Защита, данные, IOT, сеть, злоумышленники, уязвимости
Keywords: Protection, data, IOT, network, attackers, vulnerabilities

В современном мире технологий, Интернет вещей (IoT) продолжает расширять свое влияние на нашу повседневную жизнь. Умные устройства переполняют рынок, улучшая нашу жизнь, делая ее более комфортной и эффективной. Однако, за этой эффективностью и удобством скрываются уязвимости, которые могут быть использованы злоумышленниками для атак и нарушения нашей приватности. В этой статье мы рассмотрим суть уязвимостей IoT, их разнообразие и меры по защите от них. IoT охватывает широкий спектр устройств: от умных термостатов и роботов-пылесосов до медицинских устройств и автомобилей. Эти устройства подключены к Интернету и сбору данных, обеспечивая беспрецедентный уровень автоматизации и мониторинга. Однако, когда устройства подключаются к сети, они становятся подверженными угрозам. Одной из наиболее распространенных уязвимостей IoT является недостаточная безопасность устройств. Многие из них поставляются с дефолтными паролями, которые редко меняют пользователи. Это оставляет дверь открытой для злоумышленников, которые могут использовать известные пароли для получения доступа к устройствам. Важно осознавать, что часто такие устройства установлены в домах и офисах, где хранятся чувствительные

данные. Недостаточная безопасность устройств является ключевой уязвимостью IoT, которую необходимо преодолеть. Другой аспект безопасности IoT связан с сетевыми протоколами. Многие устройства используют устаревшие или небезопасные сетевые протоколы, что делает их подверженными атакам. Например, если протоколы не предусматривают шифрование данных или аутентификацию, информация может быть легко скомпрометирована. Это ставит под угрозу как конфиденциальность данных, так и работоспособность устройств. Отсутствие обновлений программного обеспечения также оставляет устройства IoT уязвимыми. Производители устройств должны регулярно выпускать обновления для устранения обнаруженных уязвимостей и улучшения безопасности. Однако многие производители не следят за обновлениями, оставляя свои продукты подверженными новым угрозам. Сетевые атаки представляют собой еще одну угрозу для IoT. Злоумышленники могут использовать различные методы, включая атаки на сетевой уровень, такие как переполнение буфера и атаки на отказ в обслуживании (DDoS), чтобы нарушить работу устройств IoT. Это может привести к потере доступа к устройству или даже его полной компрометации. Сбор и передача чувствительных данных устройствами IoT также представляет угрозу. Медицинские устройства собирают данные о здоровье пациентов, а умные дома - о расписаниях и привычках жителей. Если эти данные не защищены должным образом, они могут быть украдены или изменены злоумышленниками. Это может привести к серьезным последствиям, включая нарушение конфиденциальности и безопасности.

Чтобы бороться с уязвимостями IoT, необходимы комплексные меры. Производители должны обеспечивать лучшую безопасность устройств и регулярно выпускать обновления. Пользователи, в свою очередь, должны быть более активными в отношении обеспечения безопасности своих устройств, изменения паролей по умолчанию и установки обновлений. Индустрия IoT также должна продолжать работать над разработкой более безопасных

сетевых протоколов и стандартов безопасности. Образование и обучение пользователей, а также специалистов в области безопасности, является ключевым аспектом обеспечения безопасности IoT. IoT - это неотъемлемая часть нашей современной жизни, и она будет продолжать расширяться. Это означает, что угрозы и уязвимости IoT также будут развиваться. Поэтому критически важно, чтобы как индустрия, так и пользователи принимали эффективные меры по обеспечению безопасности IoT. Кроме того, индустрия должна стремиться к стандартизации безопасности IoT, чтобы создать единые нормы и практики, которые будут соблюдаться всеми производителями. Пользователи также играют ключевую роль в обеспечении безопасности своих устройств IoT. Важно, чтобы они выполняли установку обновлений, мониторинг сетевой активности и использовали сильные пароли. Образование и информирование пользователей является первым шагом к увеличению безопасности IoT. Борьба с уязвимостями IoT - это долгосрочная задача, и она потребует усилий как со стороны индустрии, так и со стороны потребителей. Однако важно помнить, что безопасность IoT - это не просто вопрос личной безопасности, но и вопрос сохранения конфиденциальности и защиты чувствительных данных. С ростом числа подключенных устройств, обеспечение безопасности IoT становится ключевой задачей, которой мы не можем игнорировать. Помимо обеспечения безопасности, индустрия IoT также должна разрабатывать механизмы обнаружения и реагирования на инциденты. Эффективные системы мониторинга и обнаружения аномальной активности могут помочь выявлять потенциальные угрозы и предпринимать меры в реальном времени. Другой важной частью обеспечения безопасности IoT является сотрудничество между производителями, исследователями и органами власти. Обмен информацией о новых уязвимостях и атаках позволяет реагировать быстрее и эффективнее. Прозрачность и сотрудничество могут значительно улучшить безопасность всей экосистемы IoT. Развитие технологий в сфере Интернета вещей (IoT) не только приводит

к расширению возможностей и увеличению угроз, но также открывает новые горизонты для безопасности и приватности. Недавние тенденции в области безопасности IoT включают в себя следующие важные аспекты:

Многозоновые сети и микросегментация: Для укрепления безопасности IoT-систем, многие компании переходят к использованию многозоновых сетей и микросегментации. Это позволяет разделять устройства IoT на отдельные сегменты сети, обеспечивая изоляцию и ограничение доступа к устройствам, что снижает риск распространения атак.

Блокчейн и распределенные реестры: Технологии блокчейн и распределенных реестров активно исследуются в качестве способов укрепления безопасности IoT. Они могут использоваться для обеспечения целостности данных, аутентификации устройств и обеспечения надежных транзакций в сети IoT.

Биометрическая аутентификация: Внедрение биометрической аутентификации в устройства IoT помогает устранить проблему слабых паролей или их дефолтных значений. Отпечатки пальцев, распознавание лица и другие биометрические методы могут повысить уровень безопасности и удобства для пользователей.

Искусственный интеллект и машинное обучение: ИИ и машинное обучение могут использоваться для анализа больших объемов данных, чтобы выявлять аномалии и предсказывать потенциальные атаки. Это помогает улучшить реакцию на угрозы и обеспечить превентивные меры безопасности.

Квантовая криптография: С развитием квантовых вычислений появляются новые вызовы для криптографии. Квантовая криптография может обеспечить более надежную защиту данных IoT в будущем, предотвращая дешифрование информации злоумышленниками с помощью квантовых компьютеров.

Эти последние разработки в области безопасности IoT демонстрируют, что индустрия и общество активно реагируют на растущие угрозы и уязвимости. Со временем совместные усилия производителей, пользователей и

регулирующих органов могут сделать IoT более безопасным и надежным аспектом нашей цифровой жизни.

IoT приносит массу преимуществ и новых возможностей, но оно также несет угрозы. Уязвимости IoT - это вызов, который мы должны воспринимать серьезно. Только совместные усилия индустрии, пользователей и общества в целом могут гарантировать безопасное и продуктивное развитие Интернета вещей.

Список литературы

1. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 590-595.
2. Гельфанд А. М. и др. ОБЛАСТИ ПРИМЕНЕНИЯ АНАЛИТИКИ БОЛЬШИХ ДАННЫХ В КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУРАХ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 438-440.
3. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 266-270.
4. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018. – С. 149-149.
5. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах

//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 570-573.,

6. Кирилова К. С. и др. Проблема обезвреживания руткитов уровня ядрав системах специального назначения //I-methods. – 2020. – Т. 12. – №. 3. – С. 2.
7. Пестов И. Е., Кошелева С. А. Атаки на облачную инфраструктуру //Инновационные решения социальных, экономических и технологических проблем современного общества. – 2021. – С. 113-115.

Bibliography

1. Kazantsev A. A. et al. Creation and management of Security Operations Center for effective use in real conditions // Current problems of information telecommunications in science and education (APINO 2019). – 2019. – pp. 590-595.
2. Gelfand A. M. et al. AREAS OF APPLICATION OF BIG DATA ANALYTICS IN CRITICAL INFORMATION INFRASTRUCTURES // Current problems of information telecommunications in science and education (APINO 2022). – 2022. – P. 438-440.
3. Volkogonov V. N., Gelfand A. M., Karamova M. R. Ensuring the security of personal data during their processing in personal data information systems // Current problems of information telecommunications in science and education (APINO 2019). – 2019. – pp. 266-270.
4. Kotenko I. V. et al. Model of human-machine interaction based on touch screens for monitoring the security of computer networks // Regional informatics "RI-2018". – 2018. – pp. 149-149.
5. Suvorov A. M., Tsvetkov A. Yu. Study of buffer overflow attacks in 64-bit unix-like operating systems // Current problems of information telecommunications in science and education (APINO 2018). – 2018. – P. 570-573.,

6. Kirilova K. S. et al. The problem of neutralizing kernel-level rootkits in special-purpose systems //I-methods. – 2020. – T. 12. – No. 3. – P. 2.
7. Pestov I. E., Kosheleva S. A. Attacks on cloud infrastructure // Innovative solutions to social, economic and technological problems of modern society. – 2021. – pp. 113-115.

Для цитирования: Убеев В.Г., Гельфанд А.М. ИЗГОТОВЛЕНИЕ МАСКИ ИЗ НИТРИДА КРЕМНИЯ ДЛЯ ИСПОЛЬЗОВАНИЯ В ТЕХНОЛОГИИ ВЗРЫВНОЙ ЛИТОГРАФИИ// Международный журнал прикладных наук и технологий "Integral" №6/2023.