Матеріали VIII Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології» 23 - 25 вересня 2019, Одеса

УДК 004.05 **Information Control Systems and Technologies, pp. 73-75**

Фаткулин А.Р., д.т.н. Ныркov А.П., Тяпкин Д.А.

ОСНОВНЫЕ ПРОБЛЕМЫ В ОБЛАСТИ ЗАЩИТЫ ИНТЕРНЕТА ВЕЩЕЙ

Fatkulin A.R., Dr. Sci. Nyrkov A.P., Tyapkin D.A.

THE MAIN PROBLEMS IN THE FIELD OF PROTECTION OF THE INTERNET OF THINGS

В результате быстрых социальных и технологических изменений, вызванных ростом Интернета, физический опыт человека в большей степени связан с цифровым миром, чем когда-либо прежде, и именно поэтому он должен быть защищен.

Чтобы Интернет вещей развивался эффективно, должны быть решены проблемы безопасности, связанные с его ростом:

• Доступность: обеспечение постоянной связи между конечными точками и их соответствующими службами.

• Идентификация: аутентификация конечных точек, сервисов и работы клиента или конечного пользователя, использующего конечную точку.

• Конфиденциальность: снижение вероятности причинения вреда отдельным конечным пользователям.

• Безопасность: обеспечение возможности проверки, отслеживания и мониторинга целостности системы.

Чтобы Интернет вещей развивался в ожидаемом темпе, конечные устройства должны иметь возможность постоянно общаться друг с другом, конечными пользователями и внутренними службами.

Для этого внедряются новые технологии, такие как NB-IoT и LTE-M, которые обеспечивают постоянное подключение для устройств с низким энергопотреблением.

Это хорошо согласуется с проблемой повсеместного доступа в Интернет для современного мира. Чтобы конечная точка функционировала в экосистеме продуктов или услуг IoT, она должна быть способна безопасно идентифицировать себя для своих партнеров и услуг.

Этот критический и фундаментальный аспект технологии IoT обеспечивает то, что сервисы и одноранговые узлы могут гарантировать, для чего и кому доставляются данные.

Для проверки подлинности данных и достоверности каналов их получения ведущие центры сертификации встраивают «сертификаты устройств» в устройства IoT, предоставляя возможность выполнять проверку подлинности широкого спектра устройств.

Конфиденциальность больше не может рассматриваться как дополнение к существующим продуктам и услугам. Она должна быть спроектирована на продукты с нуля, чтобы гарантировать, что каждое действие разрешено, каждая идентичность проверена, и что эти действия и связанные метаданные не подвергаются воздействию посторонних лиц.

Это может быть достигнуто только путем определения правильной архитектуры для продукта или услуги, а также применения современных технологий шифрования в каналах связи (например, Elliptic Curve Cryptography).

Для того чтобы IoT развивался, не подвергая риску огромные группы пользователей и физические системы, необходимо применять меры информационной безопасности как на конечных точках, так и на IoT-сервисах.

Защита устройств — это в первую очередь обеспечение безопасности и целостности программного кода. Так подписание кода криптографически гарантирует, что он не был взломан после подписания и безопасен для устройства.

Устройства должны быть защищены и на последующих этапах, уже после запуска кода, так защита на основе хоста обеспечивает харденинг, разграничение доступа к системным ресурсам и файлам, контроль подключений, защиту от вторжений, защиту на основе поведения и репутации.

К сожалению, уязвимости в устройствах IoT все равно будут, их нужно будет патчить, и это может происходить в течение длительного времени после передачи оборудования потребителю.

По этой причине «управляемость по воздуху» (over-the air, OTA), должна быть встроена в устройства до того, как они попадут к покупателям.

Некоторые угрозы смогут преодолеть любые предпринятые меры, независимо от того, насколько хорошо все защищено.

Поэтому крайне важно иметь возможности аналитики безопасности в IoT. Системы для аналитики безопасности помогут лучше понять защищаемую сеть, заметить подозрительные, опасные или злонамеренные аномалии.

Литература

1. IoT Security Guidelines Overview Document // GSM Association, 31 March 2019.
2. Эталонная архитектура безопасности интернета вещей // https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1.

УДК 007 **Information Control Systems and Technologies, pp. 75-77**

Д.т.н. Бурлов В.Г., Петров С.В., Грозмани Е.С.

ПРИМЕНЕНИЕ АЛГОРИТМА ГРАДИЕНТНОГО БУСТИНГА НАД РЕШАЮЩИМИ ДЕРЕВЬЯМИ ДЛЯ ВЫЯВЛЕНИЯ СЕТЕВЫХ АТАК

Dr.Sci. Burlov V.G., Petrov S.V., Grozmani E.S.

APPLICATION OF THE ALGORITHM OF GRADIENT BUSTING OVER DECISIVE TREES FOR DETECTING NETWORK ATTACKS

В основе любой деятельности лежат решения лица, ей управляющего (далее – лицо, принимающее решения (ЛПР). Человек осуществляет анализ обстановки и выбор плана действий на основе модели решения.

Таким образом, для построения системы обеспечения информационной безопасности и эффективного управления ею, требуется обладать математической моделью решения ЛПР.

В свою очередь формирование условий, гарантирующих достижение целей деятельности, осуществляется с помощью применения естественно-научного подхода, реализуемого научно-педагогической школой «Системная интеграция процессов государственного управления» [1-3].

Сложность и гетерогенность современных телекоммуникационных систем, а также высокая динамика изменения требований к ним, порождает большое число угроз информационной безопасности.

Для борьбы с данным видом угроз предназначены системы обнаружения (и предотвращения) вторжений (СОВ, Intrusion Detection