КОНТРОЛЬ БЕЗОПАСНОСТИ В «УМНЫХ ДОМАХ» НА ОСНОВЕ IOT

Прозоровский Иннокентий Тимович

студент, Российский технологический университет, РФ, г. Москва

Интернет вещей (IoT) — это технология, которая широко используется в различных областях. Такие компании, как Samsung, LG и Apple, запускают бытовую технику, использующую IoT как часть своего бизнеса в сфере умного дома. В настоящее время разрабатываются интеллектуальные вещи, которые сочетают в себе искусственный интеллект (ИИ) и Интернет вещей. Большинство этих устройств настроены на сбор и реагирование на поведение человека (движение, голос и т. д.) с помощью встроенных датчиков. Если устройства IoT не обеспечивают высокий уровень безопасности, возможна утечка личной информации.

Умный дом состоит из компьютера, смартфона и других устройств, оснащенных подключением к Интернету вещей (IoT). В последние годы использование интеллектуальных устройств IoT, интегрированных с искусственным интеллектом (ИИ), значительно увеличилось [1]. Например, интеллектуальный датчик, такой как термостат, может управляться пользователем удаленно через подключение к Интернету. Пользователь может наблюдать за домом в режиме реального времени через IP-камеру. Разрабатываются даже дверные замки, которые включают в себя возможности подключения, позволяющие дистанционное управление. Это явление увеличивает вероятность угроз реальному пространству, в отличие от кибератак (DDoS, APT-атаки и т. д.), которые наносят ущерб киберпространству. Умный дом уязвим для угроз безопасности, потому что он использует Интернет, который использует радиочастотную идентификацию (RFID), беспроводную сенсорную сеть (WSN), Wi-Fi, 3G и 4G. Это означает, что информация, собранная датчиками, установленными в устройствах IoT, может привести к утечке личной информации злоумышленнику из-за их уязвимости.

Масштабируемость киберугроз

Среда IoT выгодна, поскольку она настраивает окружение пользователя как подключенную среду для обеспечения удобства. Однако, поскольку большинство устройств IoT подключены к Интернету, их безопасность может быть поставлена под угрозу из-за одной уязвимости. Злоумышленник может похитить конфиденциальную информацию, хранящуюся на IoT-устройствах, следить за жизнью пользователя или, при необходимости, персональные данные пользователя могут быть несанкционированно использованы. Следовательно, при разработке устройств IoT необходимо внедрить процедуры идентификации, измерения и оценки рисков, чтобы определить контрмеры против несанкционированной идентификации пользователей и контроля доступа.

Многоуровневая архитектура IoT и киберугроза

Общей архитектуры для сред IoT не существует. Однако типичная многоуровневая архитектура IoT, описываемая с точки зрения безопасности, состоит из уровня восприятия, сетевого уровня, уровня обработки, прикладного уровня и бизнес-уровня [3].

Слой восприятия: этот слой, также называемый сенсорным слоем, отвечает за идентификацию объектов и сбор информации об объектах. К вещам прикрепляются RFID, двухмерные штрих-коды и различные типы датчиков для распознавания объектов. Информация, собираемая этими датчиками, зависит от местоположения, атмосферы, окружающей среды, движения и вибрации. Эти датчики могут использоваться

злоумышленником в качестве инструмента для несанкционированного мониторинга конфиденциальности.

Сетевой уровень: этот уровень соединяет уровень восприятия и уровень приложений. Другими словами, этот уровень отвечает за передачу данных, собранных на уровне восприятия, другим подключенным устройствам по каналу связи. Среда передачи может быть проводной или беспроводной (Wi-Fi, Bluetooth, Zigbee, сотовая сеть и т. д.). Возможность подключения устройств IoT уязвима для передачи вредоносных программ и сетевых атак, таких как отказ в обслуживании.

Уровень обработки: этот уровень собирает и обрабатывает информацию, передаваемую с сетевого уровня. Он отвечает за удаление бессмысленной лишней информации и извлечение полезной информации. Этот уровень может повлиять на производительность Интернета вещей при получении большого объема информации.

Уровень приложений: этот уровень использует технологию IoT или определяет все приложения, реализованные в IoT. IoT может быть реализован в умных домах, умных городах и смартфонах, которые ими управляют. Поскольку предоставляемые услуги зависят от информации, собираемой датчиками, они могут быть разными для каждого приложения. Особенно когда IoT используется в умном доме, могут возникать различные внутренние и внешние угрозы и уязвимости.

Бизнес-уровень: бизнес-уровень представляет предполагаемое поведение приложения. Этот уровень отвечает за управление и контроль приложений, бизнес-моделей и моделей доходов IoT, а также управляет личной информацией пользователя. Этот уровень уязвимости может позволить злоумышленнику использовать приложение не по назначению.

С точки зрения многоуровневой архитектуры IoT датчики смартфонов могут вызывать вторичный ущерб, например утечку личной информации. Если на этом устройстве установлено приложение, ущерб может быть продлен.

Осведомленность об IoT-среде для выявления угроз и активов

Большая часть активов представляет собой ряд систем управления информационной безопасностью, отвечающих требованиям пункта 5 ISO 27001. Этот объем должен включать управление интерфейсом в соответствии с требованиями. При определении области действия актива с точки зрения системы управления информационной безопасностью (СУИБ) важно определить критический актив, который может быть подвержен угрозе [2]. Идентификация этих активов является отправной точкой в выявлении уязвимостей и угроз в сценариях, используемых для анализа риска. На этом уровне датчики, используемые для оборудования IoT, устанавливаются в диапазоне активов.

Датчики отвечают за сбор данных с объектов. К сожалению, если программное обеспечение, установленное на устройстве IoT, заражено вредоносными программами, такими как шпионское ПО, или если пользователь подвергается воздействию незащищенного Wi-Fi, идентификатор и пароль устройств IoT раскрываются. Пользователь может предоставить злоумышленнику отрицательную возможность. для доступа к данным конфиденциальности. Типы датчиков, установленных в устройствах IoT, подразделяются на датчики движения, датчики окружающей среды и датчики положения. Утечка информации в оборудовании IoT может быть вызвана датчиками света, движения, магнитными, акустическими, GPS и камерами. Собранные данные датчиков могут раскрывать пароли, образ жизни и личную информацию о местоположении [2] (см.Таблица 1).

Таблица 1.

Датчики мобильных устройств можно разделить на датчики движения, датчики окружающей среды и датчики положения. Утечка информации возможна за счет интеграции данных с этих датчиков [2]

Тип датчика	Датчик	Описание
Датчики движения	Акселерометр	- Измерение ускорения по осям X, Y и Z - Можно проверить изменение скорости или силы мобиль
	Сила тяжести	- Измеряет гравитационное ускорение по осям X, Y и Z - Распознает горизонтальное или вертикальное направлен верхнюю и нижнюю точки отсчета
	Гироскоп	- Измеряет скорость вращения по осям X, Y и Z - Проверяет наклон или вращение мобильного устройства
Датчики окружающей среды	Световой датчик	- Измеряет свет в л х - Используется для регулировки яркости экрана мобильно зависимости от окружающей среды.
	Датчик температуры	- Измеряет температуру окружающей среды - Устанавливает или контролирует температуру мобильно
	Датчик приближения	- Измеряет расстояние между экраном мобильного устрой измеряемым объектом без физического контакта
	Аудио датчик	- Микрофон: обнаруживает акустический сигнал - Динамик: воспроизводит звуковой сигнал
	Датчик камеры	- Управляет интенсивностью освещения и атмосферой для фотографий и видео на мобильных устройствах.
	Датчик барометра	- Измерение давления мобильного устройства
Датчики положения	GPS-датчик	- Использует спутники GPS для измерения текущего мест времени мобильного устройства
	Магнитный датчик	- Измеряет азимут, используя магнитное поле Земли, и пр приложениям компаса

Злоумышленник может вывести конфиденциальность пользователя через собранные данные и утечку личной информации:

Атака с выводом по нажатию клавиши: вывод по нажатию клавиши — это распространенная угроза, которая может возникнуть в оборудовании IoT. Большинство коммерчески доступных устройств IoT включают устройства ввода, такие как сенсорные экраны, сенсорные панели и клавиатуры.

Атака с выводом задачи: вывод задачи — это тип атаки, который выводит информацию о текущей задаче или приложении на устройстве IoT. Установленный в IoT-устройстве датчик фиксирует отклонение значений данных для различных задач, выполняемых на устройстве. Злоумышленник может использовать эти значения, чтобы сделать вывод о процессах выполнения и приложениях внутри устройства.

Атака определения местоположения: вывод местоположения — это атака на конфиденциальность местоположения, основанная на акустическом побочном канале. Эта атака использует модель акустического отражения голоса в месте нахождения пользователя и не зависит от характерного фонового шума. Если злоумышленник может контролировать устройства IoT, он может идентифицировать личную информацию, такую как дом или место работы пользователя [4].

Подслушивание: устройства IoT, такие как динамики с искусственным интеллектом, используют аудиодатчик для набора номера и получения голосовых команд и других функций. Вредоносное ПО, использующее приложение голосового помощника, может использоваться для различных вредоносных действий, таких как дублирование голосовых команд и передача информации. Им можно управлять через SMS и внешний канал управления Wi-Fi [3].

В заключении отметим, что в случае умного дома оборудование IoT настраивается и используется по-разному для каждого пользователя. Следовательно, чтобы справиться с риском, необходима их количественная оценка. С точки зрения ситуационной осведомленности оценка риска направлена на побуждение лиц, принимающих решения, к принятию соответствующих решений.

Список литературы:

1. Витунскайте М., Хе Ю., Брандштеттер Т., Янике Х. Умные города и кибербезопасность: мы уже на месте? Сравнительное исследование роли стандартов, управления рисками третьих лиц и владения безопасностью. вычисл. Безопасность 2019 [Электронный ресурс]. – Режим доступа: https://www.sciencedirect.com/science/article/pii/S0167404818310423. – Дата доступа: 29.11.2022.

2. Фурман, Я.А. Комплекснозначные и гиперкомплексные системы в задачах обработки многомерных сигналов / Я.А. Фурман. - М.: [не указано], 2021.- 955с.

3. Хювёнен, Э. Мир Лиспа. Том 2. Методы и системы программирования / Э. Хювёнен, И. Септянен. - М.: [не указано], 2021. - 752 с.

4. Спрос на умный дом вызван потребностью в безопасности, комфорте и сбережении энергии. [Электронный ресурс]. – Режим доступа: URL: http://www.secnews.ru/foreign/23198.htm ixzz4d-V8WVIsD. – Дата доступа: 29.11.2022.

5. База данных об утечках данных [Электронный ресурс]. – Режим доступа: https://breachlevelindex.com/data-breach-database. – Дата доступа: 29.11.2022.