Домашнее задание

Дисциплина	Защита компьютерных сетей и систем
Тема	Тема 35. Безопасность IoT-устройств и каналов передачи данных в IoT
Форма проверки	**Выборочная проверка пяти работ студентов преподавателем на следующем вебинаре и разбор типичных ошибок.** **Форма отчёта: ссылка на файл в LMS.**
Имя преподавателя	Антон Носков
Время выполнения	180 минут
Цель задания	Научиться моделировать угрозы для уровня устройств поверхности атаки IoT: ● построить диаграмму коммуникационного уровня, ● создать инвентарь ресурсов поверхности атаки коммуникационного уровня, ● определить потенциальные угрозы с помощью модели STRIDE.
Инструменты для выполнения ДЗ	Компьютер, симулятор сети передачи данных Cisco Packet Tracer 8.1.1, подключённый к интернету.
Правила приёма работы	● Чтобы выполнить задание, используйте Cisco Packet Tracer. ● Загрузите файл на Google Диск и прикрепите ссылку на файл с выполненным заданием в LMS. Важно: убедитесь, что по ссылке есть доступ. ● Файл с выполненным заданием и файл с ответами на вопросы сохраните под своей фамилией и разместите в LMS.
Критерии оценки	**Задание считается выполненным, если:** - прикреплена ссылка на файл с выполненным заданием; - доступ к материалам открыт; - даны ответы на все вопросы. **Задание не выполнено, если:** - файл с заданием не прикреплён, или отсутствует доступ по ссылке.
Дедлайн	*3 недели после вебинара*

Описание задания

Прежде чем выполнять задание

Установите симулятор сети передачи данных Cisco Packet Tracer 8.1.1:

- Cisco Packet Tracer 8.1.1 — windows 64,
- Cisco Packet Tracer 8.1.1 — ubuntu 64,
- Cisco Packet tracer 8.1.1 — MacOS X.

Инструкция по установке

Когда Cisco Packet Tracer выдаёт запрос авторизации, выберите Skills for all и авторизуйтесь через учётную запись Google. В ряде сетей может потребоваться VPN при запуске Cisco Packet Tracer.

После установки Cisco Packet Tracer откройте файл **IoT_Communication_Layer.pka.pka** *(размещён в LMS)* и начинайте выполнять задание.

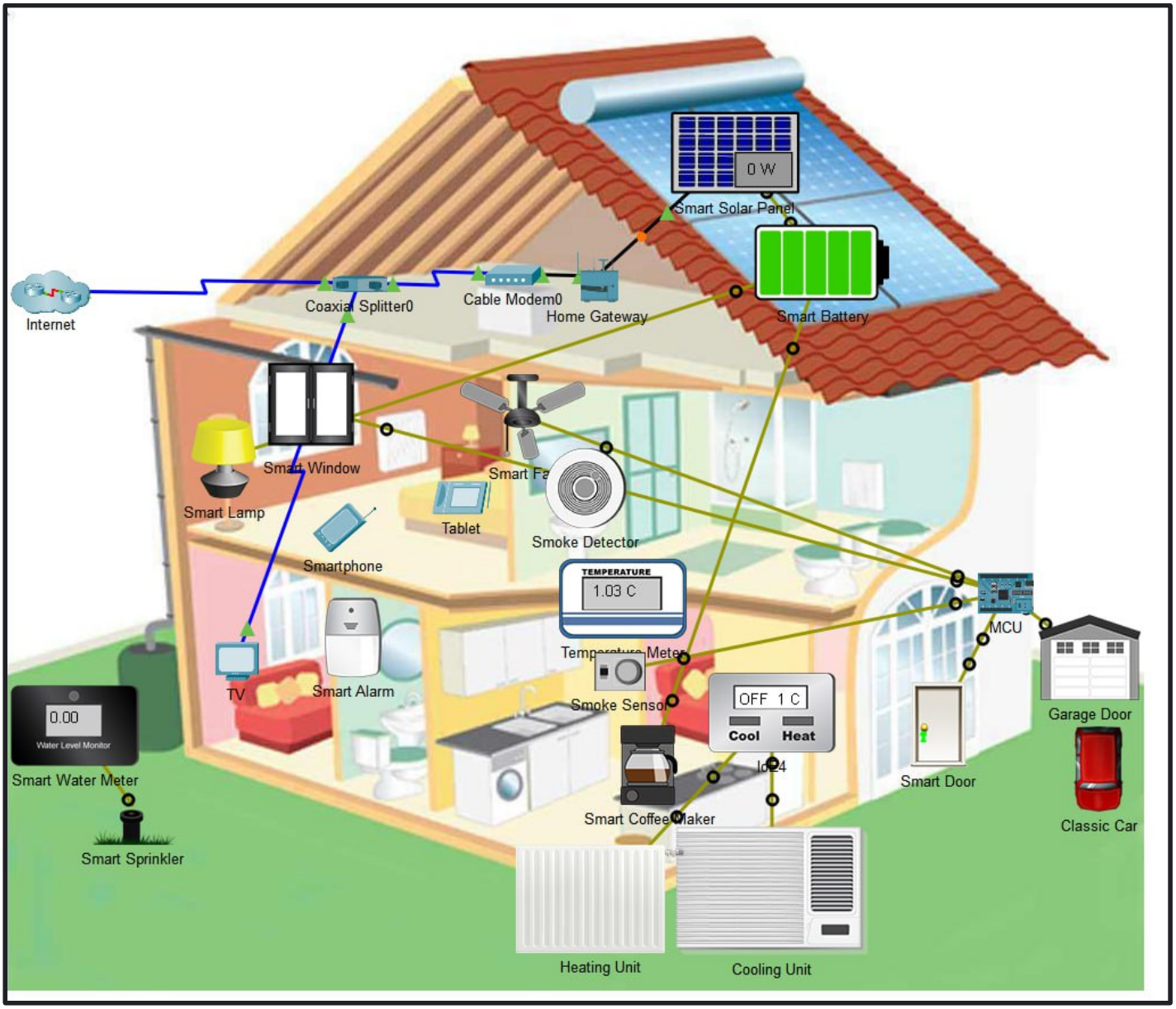
Исходные данные

Топология

Топология представляет собой домашнюю систему IoT, прототип которой был создан в Packet Tracer. На нём показан вид дома в разрезе с датчиками, исполнительными механизмами и соединениями.

Исходный сценарий

В этом задании вы будете работать с коммуникационным уровнем поверхности атаки IoT. Помните, что сеть домашней автоматизации отличается от сети CT. Сеть домашней автоматизации, с которой вы работаете, не использует Wi-Fi в качестве беспроводного протокола для датчиков и исполнительных механизмов. Вместо этого вы выберете другой протокол для сети «датчик-исполнитель-контроллер IoT», например Zigbee или Z-Wave. Контроллер обеспечивает локальную связь с беспроводными сетями в доме и интернетом. Он служит IP-шлюзом для сети датчиков и исполнительных устройств IoT. Он также функционирует как маршрутизатор, обеспечивающий связь между локальной беспроводной локальной сетью и интернетом.



Задачи

Часть 1. Построение диаграммы коммуникационного уровня.

Часть 2. Создание инвентаря ресурсов поверхности атаки коммуникационного уровня.

Часть 3. Определение потенциальных угроз с помощью модели STRIDE.

Часть 1. Схема уровня связи

Шаг 1. Выберите протокол для сети датчиков

Сосредоточьтесь на протоколах и инфраструктуре уровня связи IoT. Хотя в модели PT для связи между датчиками, исполнительными механизмами и шлюзом IoT используется Wi-Fi, для анализа вы будете использовать другой протокол.

Выберите протокол, который обычно используется в сетях домашней автоматизации для связи между датчиками, исполнительными механизмами и домашним шлюзом IoT. Помните о безопасности.

Какой протокол вы выбрали и почему?

_____

_____

_____

_____

Шаг 2. Схема сети

Используйте готовые диаграммы плана этажа из раздела «Моделирование угроз» в трассировщике пакетов IoT Device Layer из главы 3. Кроме того, заполните план чердака.

а. Заполните план чердака, включённый в приложение A PDF-версии этих инструкций Packet Tracer. Добавьте устройства сетевой инфраструктуры и их соединения, как они показаны в сети Packet Tracer.

б. Добавьте сетевых клиентов, которые не являются устройствами IoT, но всё ещё подключены к шлюзу IoT.

в. Добавьте потоки данных. Нет необходимости рисовать потоки для каждого устройства, достаточно нескольких репрезентативных устройств. Кроме того, при указании соединений между этажами можно просто написать «Подключено к…» в верхней части плана этажа. Включите несколько датчиков и приводов, смартфон и планшет, микроконтроллер.

Нарисуйте линии между устройствами IoT, шлюзом IoT и другими компонентами сетевой инфраструктуры, которые связаны друг с другом. Используйте разные цвета для соединений, использующих разные протоколы.

Помните, что некоторые датчики и исполнительные механизмы могут не иметь возможности напрямую обмениваться данными со шлюзом IoT из-за ограничений по питанию. Маркируйте или кодируйте цветом потоки данных в соответствии с используемыми протоколами.

Что позволит любым датчикам и исполнительным механизмам, находящимся вне зоны действия шлюза IoT, взаимодействовать с ним?

_____

Какие ещё протоколы используются в сети? Как планшет и смартфон могут общаться? _____

_____

Добавьте стрелки, чтобы указать преобладающее направление потока данных. В некоторых случаях потоки будут, в основном, в одном направлении. В других они будут в двух направлениях.

Какие устройства в сети домашней автоматизации подключаются к шлюзу IoT?

_____

Часть 2. Создание перечня активов поверхности коммуникационных атак

Шаг 1. Список сетей и протоколов связи

Откройте действие Packet Tracer и заполните приведённую ниже таблицу. В таблицу должны быть включены все сети, протоколы и IP-устройства, являющиеся частью сетевой системы домашней автоматизации. Определите коммуникационные отношения между активами. Сеть — это совокупность вещей, использующих один и тот же протокол. Нет необходимости перечислять здесь все устройства IoT. Вместо этого просто обратитесь к беспроводной сети датчиков и исполнительных механизмов.
Следуйте инструкциям в действии Packet Tracer, чтобы при необходимости отобразить беспроводные сетевые подключения между устройствами. Не стесняйтесь перемещать устройства, чтобы лучше понять беспроводные соединения. Обратите внимание на цветовую маркировку беспроводных соединений.

Сеть или устройство	Протокол(ы)	Связан с

Часть 3. Выявление потенциальных угроз

В этой части вы определите угрозы, используя методологию STRIDE. Постарайтесь описать как можно больше угроз, основываясь на своём опыте, странице уязвимостей OWASP IoT и других источниках информации.
Используйте модель STRIDE для создания списка потенциальных угроз. Заполните следующую таблицу угрозами для каждой категории в модели угроз STRIDE. Добавьте потенциальные угрозы, которые могут возникнуть для каждой категории STRIDE. По возможности укажите тип угрозы, используя терминологию OWASP.

Тип угрозы	Сеть или устройство	Угроза
Спуфинг — может ли злоумышленник выдать себя за того, кем он не является, или фальсифицировать данные?	Сенсорно-исполнительная сеть	
Фальсификация — может ли злоумышленник успешно внедрить фальсифицированные данные в систему?	Сенсорно-исполнительная сеть	
Отказ — может ли пользователь сделать вид, что транзакции не было?	Сенсорно-исполнительная сеть	
Отказ в обслуживании — можно ли злонамеренно отключить или сделать недоступным устройство?	Сенсорно-исполнительная сеть	
Повышение привилегий — могут ли пользователи получить доступ к привилегированным ресурсам, предназначенным только для администраторов или суперпользователей?	Сенсорно-исполнительная сеть	