Криптографическая защита данных в IoT системах

Шиляев Иван Владимирович
23.05.2022

Научные руководители:
Казловский Максим Анатольевич
Бодягин Игорь Александрович

Цели и задачи

- Изучить сетевые протоколы, применяемые в сфере IoT
- Провести сравнительный анализ этих протоколов и их безопасности
- Описать известные атаки и уязвимости
- Составить матрицу угроз
- Разработать прототип умного устройства и протокол взаимодействия с применением белорусских криптографических стандартов

Сетевые протоколы IoT

- Ближнего действия (Bluetooth)
- Среднего действия (ZigBee, Z-Wave, Wi-Fi)
- Дальнего действия (NB-IoT, LoRa WAN, SigFox)

Сравнение технических характеристик

	ZigBee	Z-Wave	Wi-Fi	Bluetooth
Стандарт IEEE	802.15.4	802.15.4	802.11	802.15.1
Скорость передачи	250 Kbit/s	100 Kbit/s	300+ Mbit/s	2 Mbit/s
Энергопотребление	Низкое	Низкое	Высокое	Низкое
Частота	2.4 GHz	908.42 MHz	2.4 / 5 GHz	2.4 GHz
Топология сети	Ячеистая	Ячеистая	Звезда	Ячеистая

Сравнение безопаности

	ZigBee	Z-Wave	Wi-Fi
Присоединение новых устройств	Предварительно загруженный ключ	DH	SAE
Шифрование данных	AES-128	AES-128	AES-128
Защита целостности	MIC	CBC-MAC	HMAC

Матрица угроз

✅ — наличие защиты
❌ — отсутствие защиты
⚠️ — зависимость от версии протокола и прочих условий

	ZigBee	Z-Wave	Wi-Fi
«Человек посередине»	✅	⚠️	✅
Атака повторного воспроизведения	⚠️	✅	✅
Защита от «чтения назад»	⚠️	⚠️	⚠️
Атака понижения версии	✅	❌	⚠️

Разработка прототипа

Проблематика

- Первоначальной задачей был поиск существующих имплементаций, позволяющих вносить изменения, с целью их доработки и внедрения белорусской криптографии
- Практически не было найдено открытых реализация последних версий протоколов
- В связи с этим был выбран подход с самостоятельной реализацией криптографического уровня поверх установленного соединения

Разработка прототипа

Задачи

- Выбор микроконтроллера
- Установка соединения между управляющим устройством (компьютером) и конечным устройством (контроллером)
- Разработка прошивки для конечного устройства и клиентского приложения для управляющего устройства
- Реализация защищённого обмена сообщениями с использование белорусского криптографического стандарта СТБ 34.101.77

Разработка прототипа

СТБ 34.101.77

- «Криптографические алгоритмы на основе sponge-функции»
- Алгоритмы предназначены для обеспечения конфиденциальности, целостности и подлинности информации
- Алгоритмы подразделяются на алгоритмы хэширования и программируемые алгоритмы

Разработка прототипа

Модель

- Конечное устройство подключается к сети Wi-Fi, в которой уже находится управляющее устройство
- На конечном устройстве запускается упрощённый веб-сервер
- Клиент отправляет запросы на включение или выключение лампочки

Разработка прототипа

Технические особенности. Распределение ключей шифрования

- Уникальный ключ шифрования располагается на корпусе каждого конечного устройства в виде QR-кода
- При первом подключении устройства необходимо считать QR-код смартфоном и передать его на компьютер
- После этого компьютер генерирует новый ключ шифрования, зашифровывает его на первоначальном ключе и отправляет на устройство в своём первом сообщении

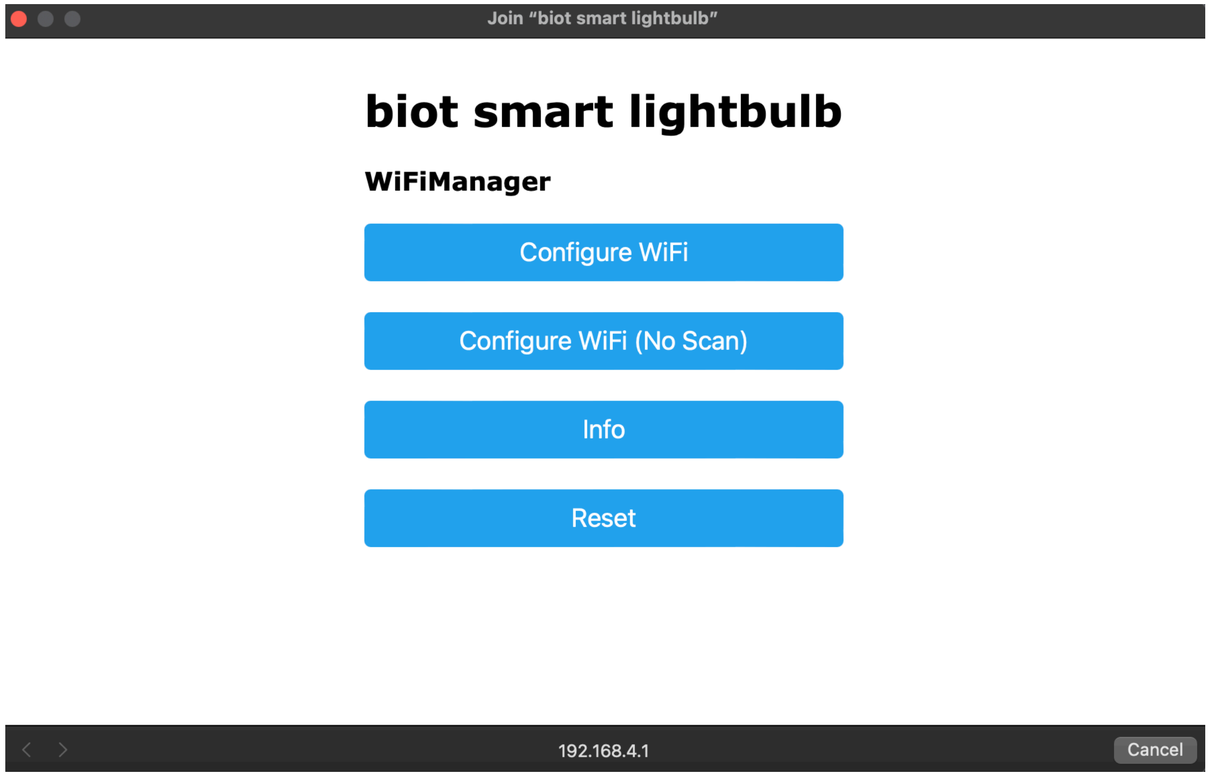
Разработка прототипа

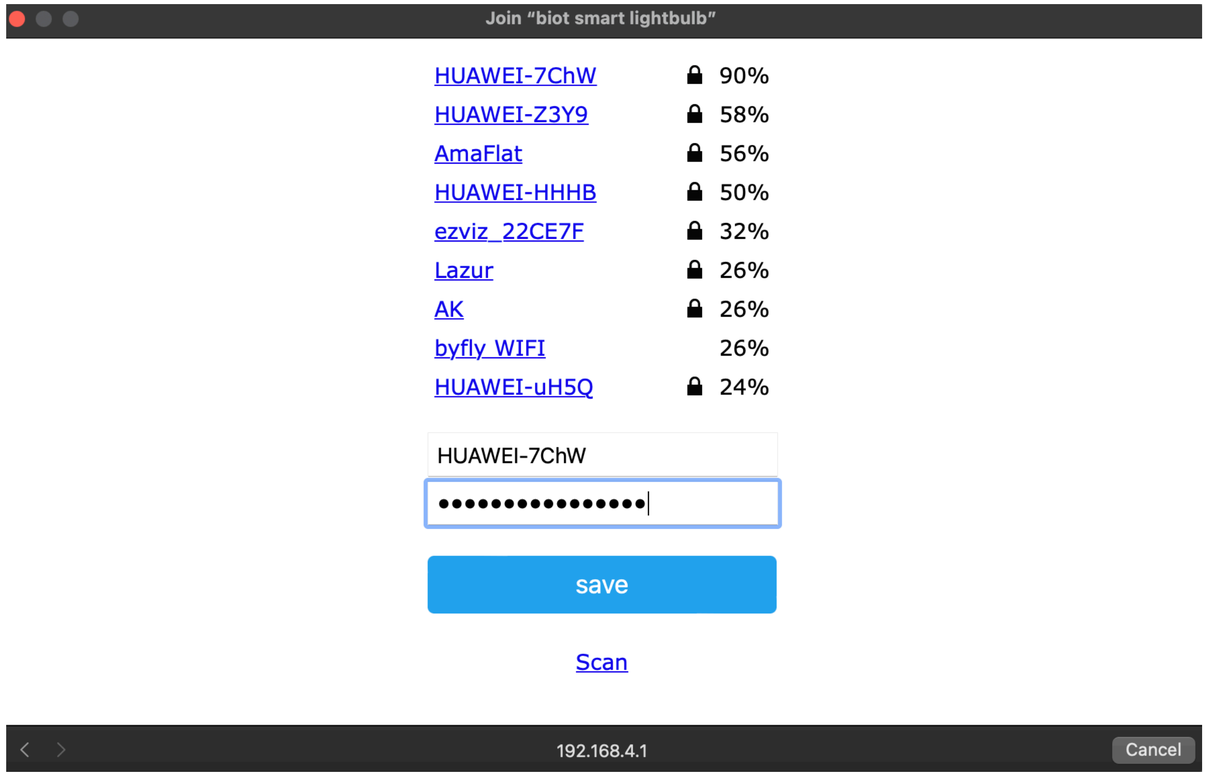
Технические особенности. Установка Wi-Fi соединения

- При запуске Wi-Fi модуль на микроконтроллере работает в режиме программной точки доступа
- На компьютере необходимо подключиться к соответствующей Wi-Fi сети, после чего откроется страница со всеми доступными Wi-Fi сетями
- В списке необходимо выбрать нужную сеть и ввести пароль
- С этого момента умное устройство будет находится в выбранной сети в качестве Wi-Fi клиента

Разработка прототипа

Технические особенности. Установка Wi-Fi соединения





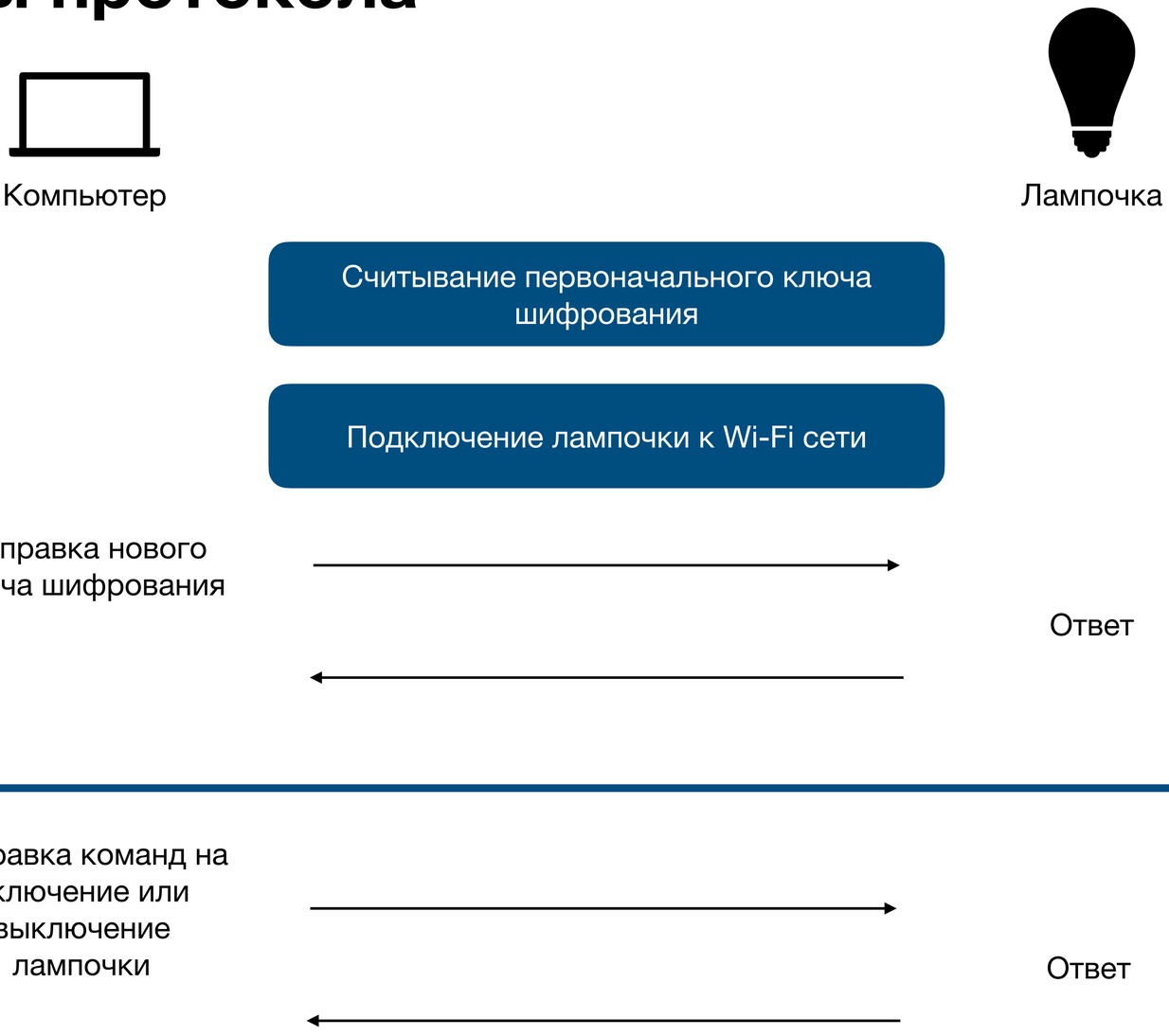
Разработка прототипа

Технические особенности. Счётчик сообщений

- Управляющее и умное устройства хранят счётчик отправленных сообщений
- На этапе установки соединения счётчик равен нулю
- После каждого сообщения (отправленного или полученного) счётчик увеличивается на единицу
- Счётчик используется в качестве синхропосылки при зашифровании и расшифровании сообщений

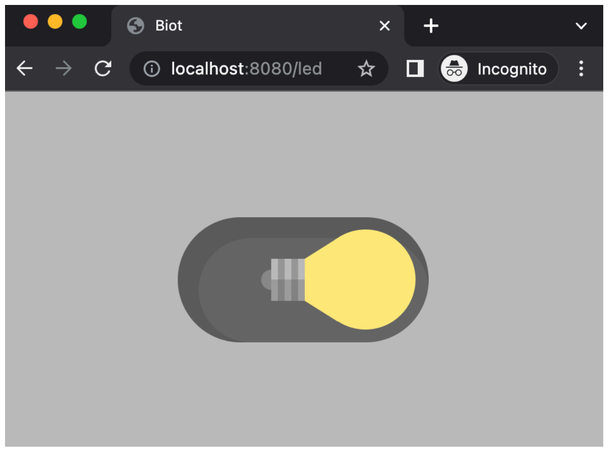
Разработка прототипа

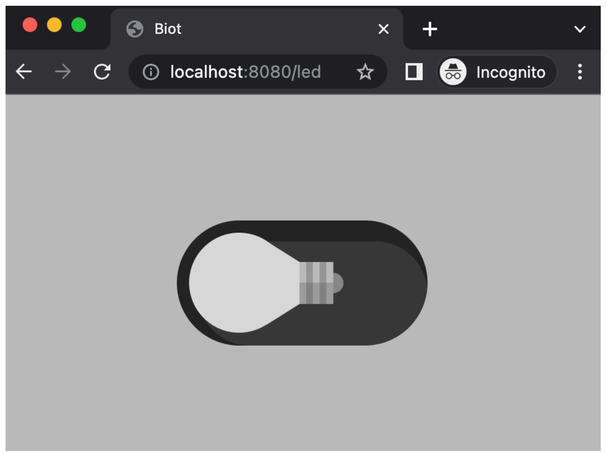
Схема работы протокола

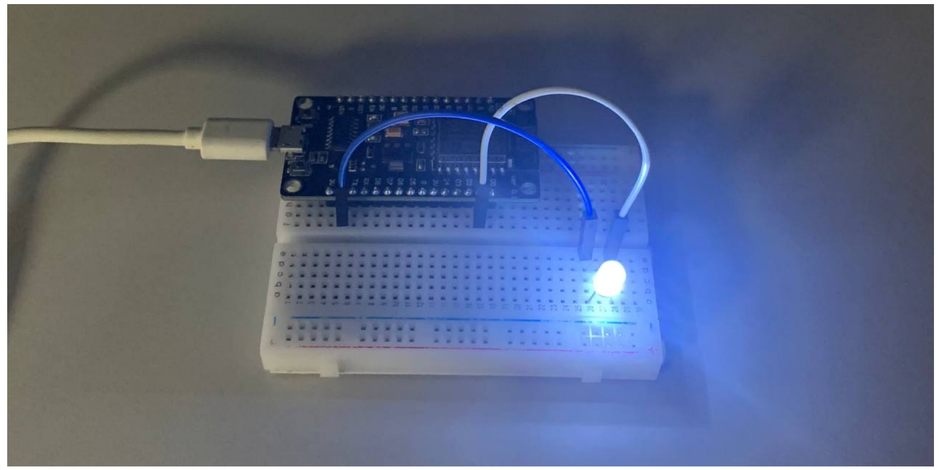


Разработка прототипа

Демонстрация







Заключение

- Выбраны три основных решения: ZigBee, Z-Wave, Wi-Fi — и проведён сравнительный анализ их технических характеристик и безопасности
- Описаны известные криптографические угрозы и успешные атаки на протоколы. Составлена матрица угроз
- Разработан собственный прототип умного устройства, а также прошивка для него с использованием белорусской криптографии

Криптографическая защита данных в IoT системах

Шиляев Иван Владимирович
23.05.2022

Научные руководители:
Казловский Максим Анатольевич
Бодягин Игорь Александрович