Криптографическая защита данных в IoT системах

Шиляев Иван Владимирович
09.06.2022, Минск

Научный руководитель:
Казловский Максим Анатольевич

Интернет вещей

«Глобальная сеть объектов, подключённых к интернету»

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 IoT системы с применением белорусской криптографии

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

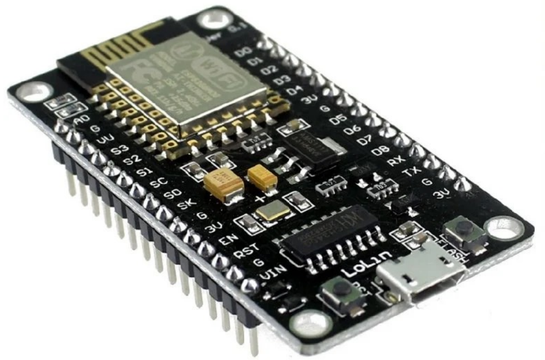
Проблематика

- Доработка существующей имплементации и внедрение белорусской криптографии
- Не было найдено открытых реализация последних версий протоколов
- Был выбран подход с самостоятельной реализацией криптографического уровня поверх установленного соединения

Разработка прототипа

Задачи

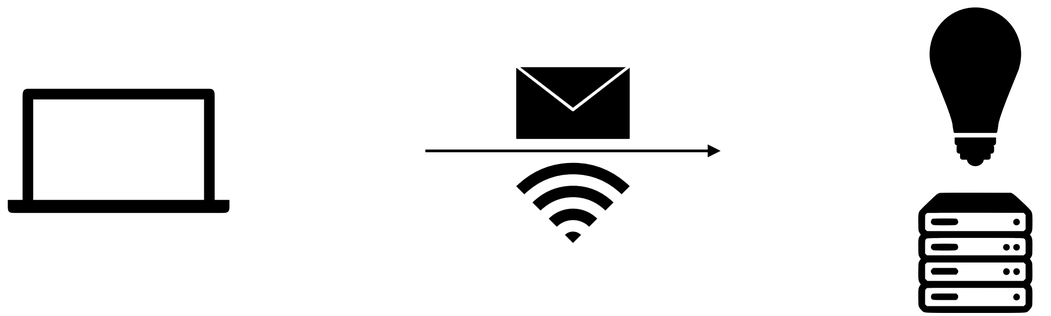
- Выбор микроконтроллера
- Установка соединения между управляющим и конечным устройствами
- Разработка прошивки и клиентского приложения
- Реализация защищённого обмена сообщениями



Разработка прототипа

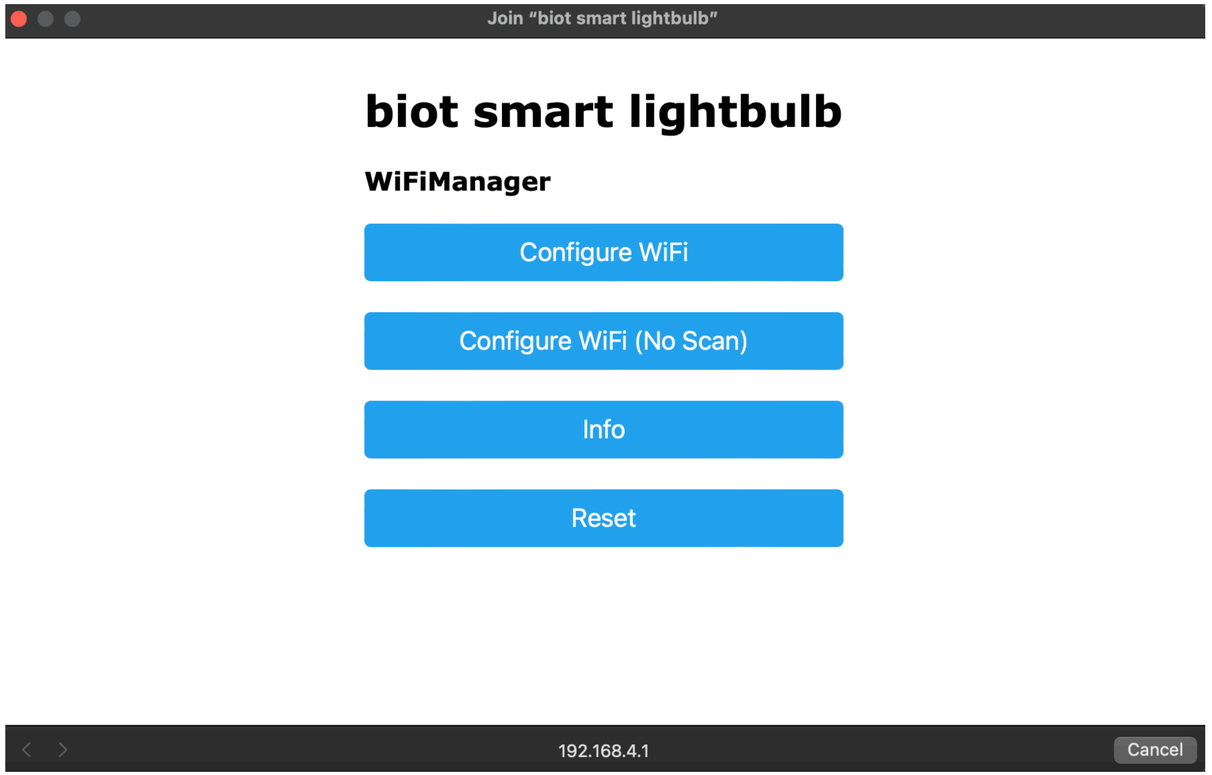
Модель

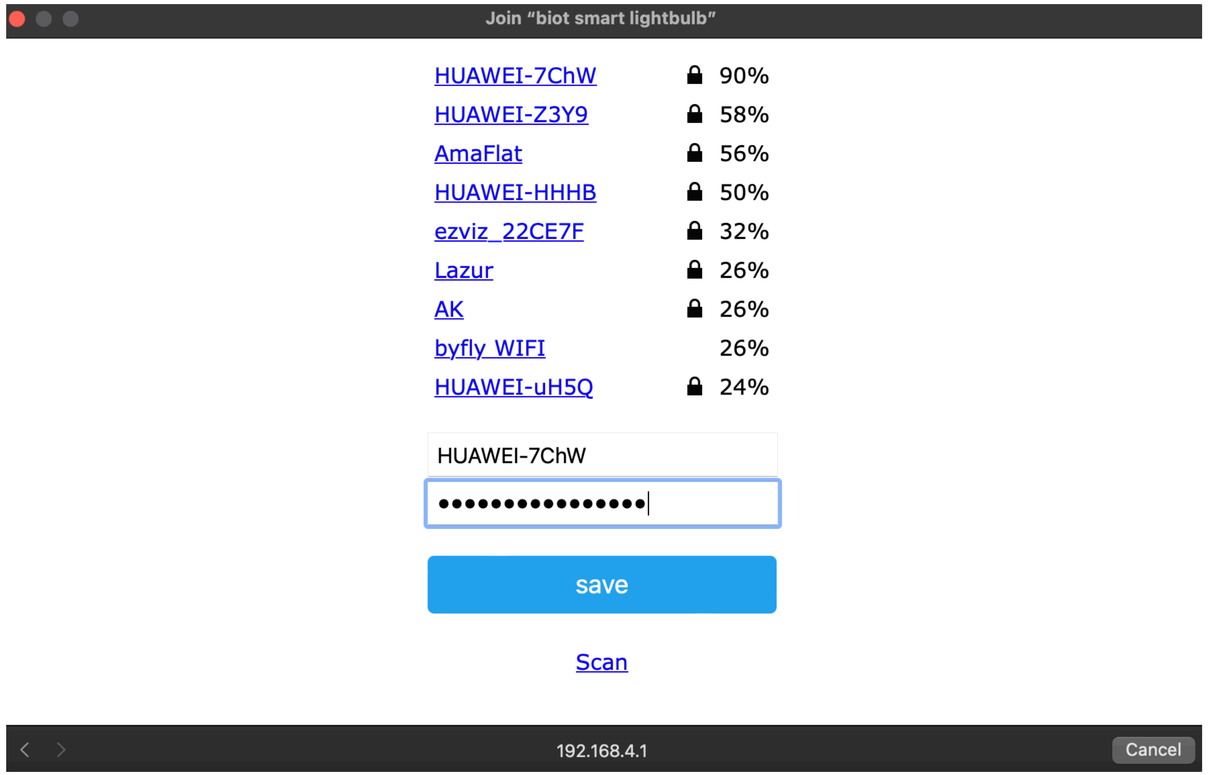
- Конечное устройство подключается к сети Wi-Fi, в которой уже находится управляющее устройство
- На конечном устройстве запускается упрощённый веб-сервер
- Клиент отправляет запросы на включение или выключение лампочки



Разработка прототипа

Технические особенности. Установка Wi-Fi соединения

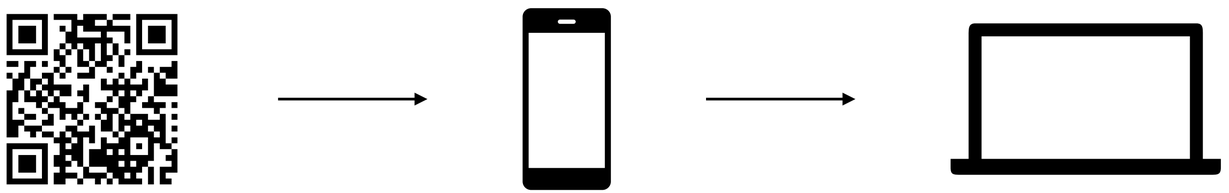




Разработка прототипа

Технические особенности. Распределение ключей шифрования

- Ключ шифрования наносится на корпус устройства в виде QR-кода
- При первом подключении QR-код считывается смартфоном и передаётся на компьютер
- Компьютер генерирует новый ключ шифрования, зашифровывает его на первоначальном ключе и отправляет на устройство



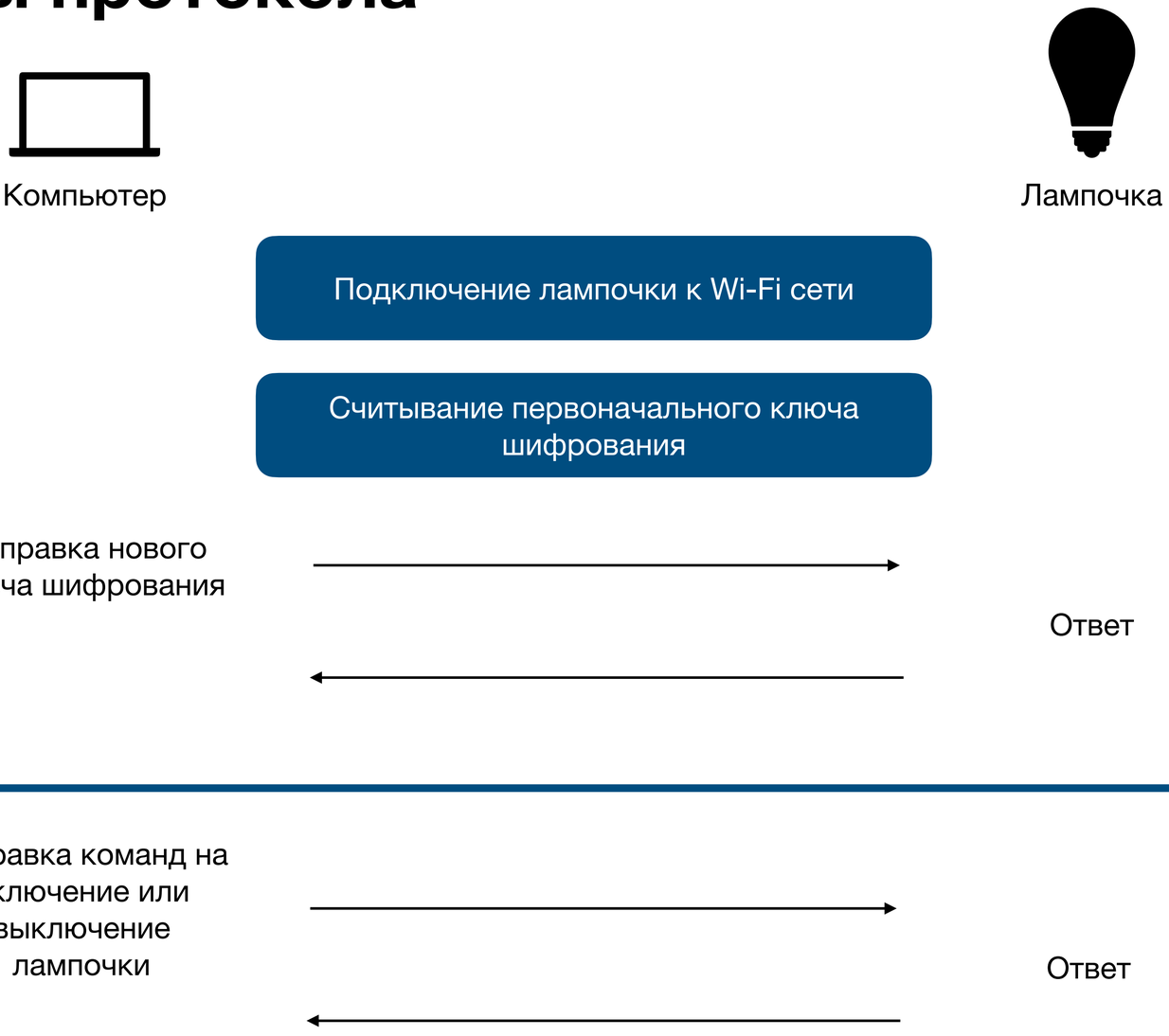
Разработка прототипа

Технические особенности. Счётчик сообщений

- Устройства хранят счётчик отправленных сообщений
- На этапе установки соединения счётчик равен нулю
- После каждого сообщения счётчик увеличивается на единицу
- Счётчик используется в качестве синхропосылки при зашифровании и расшифровании сообщений

Разработка прототипа

Схема работы протокола



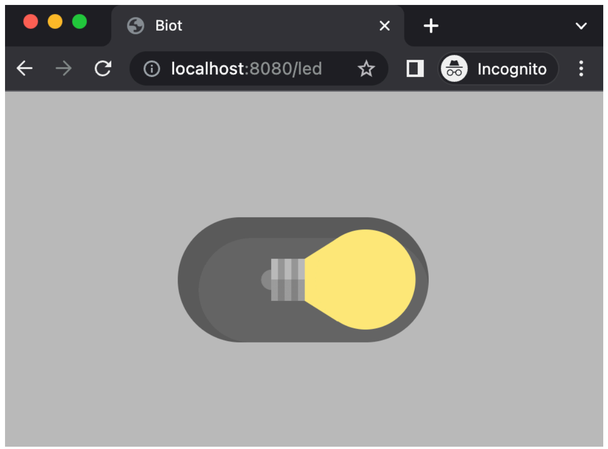
Разработка прототипа

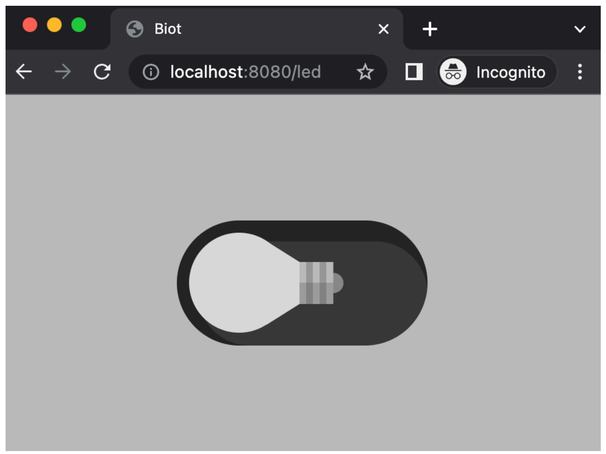
Формальная схема обмена сообщениями

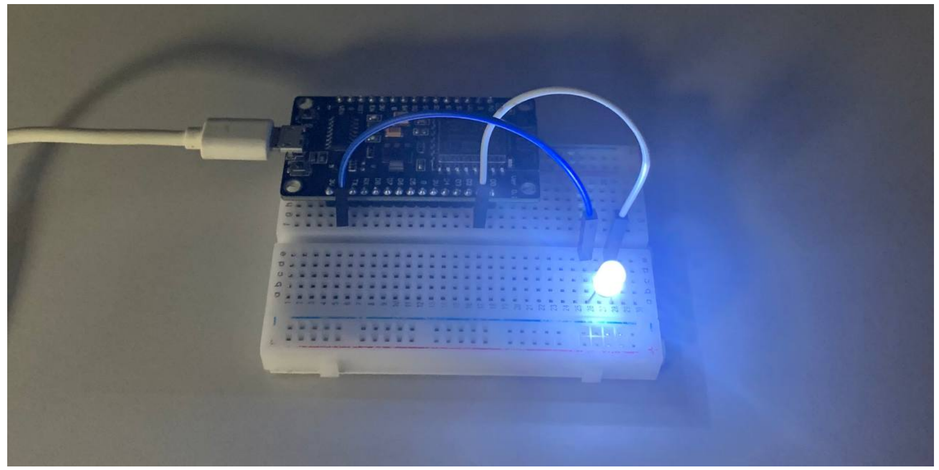
$$
\begin{aligned}
&C - \texttt{computer}, L - \texttt{light bulb}\\
&C : l \leftarrow 256\\
&\quad d \leftarrow 1\\
&\quad message\_counter\_C \leftarrow message\_counter\_C + 1\\
&\quad A \leftarrow message\_counter\_C\\
&\quad K \leftarrow \texttt{9D07352EA595...}\\
&\quad I \leftarrow \texttt{0000...}\\
&\quad X \leftarrow \texttt{«off».getBytes()}\\
&\quad (Y, T) \leftarrow \texttt{bash-prg-ae}\,[l, d]\,(A, K, I, X)\\
&C \rightarrow L : (Y, T)\\
&L : message\_counter\_L \leftarrow message\_counter\_L + 1\\
&\quad X \leftarrow \texttt{bash-prg-ae}^{-1}\,[l, d]\,(A, K, I, Y, T)\\
&\quad T_1 \leftarrow \texttt{squeeze}\,(l)\\
&\quad \texttt{if}\,(T_1 = T)\\
&\qquad response \leftarrow 200\\
&\qquad message\_counter\_L \leftarrow message\_counter\_L + 1\\
&\quad \texttt{else}\\
&\qquad response \leftarrow 500\\
&\qquad message\_counter\_L \leftarrow message\_counter\_L - 1\\
&C \leftarrow L : response\\
&C : \texttt{if}\,(resposne = 200)\\
&\qquad message\_counter\_C \leftarrow message\_counter\_C + 1\\
&\quad \texttt{else}\\
&\qquad message\_counter\_C \leftarrow message\_counter\_C - 1
\end{aligned}
$$

Разработка прототипа

Демонстрация







Заключение

- Проведён сравнительный анализ технических характеристик и безопасности сетевых протоколов IoT
- Описаны известные криптографические угрозы и атаки на протоколы
- Построена матрицы угроз
- Реализованы алгоритмы аутентифицированного шифрования и хэширования
- Разработана прошивка для умного устройства с использованием аутентифицированного шифрования и прототип умной лампочки на этой прошивке
- Разработано веб-приложение для управляющего устройства

Криптографическая защита данных в IoT системах

Шиляев Иван Владимирович
09.06.2022, Минск

Научный руководитель:
Казловский Максим Анатольевич