Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

Аутентификация в IOT.

Взгляд на традиционные схемы.
Поиск и устранение слабых мест.

Алексей Лазарев,
Ведущий менеджер проектов

Machine to Machine
M2M

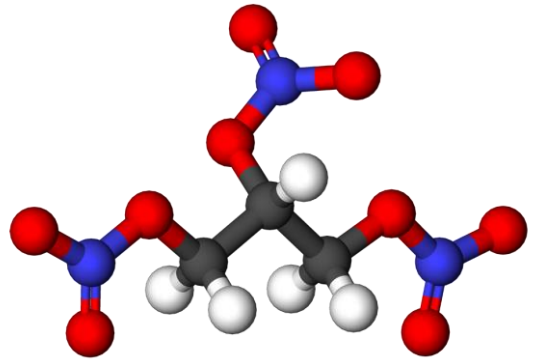
Internet of Things
IoT

- Взаимодействие без участия человека

+

- Работа в инфосетях общего пользования

=



Эволюция M2M

M2M на предприятии

- Закрытая зона
- Дружественная среда

IOT

- Среда становится враждебной
- Устройства и каналы связи и устройства подвержены атакам

Необходима аутентификация источника и его данных!

Аутентификация субъекта

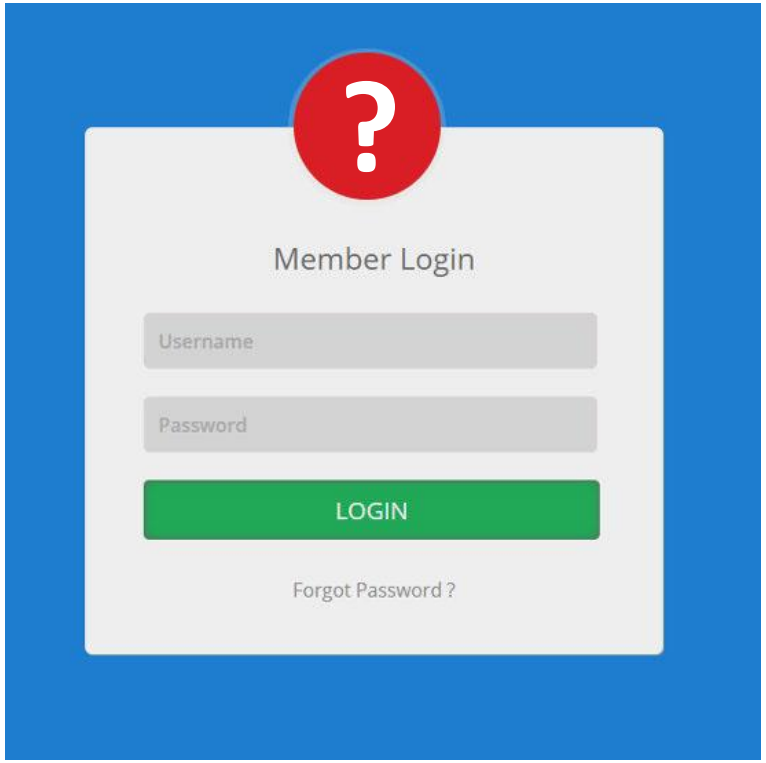
- Субъект что-то знает
- Субъект что-то имеет
- Субъект кем-то является

Аутентификация объекта

- Отсутствует фактор знания!
- У объекта нет возможности передумать и отменить аутентификацию

What are you?

Постоянные пароли

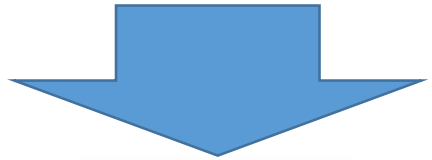


Биометрия

Двухфакторная аутентификация с применением технологии ЭП

Эффективна, если:

- Ключевой материал хранится в защищённом контейнере
- Ключ генерировался на самом устройстве
- PIN-код был изменен пользователем
- На считывателе отсутствует скиммер
- Устройство аутентификации извлекается после использования



Что есть у устройства?

- Идентификаторы
- Уникальные физические характеристики
- Данные, генерируемые объектом
- Местоположение
- Ответы на вопросы

- MITM
- Spoofing
- Replay
- Sniffing

Без криптографии – никуда!

Identity, **I**ntegrity, **I**ncessancy

M2M во враждебной среде

2013. International journal of distributed sensor networks.
How to Authenticate a Device? Forr Authentication Models for M2M Communications Defending against Ghost Compromising Attack.

1. Функциональный модуль.
   - коммуникация
   - обработка данных
   - хранение данных

2. Идентификационный модуль.
   - хранение учетных данных
   - хранение секретов

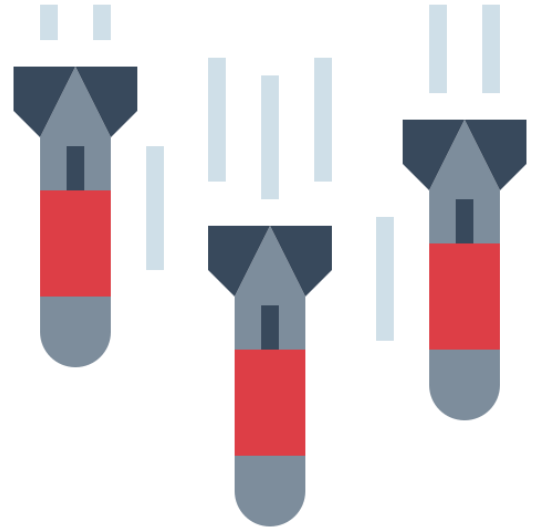
Виды атак

1. Атаки **навязывания данных**
   MITM, Replay, Spoofing

2. Атаки **компрометации учетных данных**
   Подмена, перестановка модуля, взлом модуля

3. Атаки **компрометации функционального модуля**
   Воспроизведение характеристик устройства, эмуляция

4. **Полная эмуляция устройства**
   Устройство компрометируется целиком. Комбинация 2 и 3



Аутентификация с помощью учетных данных

Выводы:

- Эффективна для защиты от атак навязывания данных канала, если есть функция **f** вида *tag=**f(cred||id||data)***, устойчивая к атакам поиска 1-го и 2-го прообраза.
- Множественные учетные данные повышают стойкость к атаке
- Не защищена от атак **компрометации учетных данных.**

Аутентификация с помощью машинных метрик.

Фингерпринтинг. Локации.

В роли идентификаторов — физические характеристики устройства

Выводы:

- Эффективна для защиты от атак компрометации учетных данных
  *tag=f(**prgrm()**||id||data)*
- Множественные характеристики повышают стойкость к атаке
- Не защищена от атак **компрометации функционального модул**я.

Аутентификация на основе ссылочных данных

Сравнение показаний с заведомо доверенными эталонами (история, соседи).

Выводы:

- Эффективна для защиты от атак компрометации функционального модуля
- Не защищена от **атак полной эмуляции**.

Аутентификация на основе свидетелей

Атака полной эмуляции не может быть отражена только лишь средствами проверяемого устройства.

В процессе аутентификации используются данные свидетелей по различным альтернативным каналам:

- датчики вскрытия
- датчики перемещения устройства
- датчики движения
- видеонаблюдение за объектом

Аутентификация на основе показаний свидетелей

Полная эмуляция устройства

Аутентификация на основе ссылочных данных

Атаки на функциональный модуль

Аутентификация на основе машинных метрик

Атаки на модуль учетных данных

Аутентификация на основе учетных данных

Атаки навязывания данных

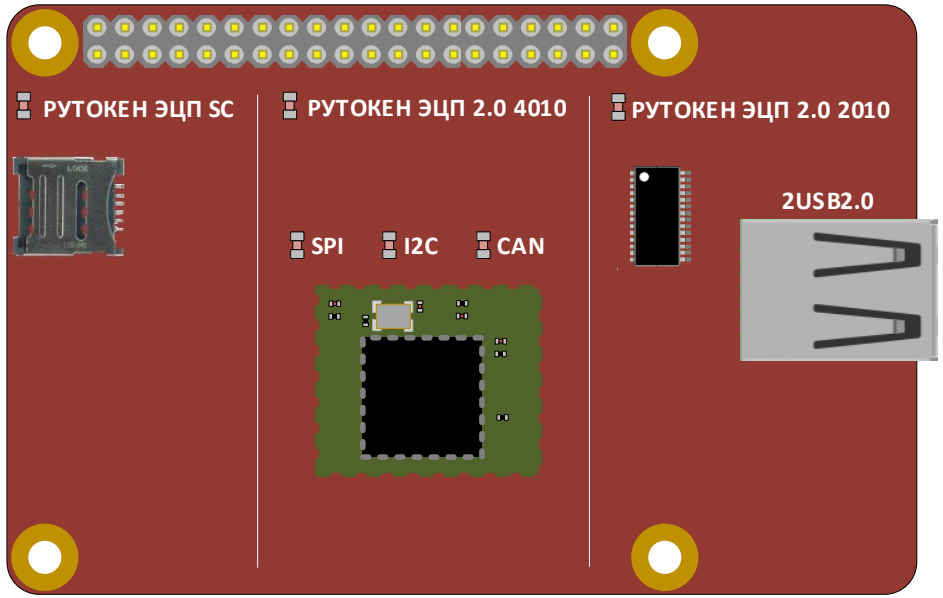
Аутентификация на основе учетных данных

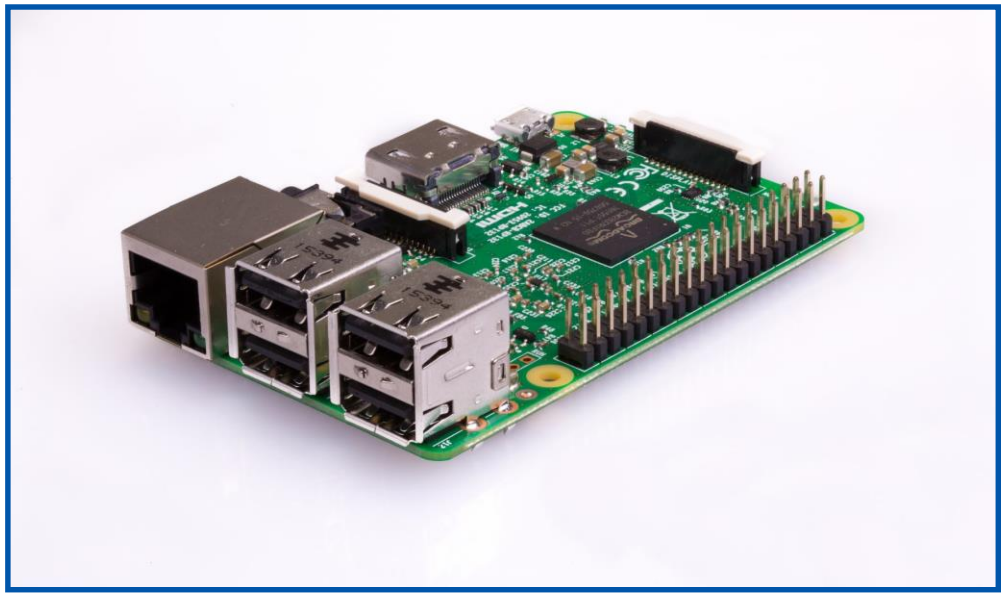
- Рутокен ЭЦП 2.0 4010
- Смарт-карта Рутокен 2151
- Смарт-карта Рутокен ЭЦП 2.0 2100
- Рутокен ЭЦП 2.0 2010

Аутентификация на основе машинных метрик. Вопрос-ответ

- Guardant SP
- Guardant Sign
- Guardant Code

Рутокен 4990





Контактная информация

Алексей Лазарев

Электронная почта:

lazarev@rutoken.ru

Телефон:

+7 (495) 925-77-90

Сайты:

www.rutoken.ru

www.aktiv-company.ru