IoT security testing starter kit

Никита Лычаный, Яндекс

whoami

- Инженер информационной безопасности в команде Алисы и Умных устройств, Яндекс
- Security: hardware, OS, mobile, reverse engineering
- Speaker: DCG#7812 2022, OffZone 2024,
  ШАД 2024 - настоящее время

Содержание

Содержание

Содержание

Содержание

Для чего безопасность IoT

Около 18 миллиардов IoT устройств

Безопасность – такое же требование к качеству продукта

Уязвимость до релиза – строчка в баг-трекере, после – отзыв партии и новости в СМИ

OWASP IoT Security Testing Guide

01 IoT device model

02 Attacker model

03 Testing methodology

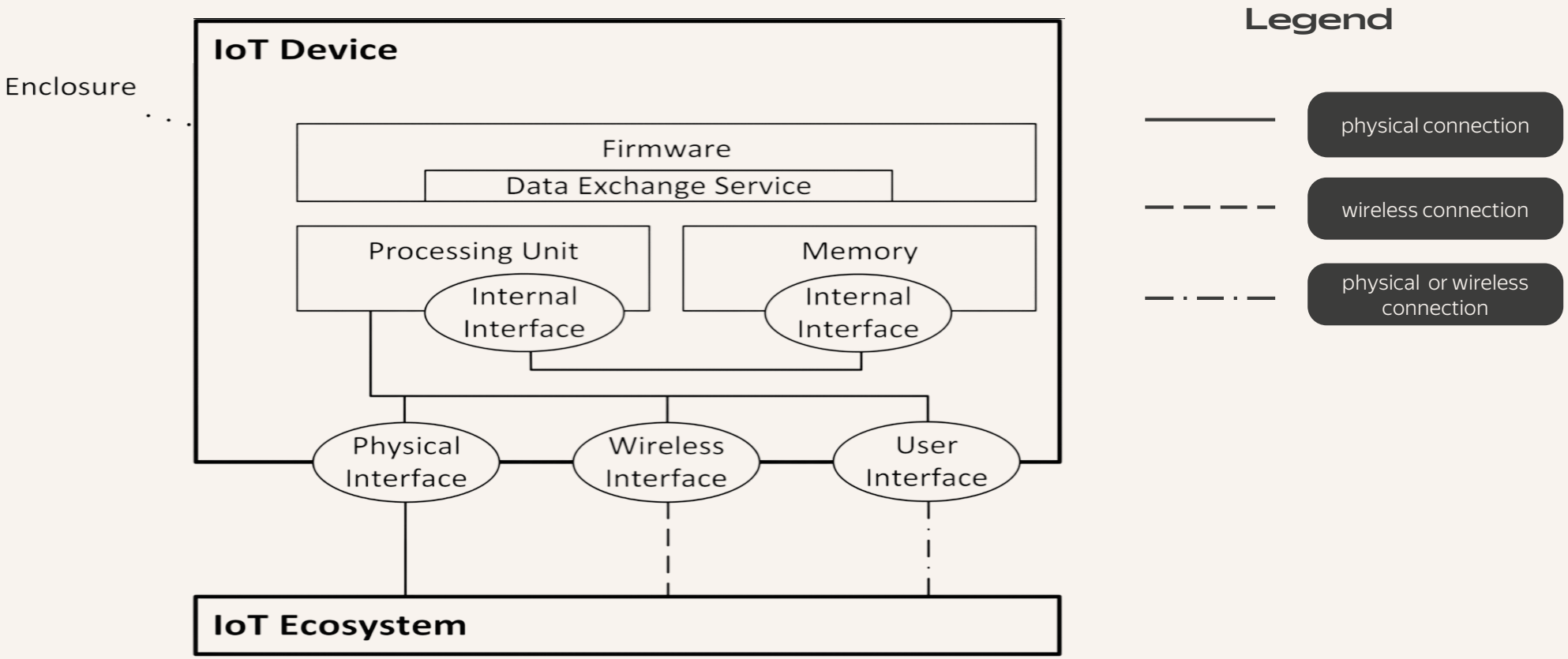
OWASP IoT Security Testing Guide

01 IoT device model

02 Attacker model

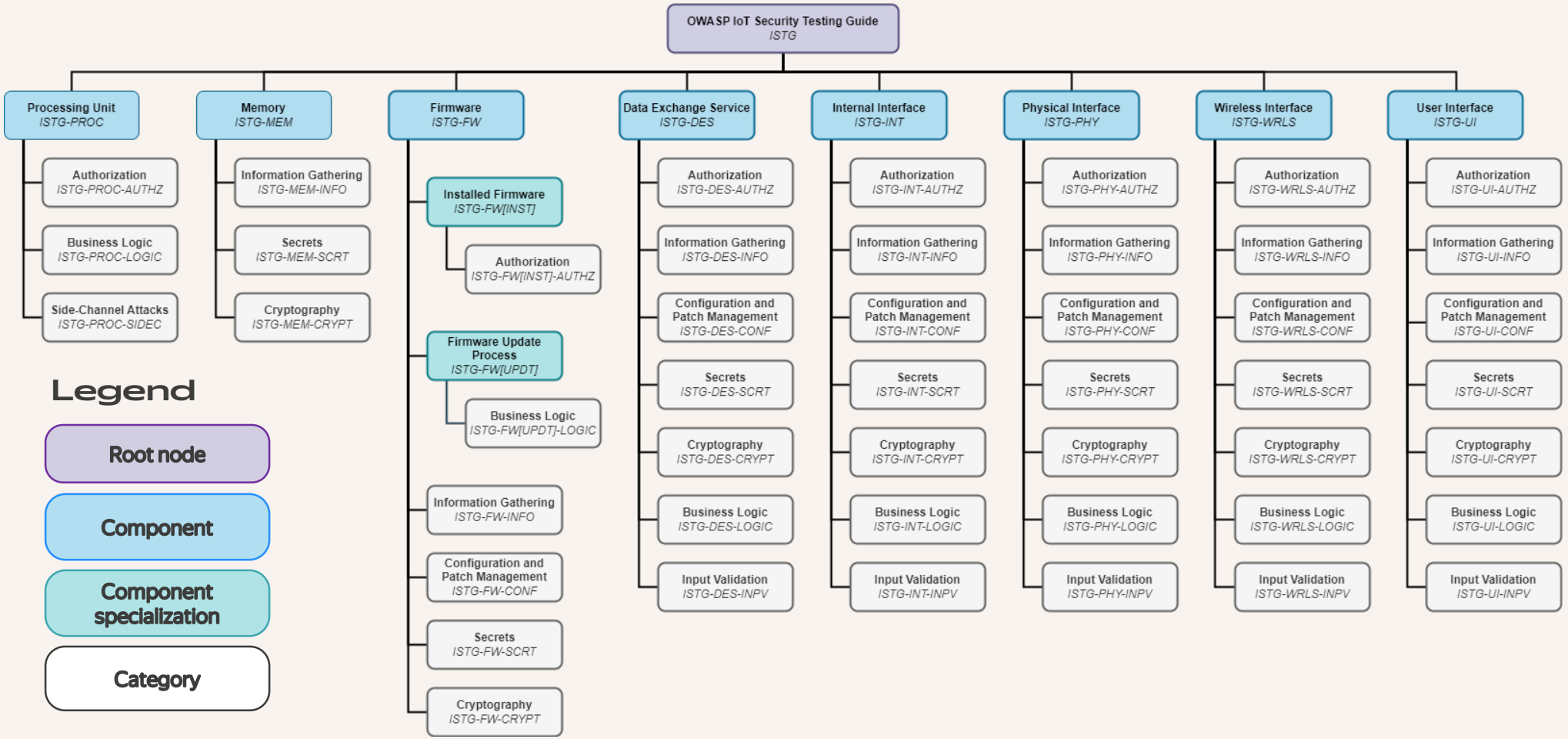
03 Testing methodology

IoT device model



https://owasp.org/owasp-istg/02_framework/device_model.html

Testing methodology



https://owasp.org/owasp-istg/02_framework/methodology.html

Testing methodology: categories

- Authorization
- Information Gathering
- Cryptography
- Secrets

Testing methodology: categories

- Authorization
- Information Gathering
- Cryptography
- Secrets
- Configuration and Patch Management
- Business Logic
- Input Validation
- Side-Channel Attacks

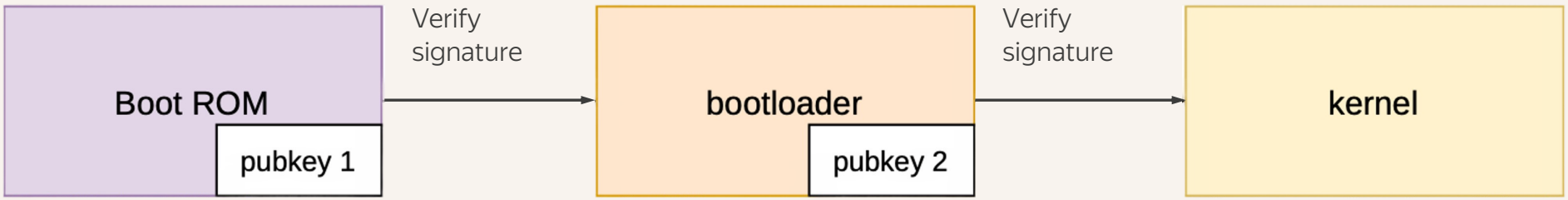
HOW and WHAT to test

Аппаратный уровень

Низкоуровневые ОС (загрузчики)

Пользовательские ОС

SecureBoot


Boot ROM
pubkey 1
Verify
signature
bootloader
pubkey 2
Verify
signature
kernel

Как проверить

01 Попробовать загрузить сторонний образ

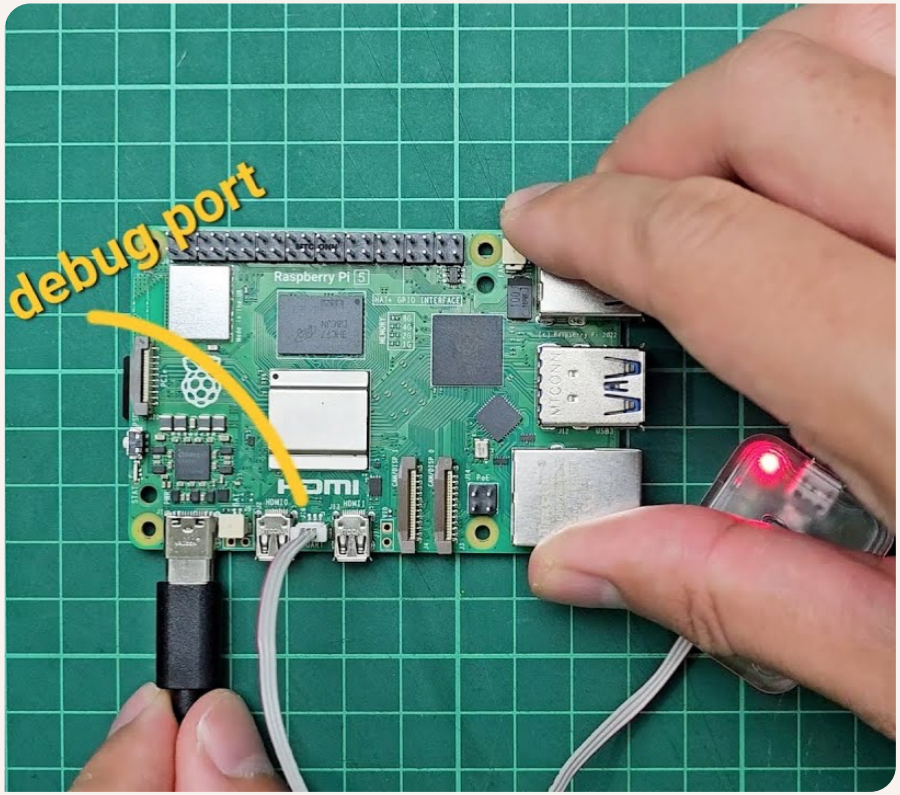
02 Проверить в логах загрузки

03 Использовать инструменты вендора

Как проверить (esp32)

```
idf.py secure-verify-signature --keyfile ./my_signing_key.pem image_signed.bin
```

Debug interfaces



01

Должны быть отключены дебажные интерфейсы USB, UART, SPI, JTAG и т.д.

02

Если нет возможности отключить – внедрить аутентификацию

Raspberry Pi 5 UART Debug Port - Cytron Technologies (YouTube)

U-Boot

- Прерывание загрузки – доступ к CLI
- Подмена env, bootargs – загрузка своего ядра
- Загрузка по сети (TFTP) или с внешнего носителя (USB/SD) без проверки подписи
- Команды md/mw – чтение и модификация памяти напрямую

Как проверить

```
CONFIG_BOOTDELAY=-2 — автозагрузка без возможности прерывания
CONFIG_AUTOBOOT_KEYED — прерывание только по секретной комбинации
CONFIG_ENV_IS_NOWHERE — environment read-only, нельзя перезаписать
CONFIG_FIT_SIGNATURE — обязательная верификация подписи образа
Отключены команды: md, mw, tftpboot, usb, mmc
```

Как проверить

depthcharge

(https://depthcharge.readthedocs.io/)

Пользовательские ОС

01 Шифрование данных + проверка целостности

02 Взаимодействие только по https

03 Только доверенный список сертификатов

04 Механизмы безопасности ОС

05 Принцип минимальных привилегий

Шифрование данных + проверка целостности

01

Шифрование и проверка целостности включается
на этапе сборки прошивки

02

Проверить: утилиты dm-verity (Linux) avbtool (Android)

Linux

```
# Проверить что dm-verity включён
veritysetup status

# Проверить таблицу verity
dmsetup table --target verity
```

Android

```
# Проверить статус verified boot
adb shell getprop ro.boot.verifiedbootstate  # → green

# Посмотреть vbmeta-информацию образа
avbtool info_image --image vbmeta.img

# Верифицировать подпись образа
avbtool verify_image --image vbmeta.img --follow_chain_partitions
```

HTTPS + доверенный список сертификатов

01

Использовать стандартные протоколы и шифрование TLS

02

Проверять и использовать стандартный список корневых сертификатов

03

Можно ориентироваться на:
https://wiki.mozilla.org/CA/Included_Certificates

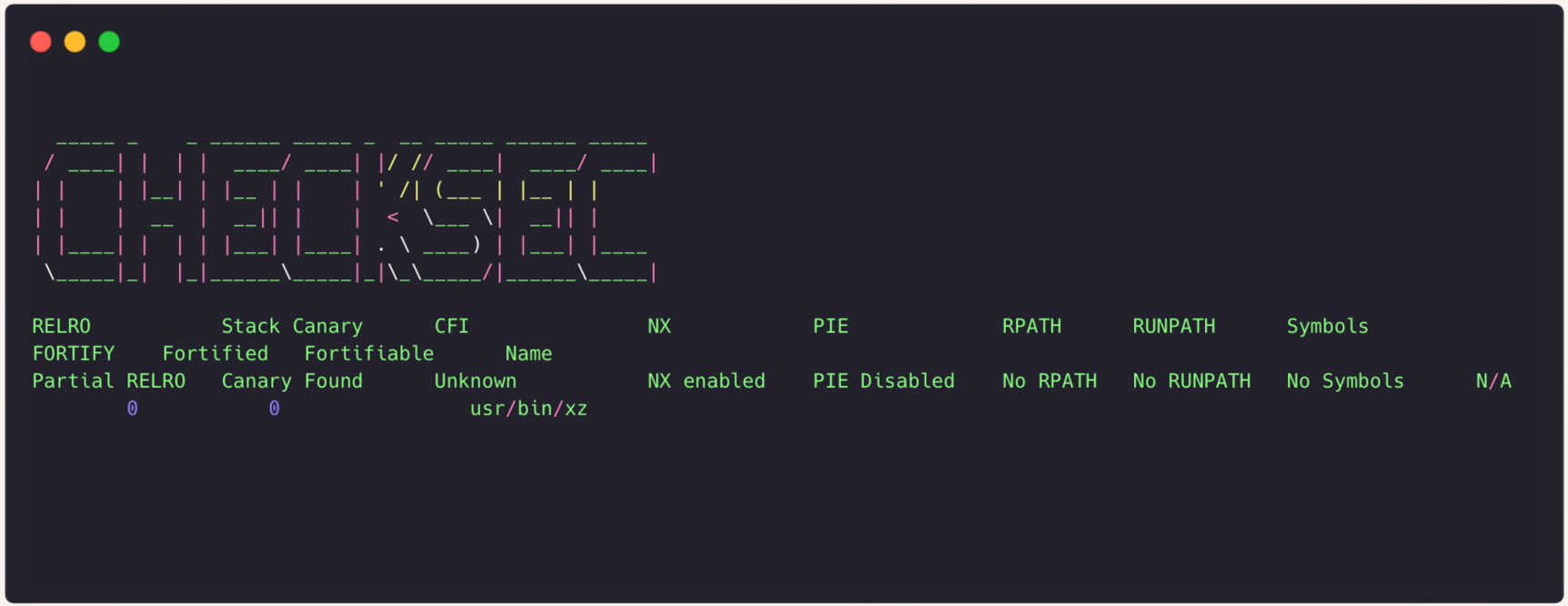
Механизмы безопасности ОС

01

Включение механизмов защиты ASLR, KASLR, NX, RELRO, PI

02

Проверить: утилитой checksec (https://github.com/slimm609/checksec)


checksec
RELRO Stack Canary CFI NX PIE RPATH RUNPATH Symbols
FORTIFY Fortified Fortifiable Name
Partial RELRO Canary Found Unknown NX enabled PIE Disabled No RPATH No RUNPATH No Symbols N/A
0 0 usr/bin/xz

Принцип минимальных привилегий

01 Отсутствие SUID-приложений

02 SELinux в режиме enforcing

03 Дефолтный пользователь – не root

```
# Кто дефолтный пользователь
whoami / id

# Сервисы от root
ps aux | grep root

# Поиск SUID
find / -perm -4000 -type f 2>/dev/null

# SELinux статус
getenforce              # Linux
adb shell getenforce    # Android

# Лишние пользователи
cat /etc/passwd
```

Android

01 Android CTS – https://source.android.com/docs/compatibility/cts

02 CtsSecurityTestCases – SELinux, CVE-патчи, права доступа

03 CtsSecurityHostTestCases – ядро, подпись прошивки, конфигурация защит

04 CtsAppSecurityHostTestCases – изоляция приложений, permissions, подпись APK

```
cts-tradefed run commandAndExit cts -m CtsSecurityTestCases

cts-tradefed run commandAndExit cts -m CtsSecurityHostTestCases

cts-tradefed run commandAndExit cts -m CtsAppSecurityHostTestCases
```

Минимальный чек-лист

- [x] SecureBoot
- [x] Debug interfaces
- [x] U-Boot hardening
- [ ] Шифрование данных + проверка целостности
- [ ] HTTPS + доверенный список сертификатов
- [ ] Механизмы безопасности ОС
- [ ] Принцип минимальных привилегий

Минимальный чек-лист

- [x] SecureBoot
- [x] Debug interfaces
- [x] U-Boot hardening
- [x] Шифрование данных + проверка целостности
- [x] HTTPS + доверенный список сертификатов
- [x] Механизмы безопасности ОС
- [x] Принцип минимальных привилегий

Спасибо за внимание!

Вопросы?

Contact @elnxl