ISEN | école d'ingénieurs
ALL IS DIGITAL!

Attack Surface Analysis

ISEN | école d'ingénieurs
ALL IS DIGITAL!

The device layer

The Device Layer

The OWASP (Open Web Application Security Project) approach

ISEN
ALL IS DIGITAL!
yncréa

- Vulnerabilities:
  - Environment manipulation
  - Tampering
  - Damage
- Device memory:
  - Default username & password
  - Sensitive Data
  - Plaintext usernames & passwords
  - Encryption keys

The Device Layer

The OWASP (Open Web Application Security Project) approach

ISEN
ALL IS DIGITAL!
yncréa

- Physical interfaces attacks
  - Storage media
  - Reset to insecure state
  - Device ID/Serial number exposure
  - Serial interface connections (UART, JTAG, I2C, SPI)
  - User & Admin access
  - Privilege escalation

The Device Layer

The OWASP (Open Web Application Security Project) approach

ISEN
ALL IS DIGITAL!
yncréa

- Firmware vulnerabilities
  - Backdoor accounts
  - Hardcoded credentials
  - Encryption keys
  - Firmware version display & last update date
  - Vulnerable services
  - Security related function API exposure

The Device Layer

The OWASP (Open Web Application Security Project) approach

ISEN
ALL IS DIGITAL!
yncréa

- Firmware updates:
  - Sent without encryption
  - Not signed
  - Update location writable
  - Verification
  - Authentication
  - Malicious updates
  - Missing update mechanism
  - No manual update mechanism

The Device Layer

ISEN ALL IS DIGITAL! | yncréa

- At the device layer two sub-layers must be analyzed:
  - The physical layer
  - The software layer

The Physical Layer

ISEN ALL IS DIGITAL! | yncréa

- Hackers can easily retrieve information about physical components:
  - CPU type
  - Memory components (SD, EPROM, eMMC, SRAM,…)
  - Radio chipset reference
  - Available physical ports: UART, JTAG, I2C, SPI
    - Ports with direct access
    - Ports on the board

Case Study

ISEN ALL IS DIGITAL! | yncréa

- Lab Work
  - FCC database information:
    - https://www.fcc.gov/oet/ea/fccid
    - Foscam camera: FCCID ZHH FI8910W
  - Things to retrieve:
    - Radio frequencies and base protocols
    - Physical access ports

The Software Layer

ISEN ALL IS DIGITAL! | yncréa

- Device firmware:
  - An embedded software containing the necessary programs used to control the IoT device
  - Can be:
    - As simple as MCU code
    - As complex as embedded versions of full operating systems

The Software Layer

ISEN ALL IS DIGITAL! | yncréa

- Firmware POIs:
  - Passwords
  - Backdoor accounts
  - Configuration files
  - Vulnerable services
  - Private keys
  - API tokens & endpoints (URLs)
  - Data storage
  - Specific code binary or source code reference

The Software Layer

ISEN ALL IS DIGITAL! | yncréa

- Security information about the firmware can be obtained through:
  - Official announcements (CERT advisories)
  - Forums & Specialized sites (Bugtraq archive, vendors' forums)
- Firmware challenges:
  - Obtaining the firmware
  - Analyzing the firmware
  - Modifying the firmware
  - Uploading a customed version of the firmware