CENSUS

IT Security Works

IDENTIFYING IoT SECURITY VULNERABILITIES

DIMITRIOS GLYNOS (@dfunc on Twitter)
dimitris@census-labs.com

IoT Nuggets - “Cybersecurity in the IoT Ecosystem” Event
Oct. 10th 2019 / Savoy Hotel, Piraeus, Greece

www.census-labs.com

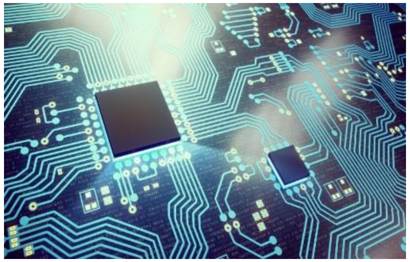
> INTERNET OF THINGS (IoT)

“the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data” – Oxford Dictionary

> TESTING THE SECURITY OF IoT DEVICES

Device

Hardware Security



Is it possible to decrypt stored data just by communicating with the secure chip?

Software Security

```
document.getElementById(
}

function updatePhotoDescription() {
    if (descriptions.length > (page * 9) + (currentImage.substring(
        document.getElementById(
    }
}

function updateAllImages() {
    var i = 1;
    while (i < 10) {
        var elementId = 'foto' + i;
        var elementIdBig = 'bigImage' + i;
        if (page * 9 + i - 1 < photos.length) {
            document.getElementById( elementId ).src =
            document.getElementById( elementIdBig ).src =
        } else {
            document.getElementById( elementId ).src = '';
        }
```

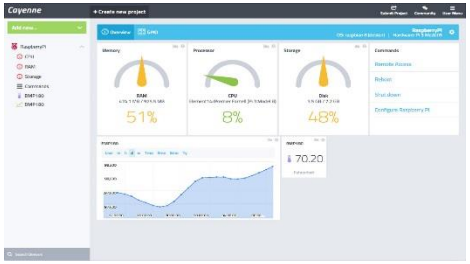
Is it possible for an unauthorized actor to remotely control the device due to a bug in the software?

Communications Security

Is it possible for someone to eavesdrop on device communications?

Command & Control

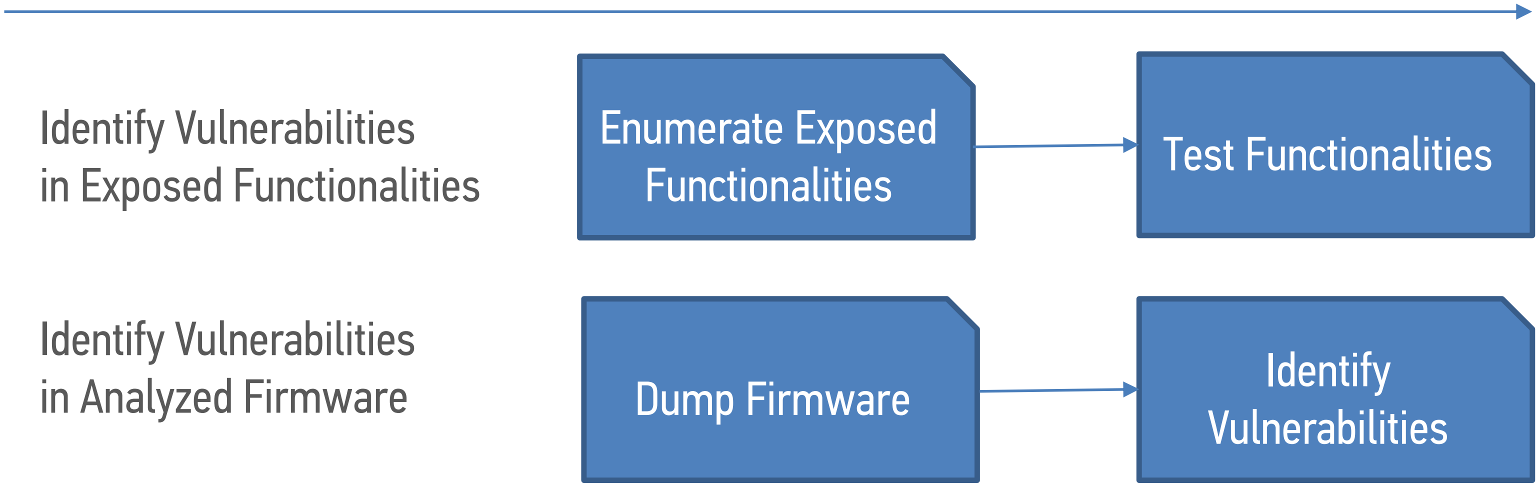
Management Platform Security



Is it possible for an unauthorized actor to collect all data gathered by the devices?

> TESTING THE SECURITY OF IoT DEVICES

Black Box Testing Timeline



Identify Vulnerabilities in Exposed Functionalities

Enumerate Exposed Functionalities → Test Functionalities

Identify Vulnerabilities in Analyzed Firmware

Dump Firmware → Identify Vulnerabilities

> TESTING CONTEXT

- Sometimes a *product* is tested before it enters the market
- Sometimes a configured *device* is tested within the context of an organization’s infrastructure
- Different contexts require different methodologies
  - And different methodologies may yield different findings!

> TYPICAL ISSUES FOUND DURING IoT PRODUCT TESTING

- Use of hardcoded credentials
- Missing/broken authentication for critical functions
- Device spoofing
- Exposure of sensitive user information
  - Unprotected cloud storage
  - Device Theft scenarios
  - Security defects in Command & Control
- Firmware uses vulnerable third party components

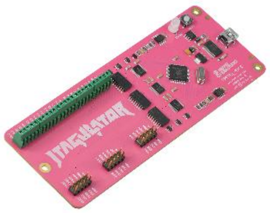
> TYPICAL ISSUES FOUND DURING PENETRATION TESTING

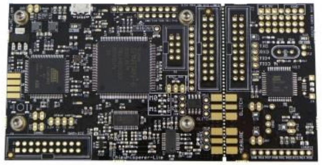
- Use of default credentials
- Disabled authentication for critical functions
- Firmware comes with known vulnerabilities
  - Unpatched device
  - A device that no longer receives security updates

> DEMO OF IoT DEVICE BUG EXPLOITATION

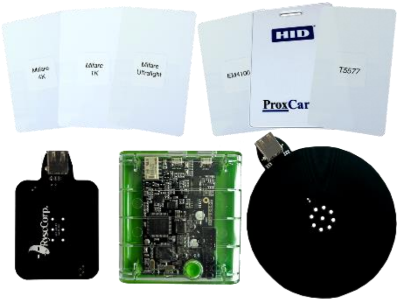
> IDENTIFYING VULNERABILITIES: THE TOOLS

Inspection Level: Hardware

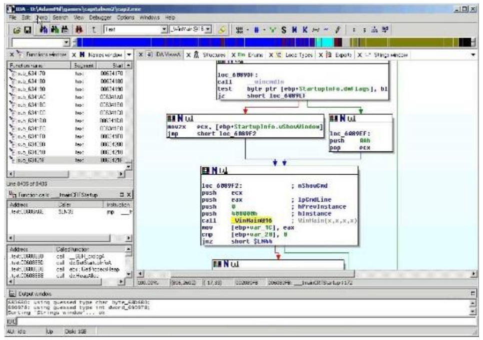


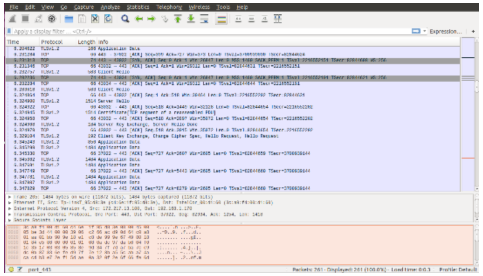


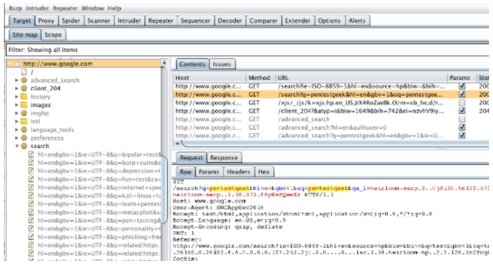
Communications



Software






Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Filter: Showing all items
http://www.google.com
Contents Issues
Host Method URL Params
Request Response
Raw Params Headers Hex

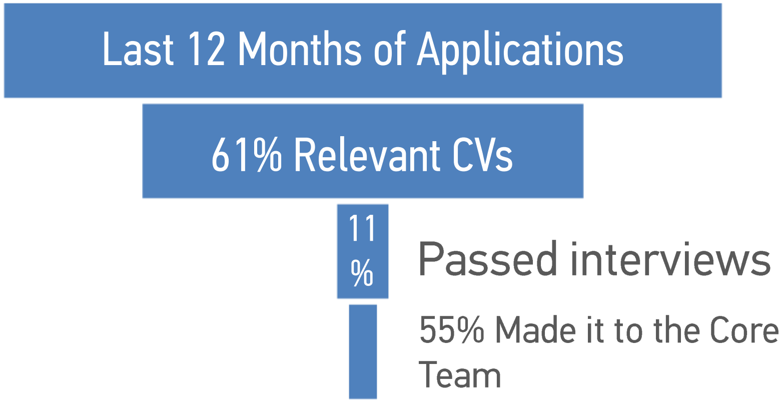
> IDENTIFYING VULNERABILITIES: THE SKILLS

- Information Security Skills
- Analytical Thinking
- Software Engineering & Debugging Skills
- Systems Administration & Network Engineering Skills
- Systems Programming Skills
- Reverse Engineering Skills
- Good Communication Skills (in English)
- Hardware Debugging Skills
- Radio and SDR Skills

> IDENTIFYING VULNERABILITIES: THE PEOPLE

- *“Cybersecurity workforce gap” 2019 report from csis.org*
  - lack of required technology skills was one of the greatest challenges facing organizations when hiring cybersecurity candidates
  - 61% percent of organizations believe that **fewer than half** of all applicants for open cybersecurity positions are actually qualified for the job
  - 23% (of IT employers) thought education programs were fully preparing students to enter the cybersecurity industry

- *Last year’s HR stats:*



Last 12 Months of Applications

61% Relevant CVs

11 %

Passed interviews

55% Made it to the Core Team

> CONCLUSION

- IoT devices have their share of security vulnerabilities
- Vendors should follow a *Secure Development Lifecycle* to catch issues early and efficiently
- Connected devices should not be used after their *security support* period
- IoT Security Testing requires a diverse skillset

Thank you!

CENSUS
IT Security Works