IoT: Client Devices

Attack Surfaces

What is an attack surface?

The attackable surface of a system

- Anything an attacker can access
- Includes things like configuration files, function arguments, network traffic, music files
- Really, anything the system touches

IoT clients have large attack surfaces

Why is it Important?

How systems can be attacked

- An attack surface describes how attackers will attempt to compromise a system

How systems can be hardened

- Understand the vulnerabilities? you can harden them

What can be neglected

- Just as important!

How to Document?

Not in code, but a document

- The exercise is worth more than documentation
- But you should document so you can review

Pictures are a good thing!

- Make it a simple and clear as possible

What kind of document?

- Doesn’t matter; PDF, MS Word, Wiki, Text, all okay

Example

THE LS COMMAND ON LINUX

- Inputs:
  - various command line options
  - some support user-defined input (—block-size, —color, etc.)
  - what about environment variables? yep! (LS_COLORS)
  - How about the filesystem?

This is the attack surface

Hardening

WE HAVE THE SURFACE DEFINED, NOW HARDEN

- Support different command line options *and combinations*
- Check for well-formed environment variables
- Check buffer lengths
- Check for well-formatted submitted data
- Attackers will submit odd characters, binary code, huge arguments, inconsistent arguments, anything that might break your system

Never ever trust user input!