IoT: Client Devices

Looking over libcurl.so

Let’s use Our RE Skillz

Reverse engineering libcurl.so

- Grab it from your guest
- $ scp -P 2222 localhost:/usr/lib/libcurl.so .

Let’s take a look at it.

TAKE A LOOK AT THE HIGH LEVEL STUFF FIRST

- arm-linux-gnueabi-readelf -a libcurl.so
- arm-linux-gnueabi-objdump -d libcurl.so > libcurl.dump
- arm-linux-gnueabi-strings -n 5 libcurl.so > strings.out
- cat strings.out | grep curl > curl-strings.out

This gives you insight into the library.

Does it look legit?

We can see the machine instruction set

- ARM, little-endian

We can see the libraries this links with

- Do we have them all on the system?

We can see exported (and imported) functions

- Check out the **curl**_ prefix

Other Metadata

SSL versions? encryption algorithms? websites?

What about the disassembly?