

## Embedded in Thin Slices

# Internet of Things Security (Part 5)

## Identifying Assests

```
{ ($_GET['defaults'] == 1)
$reboot_needed = 1;
$response = ` /apps/cmdxmlin defaults `;
}
```

In this next part of his article series on IoT security, Bob looks at how checklists and the common criteria framework can help us create more secure IoT devices. He explains how to create a list of security assets and to establish threat checklists that identify all the threats to your security assets.

By  
**Bob Japenga**

A few weeks ago, I sat through a webinar by a large player in the cell modem market. It was a well thought out presentation but I was surprised at the proposed methodology it presented for approaching IoT security. What surprised me was that it didn't address the need for identifying and assessing those assets that you want to protect. That's what I want to talk about in this article.

The problem with failing to identify and quantify the assets that you want to protect right up front is that you may expend valuable resources in securing something that does not need to be secured. Adding security features costs time and resources. Sometimes as engineers we get excited about applying new technologies even if they aren't needed. The new microprocessors are coming out with a lot of bells and whistles to help make our IoT devices more secure. Okay, maybe you don't do that. But I've been known to apply a technology or two before its time.

Let me give you one example. Many of the new chips provide tamper detection logic to notify the processor and take action if the chip has been tampered with (**Figure 1**). As designers we need to ask the question: "If someone could obtain the complete binary image of the software contained in my device, what assets would be at risk?" In some cases, none. But it is important to ask the question.

I contend that one of our first tasks in designing secure IoT devices is to identify the tangible and intangible assets that you want

to protect. Once identified, we need to assign a risk factor to the asset for this particular design.

So, what is an asset? According to ISO 27001, an asset is "anything that has value to the organization" (**Figure 2**). Is that broad enough for you? Not completely for me. Okay, I hear my readers saying: "Bob, there you go again, you old curmudgeon. Disagreeing with an international standard!" I want to make sure we use "value" as broad as possible. For a given device, an asset that needs to be protected by my design may not have value to my organization. But it might have value to the organization that owns the wireless network that the device is connected to. Although you could argue that the 27001 definition encapsulates this, I want to make sure that our definition includes not just things that are of value to our organization, but things that are of value to our customers and the public network that we are dependent upon. I would say an asset is "anything that has value to the organizations involved."

### IDENTIFYING THE ASSETS

Let's look at some of the assets that I think need to be considered to be protected. I would love to hear from you if you can add to this list. I will include them in a future article.

**Intellectual property:** At the beginning of the design of a product it's important to identify what is the intellectual property that you want to protect? For example, the electronic design might be something that

you want to protect as a whole. We have seen entire projects that we designed copied chip for chip and manufactured and marketed in another country. We have even seen drawings copied and crudely erased drawing numbers replaced with the thief's own drawing number. Sometimes, we may not be concerned with the entire electronic design, but we want to protect a particular proprietary circuit. On the other hand, perhaps the electronic design doesn't need to be protected because it would be of very little use without the software.

The binary or executable of the software is another piece of intellectual property. Is that something you want to protect? We have worked with some customers who have said: "No. We don't need to protect against someone stealing the binary of the software since we are continually innovating. By the time they reverse engineer the software, we will have greatly enhanced the product and their binary will be worthless in the market place." Not all of us have that luxury.

Certain proprietary algorithms may be the "secret sauce" that makes a product successful. If the algorithm was discovered by a competitor, would the organization suffer significant harm?

With the advent of interpretive languages, many products embed the source code—script files, Python code, Basic code, PHP, Javascript and so on—in the device. Does any of the source code embedded in the device need to be protected?

The IoT device may store other information of a proprietary nature that needs protection. For example, the device may store a history of the device soft-failures that were corrected or worked around that could be exploited by a competitor. This is not an easy item to drill into. We have to think like a crook. Is there any data that, if it got into the wrong hands, could cause harm to your company, your client or someone else?

The entire file system may be another asset that you may want to protect. Certainly, if stored on a removable device without encryption, the file system is important to protect.

**Company reputation:** This is not a very useful asset on our checklist. It is both intangible and hard to place a value on. And of course, we want to protect the company's reputation. In this day and age however, it seems like there are more security experts looking to uncover security breaches than there are true security breaches. This is very significant. How was Comcast's reputation harmed by Rapid7's discovery of a security breach? No one actually has to break into your system to damage your reputation. Be forewarned: Designing an insecure IoT device



**Figure 1**

Many new chips provide tamper detection logic to notify the processor and take action if the chip has been tampered with.

can destroy your reputation as a company or at least destroy it as a company in a particular field. Comcast may continue to sell cable services but will have a harder time selling the security systems after this security flaw was uncovered.

**Loss of functionality of an individual product:** This is an obvious asset. The device must function as advertised for the customer. But what functionality can be lost without compromising the primary function of the device? For example, we designed two different portable oxygen concentrators for a customer. Both have a cell modem in them for reporting data to the customer's server. If a Denial of Service attack were to take place, the delivery of oxygen to the patient should not be affected. So, for our checklist, the functionality of the device should be placed on a hierarchical list and a determination made as to what functionality cannot be lost under a security attack.

**Changed functionality of an individual product:** Another take on the above concern is the question: "If someone could completely reprogram one device to do whatever they



**Figure 2**

According to ISO 27001 an asset is "anything that has value to the organization." But it's important to view that as encompassing not just things that are of value to your organization, but things that are of value to your customers and the public network that you are dependent upon.



**Figure 3**

Even though it doesn't belong to your organization, the wireless network you use is an asset. Those networks can be vulnerable to various kinds of attacks.



wanted, would that bring any harm to the company?" "What if they could reprogram the entire fleet?"

*Loss of functionality of product line:* As more and more of our designs are being deployed in large scale fleets, identifying the risk of losing the functionality of the entire fleet is extremely important. In assessing assets, shutting down one product may be embarrassing and affect the organization's reputation, but shutting down the entire line is much more serious. Most if not all of us would put this as an asset that must be protected at all reasonable costs. This asset can then be translated into a high-level requirement like: "The system shall be designed such that a security breach on one device cannot be used to shut down the entire fleet."

*Loss of functionality of entire portfolio of products:* With the advent of re-use in both software and hardware, potential security flaws do not just affect a particular product line but could permeate a whole portfolio of products. As you design a new device in the portfolio—hopefully armed with all of this good advice from this article—keep in mind legacy devices that potentially could do things that the new design could not do, potentially even to the new device.

*Personal Information:* Personal information is a big deal today. Companies are mining our personal information for everything that it is worth. We need to think of any personal information (direct or indirect) in our devices as an asset to consider protecting. In terms of direct personal information—names,

addresses, phone numbers, social security numbers, age and so on—all may be of value to some malevolent hacker. But there may be indirect assets available for sale by those who would hack into your system. For example, a device with a GPS could be used for tracking the user if not protected. A smart meter that provides energy usage could be of use to those persistent telemarketers who are trying to get me to switch energy carriers. You get the idea. You have to take time to ask the question: "Is there personal information, direct or indirect, available in our device that needs to be protected?"

*Password, keys and certificates:* Certainly, assets that need to be protected are the passwords, keys and certificates used for signing and encrypting the data both used in transport and in storage. A couple weeks ago I was sitting in on a conference call and a company was considering having one set of symmetrical keys used for the life of the product across an entire fleet of more than 300,000 units spread across 3,000 locations. Those keys would require some pretty secure methods and mechanizations to protect throughout the 20-year lifetime of the product. Cooler heads prevailed thankfully. But how many keys are there, how often are they refreshed and how many devices are they used on, affects how much protection we need for the keys. For example, if the keys are different at each site, reverse engineering one box would only provide a security breach at that site. If the keys are refreshed each day, then reverse engineering one box would only give you access for one day to one site. This may not be pretty to think about but if the mechanism exists for refreshing a whole subnet of devices keys on a regular basis, why not use it?

*Wireless network:* Clearly, the wireless network, even though it doesn't belong to your organization, is an asset (**Figure 3**). Not all wireless carriers have the same requirements for what it takes to put your IoT device on their network. For example, one carrier puts a limit on the number of times you can put your device into and out of airplane mode. If your device were to violate the requirements of the wireless network provider they have the power to shut your device down and perhaps even the entire fleet until you fix whatever they consider wrong. A hacker could find out what causes your device to go in and out of airplane mode, do it on one device and cause the wireless carrier to shut down your entire fleet.

*Customer wired network:* Many of our devices hang off a customer's network. Typically, these networks are local but they could be wide area networks. This network

For detailed article references and additional resources go to:  
[www.circuitcellar.com/article-materials](http://www.circuitcellar.com/article-materials)

A link to Bob's IoT Checklist is available there.

must be considered an asset to be protected in the same way that the wireless network does.


## ASSIGNING RISK TO ASSETS

Finally, I want to briefly mention how we have assigned risk to these assets. It is both simple and complicated at the same time. It is simple because you just have to assign the cost to the company if you lose all or part of the asset. Then you assign the probability of losing the asset over the life of the product. Multiplying those two together will give you an idea of the risk. It will also help you convince your manager or in our case your customer that you need to invest in security measures to protect against these threats.

Here's the complicated side: What is the probability that a malevolent former employee steals one of your boxes out of the spare inventory and sells it to a hacker? The hacker reverse engineers the system and discovers the passwords to get into the device through the console port. There the hacker finds the one private key that unlocks the entire network. Once on the network, the hacker is able to break into your customer's customer network and shut down all 300,000 devices until you pay a ransom. Hopefully you

can see the complication. But that's why our managers pay us the big bucks. We make the best guess that we can and, so far, this method has worked for us.

To see our IoT Checklist, go to the *Circuit Cellar* article materials webpage. We will add to this with each new article in this series.

In my last article I closed with: "Security is complicated." But identifying the assets with a checklist is a start. Next time we will look at identifying the threats. But of course, only in thin slices. 

## ABOUT THE AUTHOR

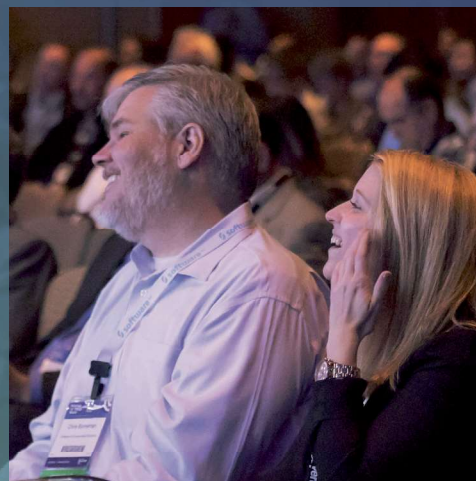
Bob Japenga has been designing embedded systems since 1973. In 1988, along with his best friend, he started MicroTools, which specializes in creating a variety of real-time embedded systems. MicroTools has a combined embedded systems experience base of more than 200 years. They love to tackle impossible problems together. Bob has been awarded 11 patents in many areas of embedded systems and motion control. You can reach him at [rjapenga@microtoolsinc.com](mailto:rjapenga@microtoolsinc.com).



# RISC-V Summit

December 3 - 6, 2018  
Santa Clara Convention Center  
CA, USA

**JOIN US AND LEARN  
HOW THE FREE AND OPEN  
RISC-V ARCHITECTURE  
IS REVOLUTIONIZING  
THE SILICON MARKET  
AND BEYOND**



## SPONSORED BY

Lead Sponsor

**Western Digital.**

Emerald Sponsor

**Microsemi**  
a Microchip company

Diamond Sponsors

**antmicro**

**NXP**

Silver Sponsor

**ultrasoc**

**REGISTER TO ATTEND:**

[tmt.knect365.com/risc-v-summit](http://tmt.knect365.com/risc-v-summit)

@risc\_v

**RISC-V**

Delivered by  
**KNect365**  
TMT  
an informa business