Issues with Embedded Device Disclosures:
Helping the Vendors and Recognizing the End-Users

Jerome Radcliffe, Director Security Threat Center for Mocana

The issue of vulnerability disclosure is not new. For well over twenty years we have been discovering problems in software and networks that can cause disruptions to personal and business computer systems. We have grown in dealing with these problems and companies have a wealth of experiences in the best way to handle problems associated with vulnerabilities. Now there are a new group of companies that, while well established in their primary industries, have little to no experience in dealing with vulnerabilities associated with computer systems. These companies produce devices that utilize embedded computing power. The issue of vulnerability disclosure is not new. For well over twenty years we have been discovering problems in software and networks that can cause disruptions to personal and business computer systems. We have grown in dealing with these problems and companies have a wealth of experiences in the best way to handle problems associated with vulnerabilities. Now there are a new group of companies that, while well established in their primary industries, have little to no experience in dealing with vulnerabilities associated with computer systems. These companies produce devices that utilize embedded processors with unique proprietary software. These devices are used seemingly everywhere in the world around us. They control the water that flows to your house, the natural gas used in industry, delivering oil from remote areas of the world, and keeping those that are ill alive, among other things. In addition to that, the market place is demanding more connectivity from all of their devices. Our new cars will e-mail us when it's time for an oil change, smart meters will contact us when there is an unexpected spike in energy usage, and out refrigerators will tweet when we are low on milk. The pressure to accommodate these demands means less testing and less time developing fully mature features. Security researchers are starting to look at these devices in a new light. The discovery of vulnerabilities in these connected devices will continue to rise, at a rapid pace.

Current Problems with Vulnerability Disclosure

The process of vulnerability disclosure is fraught with problems and difficult decisions. The debate over how much we disclose, to whom, and when will be endlessly debated. There is no single correct solution. Each vulnerability has a unique set of factors that need to be addressed when considering how to proceed. Companies also have many different directions they can take, each of them has advantages and consequences. Let's look at some examples:

- Company A has been notified by a researcher of a vulnerability in their product. Upon notification the legal department immediately takes over the situation and issues a strongly worded Cease and Desist letter to the researcher. They do this without consultation of the engineering group. The goal of the letter is to intimidate the researcher into not publically disclosing the information, or talking about the security of the product at all.

- Company B gets notified by a security researcher of a vulnerability in their product via email. They have no experience in dealing with security issues with their product, and are not sure what to do. The company makes a decision to not contact or acknowledge the researcher or vulnerability, even after the researcher has sent multiple emails. They are going to try and handle the issue internally with the small amount of information the researcher provided in the original email.
- Company C gets notified by a security researcher of a vulnerability in their product. The company does respond initially to the researcher, but is not sure who the researcher should talk to. Over the course of multiple months, the researcher gets directed to multiple people in the company, none of whom believe that they are the ones to deal with vulnerabilities. Quite often it takes weeks to get these individual responses.

There are several conflicting interests in the debate on the topic of vulnerability disclosure, but the primary one is the relationship between the public having knowledge of the vulnerability (so they can better prepare and protect themselves against those that can leverage the vulnerability) and limiting the number of people that know about the vulnerability (to prevent the risk of the vulnerability actually being used). There is no correct answer here. Usually it is going to be some kind of balance between the two.

How Security Researchers can Help

Intermediaries

Security researchers as individuals often might be confused on the process of how to contact a vendor about vulnerability found in a product. Especially if the researcher has limited experience. Conversely, companies might be reluctant to an unknown individual claiming to have found a vulnerability in one of their products. This is a situation where an intermediary should be brought in to work with both the company and the researcher. There are some well established groups such as US-CERT, ICS-CERT and as of late the US Department of Homeland Security. The use of a high profile intermediary lends credibility to the process and makes both parties feel more secure in exchanging information on the vulnerability.

Professionalism

This is an important issue that we are often reluctant to avoid talking about. The persona of our field is the “geek” in his mother’s basement. We speak in jargon, using obscure references to old Sci-Fi shows. This lends no credibility to our work, our field, or our ability to work with a company. Moving forward in the field this is an important aspect of the field that needs to grow up a little, and learn to show more professional aspects of ourselves. Imagine showing up to a professional workplace, everyone in buttons downs, slacks, loafs, and me in my DefCon 3 shirt and Chuck Taylors. I talk of being “31337” and “what garbage” their security systems are. It is unlikely that I will be hired.

Now, in this new, adult, version of our field I show up in my khakis, a polo (heck even a def con polo) and my nicest Chuck Taylors; and I speak in proper English of my experiences in the field, the

vulnerabilities of the field, but also how hard I they have worked with what they have and how I, the professional, can help them manage to improve their security. This is the direction we need to go. Shirts with collars, pants with no holes, and shoes that tie.

Respectful Discourse

One of the biggest turns offs, when walking in to a new company, is the "what were you thinking" talk. We have all been in that situation, where part of your mind is screaming at the last IT "professional" who set up their network, the hack who should never have been given access to anything with a keyboard, the person who set up this mess that you are now charged to fix. Rather than engage in the rant that is forming quickly in your mind, it is our job as professionals to calmly discuss the holes in their security, the tweaks that can make them safer, less vulnerable, and to offer suggestions of how to close the gap from where they are to where they need to be. It is also important, while making these suggestions, to take into consideration what is realistic for this company. In a perfect word, we rip down all the parts of the structure that get in the way of our ability to secure a device, a system, a network; we remove all the current technology that just does not meet the current standards for security from the market and out of the hands of the current users; we are free to tell them how "stupid" they were for setting up their technology to not accept upgrades. Instead, as professionals, we engage in a discourse that recognizes that the company cannot do many of these things, that every person has had short sided thinking in the past, and we offer real world, respectful, suggestions on how to fix these issues. This is what professionals do. This is what will gain us respect as a person, as a professional, and as a field.

How Companies can help

Plan Ahead

As a company in this field, you are going to make a mistake. Even the most trusted, most thoughtful, and most thorough companies make errors; they cannot visit every factory, they rush a product to market, or they did not find the bug that others had found. It is important that, as a company, you accept that someone else is going to find a mistake that you have made and that you plan ahead for the scenario, that you know how you and your people will respond, and that the plan includes some level of respect for your user and some amount of grace in how you deal with the issues presented to you. Below are some suggestions on how to set up a protocol for how to respond to vulnerability.

1. Use well tested processes
   Many embedded device companies shy away from using publically known and published standards in their equipment. This policy amounts to "security through obscurity". The thinking is that the less people know about how the device works, the less likely it is for a vulnerability to be found. This concept is quite often proven to not be reliable. The problem is that one or two developers that do not specialize in security can not create the same strength security methods as large groups of experts using peer reviewed methods. This is especially true in key exchange and encryption methods. Companies should try and use these widely used, peer reviewed methods when possible rather than trying to recreate the wheel.

2. Establish an IRT or Policy
   Security researchers often struggle with not only how to contact companies about vulnerabilities, but also what to expect from companies when they are faced with these vulnerability disclosures. Companies should create an Incident Response Team (IRT) or at a minimum a policy on who to contact and behaviors associated with vulnerability disclosures. This will not only save quite a bit of time for the researcher, but also set a foundation for expectations on the behavior of the company. For example, part of your policy might be a moratorium on public disclosure of the vulnerability for a set period of time.
3. Have a Plan
   Companies have pushed really hard in the past ten years to develop business continuity plans. These plans are used to keep the business operational in the event of unforeseen disasters and problems. Quite often this includes physical destruction of the building, natural disaster or other events that would significantly derail the standard operation of business. These plans are tested multiple times a year in order to make sure everyone knows their role in the plan, and how to act in the event the plan has to be put into action. The same thing should be done for vulnerability disclosure. There are many different groups that need to act in handling a disclosure: PR, Legal, Engineering, and Executives all have a role in the process. Having a plan and practicing it from time to time will help when the time comes to handling a vulerability
4. Make Friends with Researchers
   Often, companies have a negative association with security researchers. Typically they are stereotyped as "hackers" that are egotistical nerds that only care about destroying devices and doing damage. While this can be the case, it often is not. Professional security researchers are more concerned with learning how things function and making the world a safer place to live. They will usually happily talk to your engineers about how they discovered the problem, and usually have several ideas on how to fix it. Respecting them and having an open dialogue with them will be much more productive then shunning them.

Accepting Imperfection

There are situations that will require complete lack of public disclosure. This is a difficult truth for some researchers to accept. These devices we are looking at now control important components of our civilization. Take our water infrastructure for instance. There are multiple embedded devices in that control and monitor the water from the point of origin to the delivery point in your home or business. A significant security vulnerability in that system might impact the delivery of water to thousands if not millions of people. The impacts of an event of that scale cannot be quantified, but we can speculate that it would be disastrous. Due to the age of some of these systems, there might not be a realistic solution to the problem. In these cases it is more important to forgo public disclosure to limit not only the number of people that know of the issue, but to avoid public panic over the situation.