Security and the Internet of Things

featuring Art Manion as Interviewed by Will Hayes

Will Hayes: Welcome to the SEI's Podcast Series, a production of Carnegie Mellon University's Software Engineering Institute. The SEI is a federally funded research and development center housed at Carnegie Mellon University. A transcript of today's podcast is available on our website at sei.cmu.edu/podcasts.

My name is Will Hayes. I am a principal engineer in the Software Solutions Division here at the Software Engineering Institute. It is my privilege today to introduce my colleague, Art Manion, a senior vulnerability analyst in SEI's CERT division.

Today, we are going to talk about Art's research in the Internet of Things. Art, would you please introduce yourself?

Art Manion: My name is Art Manion. I work on the vulnerability analysis team, part of the CERT division. I have been at the SEI for 15 years. Vulnerabilities are generally some sort of software defect that has a security impact. This is the sort of thing we have been studying a lot in my part of the SEI.

In the last 5, 6, 7 years, there have been a lot more things, devices on the Internet…not your typical servers and workstation and laptops but cell phones, cars, toasters, airplanes. Many more things are connected these days. When I consider Internet of Things, I am thinking about all of these sorts of things. So, a lot more devices, a lot more software, a lot more vulnerabilities, a lot of newer devices that have not had the years of experience and the exposure to Internet security issues. That is the Internet of Things problem to start out with from my point of view.

Will: Why in particular for that kind of domain is security a concern?

Art: Again, for Internet of Things, a fairly broad definition, at least the way I look at it: home automation, toasters, your Nest thermostat, a crockpot. There is even a toilet, I think, that connects to the Internet, believe it or not, a home router, cell phones, there is a class of things there.

Our particular concern is safety devices, so devices that could have a physical impact if something goes wrong. Your car is a great example. We have been looking at cars a lot.

Medical devices, insulin pumps have received a lot of attention in the last two, three, four years. Airplanes have received some news, although not a lot of actual research that I am aware of that is come out with any actual findings. Of all of the Internet of Things things, we are particularly focused on sort of safety-critical systems.

Will: As a casual thinker on these kinds of topics, when we think about such devices, we don't tend to think of them as interacting on the Internet, we think of them, perhaps, as things you could get to from the Internet. They would have a more limited communication bandwidth, is that not the case?

Art: That is. We are seeing a lot of Bluetooth, Wi-Fi, some other types of shorter-range radio to get these things to be wireless and play together nicely and be very easy for the consumer. I think—this is our observation, we have not really proven this out yet, but we have a lot more devices. They are commodity things. The users are not experts. They are not sitting at a computer. They are not a server administrator who knows about security and what they are doing with their device. You have your Fitbit attached. Your toaster is connected to your Wi-Fi. Your refrigerator is connected to your Wi-Fi. Your car is telling you where to go and putting a map on the screen or something while you are driving.

There is the end user, and the consumer class of end user is not really thinking about the radios or the security or the computer parts. It is just all working. The issue though is, with a lot of new devices and a race to market, security is perhaps not being considered early enough in the process.

We are seeing classes of vulnerabilities that are not very difficult things to prevent. If you are doing some architectural review or some threat modeling up front, you would have caught these things. We are not seeing the very complicated vulnerabilities that we see in traditional computing these days.

Again, very new markets, race to market. I believe that race and a large number of devices is causing quick mass production and not enough consideration for security up front.

Will: Interesting. It seems there is an ecosystem for these things to live in. Perhaps something is previously outlandish as the Bluetooth connection in my car acts as a connection between my toaster and my refrigerator, propagating some vulnerabilities, is that a possibility now?

Art: Yes, I mean we have not looked at all of those sorts of connections really well yet. but it is possible. You pull in our driveway, your garage, your phone is active, your car is active, they are

talking on Bluetooth. Something talks to your house gateway, which tells your refrigerator something. There could be interesting worm or malware propagation that could go on there.

The angle we looked at really to date is a little bit different than that. It is more…I will pick on the car because that is what we have looked at a lot. The car is a safety-critical system, right? You need the brakes to work, the throttle, the steering, and all these things. What we are doing now is connecting the car to the Internet in a variety of ways. It might be Bluetooth via your phone. It might be a direct cellular modem, like OnStar, or something in the car.

The car is directly connected. The question is really, of all of the bad things happening on the Internet or an attacker trying to find cars, can they get to them over the Internet and do something that affects the safety system. There has been a handful of cases where that has been proven to be the case, proven to be possible.

Probably the most notable was last summer, there was a Fiat Chrysler automotive. A Jeep was hacked into while on the road. A *Wired* reporter was driving it, and they cut the engine I believe. That is concerning, and that is our immediate threat that we are trying to look at.

Will: You could certainly see how the manufacturers of these devices ought to be concerned and would be motivated, but the Department of Homeland Security (DHS) is really championing the work you are doing. Can you talk a little bit about why they are interested?

Art: Sure, DHS and NCCIC [National Cybersecurity and Communications Integration Center] and U.S. CERT are the areas we work with most closely, my team at least. They also recognize the proliferation of things connected to the Internet. They actually asked us to give a bit of guidance, do some review of all the things and classes of things and figure out maybe what the priorities would be.

It is a big, big set of devices to go after all at once. The results of that were an earlier paper, where we thought the safety-critical things were a priority. So cars, medical devices, aviation. There were a couple of difference variants of car. To my knowledge, I just called it cars, cars in general, automotive, vehicles.

There was the *Where do we apply our energy first?* We chose safety-critical sectors. And then [with respect to] vehicles, we have been working with the Department of Transportation [DOT] and DHS on some vehicle work. We actually had a car on loan via the DOT to look at in person. So again, review, pick an area to prioritize in, safety critical and cars is the path that we have taken. Not that there were other paths, but that is the one that was most approachable for us.

Will: Clearly, there are technological frontiers. There are discoveries that lead to advances in engineering. Are there policy implications that you are contributing to as well?

Art: There are. One of the things my team has been doing—and this goes back well past my 15 years to I think 1988—was the first CERT advisory. There is a policy process thing we call coordinated vulnerability disclosure.

The idea here in a nutshell is a security researcher finds a vulnerability or a bug in something and attempts to report it to the manufacturer or the vendor, talk to the vendor, develop a fix. Then, once the fix is ready, you tell the users and tell the world, publish what is happened. The idea is before publication, the manufacturer has a chance to address the vulnerability.

The theory is that is harm reducing as opposed to…If you do not tell the vendor, the vendor does not know. They never fix it. There is the potential to exploit that vulnerability that lasts forever potentially. If you disclose or publish immediately, there is no patch in place and customers are at risk sort of early on.

The middle ground is this coordinated disclosure process. We have been doing it since 1988, and that process definitely applies in the IoT space. There are probably some tweaks to the process that need to happen for safety-critical devices like vehicles or medical devices. Applying the same principle, and we are talking a lot in…Regulators, safety critical systems are often regulated industries, which is why we are talking to DOT about cars, for example.

There are policy considerations about how our research is conducted, how publication happens, how devices are tested, how devices are fixed, manufacturer requirements for testing and fixing devices. Those are getting a lot of attention now that it is been shown publicly that, for instance, it was possible, at least one point, to break into a car over the Internet and cut the engine. NHTSA [National Highway Traffic Safety Administration] and DOT are very concerned about that possibility.

Will: Clearly, the things you are learning and the new frontiers you are discovering in order for society as a whole to benefit from this knowledge, you have to manage the dissemination of that knowledge. You have to really strategically think about how to use it.

Are there other ways that working with DHS has helped you update your methodologies or focus your work?

Art: Well, another—and this is more of a process angle—another piece of it might be, I mentioned earlier architectural review or threat modeling. Again, the disclosure piece, the publishing piece, is what happens after a bug has been found. It is already shipped. It is already out in the world and distributed. *How do you clean up afterwards?*

Threat modeling is far on the other side of the development process. Considering I am going to plug a Bluetooth device into the diagnostics port in my car. I am going to build this device. Early

on, you might think *Well, how can someone connect to this device*? Of course you want the owner of the car, the user of the device, to connect to it with their phone or something. Did you think about how an attacker might connect?

And literally list – there is a Wi-Fi connection so if you are in Wi-Fi range, an attacker might connect. What stops them from connecting? The Wi-Fi password, WPA [Wi-Fi Protected Access], for instance. Is there an Internet connection? What stops an attacker from connecting? Bluetooth. What stops an attacker from connecting?

There are threat models. There are threat modeling systems that exist. There are several to choose from. We strongly, strongly recommend manufacturers of things look at threat modeling, as well as other development process security options that they have available to them.

Will: As you spoke of earlier, the pace associated with commercial market, this kind of thinking about things upstream and laying the foundation for making smart choices would seem to be a high-leverage opportunity for DHS or the SEI in general to participate.

Art: Yes, that is the plan. That is one of the approaches we are taking certainly. Again, that means more of a policy discussion or a discussion with regulators or industry groups from time to time. That is a little bit less technical and more on the policy side.

I am convinced at this point, we certainly have technical problems, but the problems to a lot of the security issues we deal with are absolutely not technical. They may include technical components, but they are going to be public policy issues. Regulation…you want to be careful about it. We have the classic speed of Internet problem, right? The Internet develops, laws and regulations follow behind by months or years, possibly decades.

By the time you update the policy or the regulation, the technology has changed six more times. The entire world is dealing with this problem. *How do you have public policy keep up with technology?* But we very much are playing that space to try to sort of these safety-critical devices.

Will: So we have seen a lot of great publications, some webinars from you and your group of late. Can you tell us some highlights of where you are in the research, and what is coming in your term?

Art: Yes, the car work, which I will, you know, focus on again. We have got some good engagement with DHS and DOT. We have looked at and published some results on devices that you plug into the diagnostic port. They may have Bluetooth or Wi-Fi or cellular connections. There is clearly some concerns there. There is some upcoming work. The terminology is vehicle-to-vehicle and vehicle-to-infrastructure.

The idea with a smarter or autonomous car might be that I am driving down a highway or an arterial road in a major city, and there are pylons or billboards or signage that they are communicating with my car and telling me, *Stop traffic at the Squirrel Hill Tunnel. Slow down now*, rerouting safety messages, things like that.

Cars talking to each other or infrastructure talking to cars. There is a whole system…again, you mentioned earlier, new radio connections, short distance, low-bandwidth radio, to convey all these messages. This is not in place yet, but it is under development. One of the questions is *Well, what if I can spoof one of those messages?* and tell you to slow down or give you false information. What is the threat model for that?

There is a PKI model that has been designed to protect the integrity of these communications and potentially privacy, but that is not in place yet. *There are questions as to Will that PKI model scale well?* You do not want to have a safety message slow down by a failed certificate check or something like that, for instance.

We are going to be looking into that, which will be our next piece of work that is coming up. We are going to continue the work into the telematics units, whether that is an attachable device or whether it is built into the car itself. Again, these are things that really communicate with the safety systems on one side and the big, bad, dangerous Internet on the other. Those gateways between the Internet and the safety systems are, we think, a good place to focus energy.

Will: Terrific, it sounds like you are really getting ahead of something that is moving at quite a rapid rate.

Art: It is a race to keep up.

Will: Well, thanks very much for your time today. I appreciate you coming in.

Art: Thanks for having me.

Will: Art, thank you very much for joining us today.

Art: Sure.

Will: A story highlighting this research is available in the SEI's 2015 Year in Review, available for download on our website. This podcast is available on the SEI website at sei.cmu.edu/podcasts. It is also available on Carnegie Mellon University's iTunes U site. As always, if you have any questions, please do not hesitate to reach out to us at info@sei.cmu.edu. Thank you for your attention.