173012511 © Blackboard373 | Dreamstime.com

ESTABLISHING TRUST IN CYBERSECURITY FOR EMBEDDED SYSTEMS

by **Alix Paultre**, Editor

Cybersecurity has become a serious issue in every aspect of electronics, from server farms to the smallest and least significant devices operating in the IoT. Even something as minor as an intelligent thermostat has been used as an attack vector in a hacking theft. Establishing a design's security protocols have become a major part of device development, evaluation, and qualification.

One of the companies operating in the Cybersecurity space is Sectigo, a provider of automated digital identity management and web security solutions, and

Grau

is a Certificate Authority offering a comprehensive website security solution, combined with TLS/SSL certificates, DevOps, IoT, and enterprise-grade PKI management. To get an overview on the situation facing designers today, we spent some time talking to Alan Grau, Vice President of IoT/Embedded Solutions .

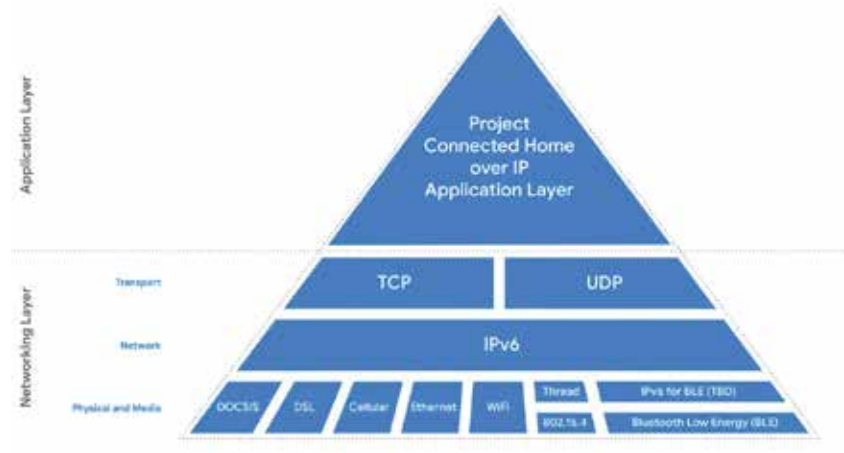
EE: **Implementing security is something that's done now before you turn the device on, and it's got to be done before the product goes on the shelf. Well, you used to be once upon a time, that's how you did security, but now you can't just buy a product, unbox it, turn it on and then implement security. You know what I mean?**

Alan Grau: In the embedded world, it's very different, right? All the software and firmware is baked into the device. Many of the devices don't h ave an ability to update the firmware on them at all. And if they do, firmware still has to come from the OEM or from a trusted partner of the OEM. So it's not an open platform, like a PC or a Mac, where anybody can write software for it. So for the PC world, users can go and install applications after the fact for security or for other reasons. So it's a different world in that regard. And so, you're absolutely right, it has to be baked in by the OEM.

EE: **Now, when looking at it from that point of view right now, addressing the fact that this has got to be done at the OEM level, how would you, at what point would you say, I need to start thinking about it? I'm making, let's pick a random application. I'm making a set of smart glasses that take pictures when I blink or something, it's got RF, that means I got to worry about my RF protocols. It's got storage, it's got a camera, all you typical IoT-type device issues. So at what point do I start thinking about security in a device like that?**

AG: Well, you should be starting at the beginning, right? You're saying, okay, we need to support RF on this. We need to support, whatever the different capabilities are on it. And security has to be on that list from day one or should be on that list from day one, so that you can make the right choice in terms of hardware platforms. Maybe you're going to look at it and say, well, do we want to use Bluetooth Low Energy for the protocol? Or do we want to use some other protocol? And as early on, is you can start thinking about that, you can start looking at the security ramifications of those choices. So, I think it's definitely, got to be done just from that very, very early point.

EE: **Now, are there issues when you start talking about security, we now have to worry also about hardware security**



and obviously not necessarily for a consumer level device, although if it's got camera and microphone in it, you might really have to start thinking about it. Things like Secure Boot and Chain of Trust and the like. Can you talk a little bit more about that?

AG: Yeah, absolutely. And those are some of the things you do need to think about earlier on or because you need to think about those features, they do need to be considered early on because they do have hardware ramifications. In my opinion, any device needs to have, you should have Secure Boot included in the capabilities. And so, that means having some hardware hooks so that you've got some ability to have some piece of code that's immutable on the device, or to have some Secure Boot artifacts on the device.

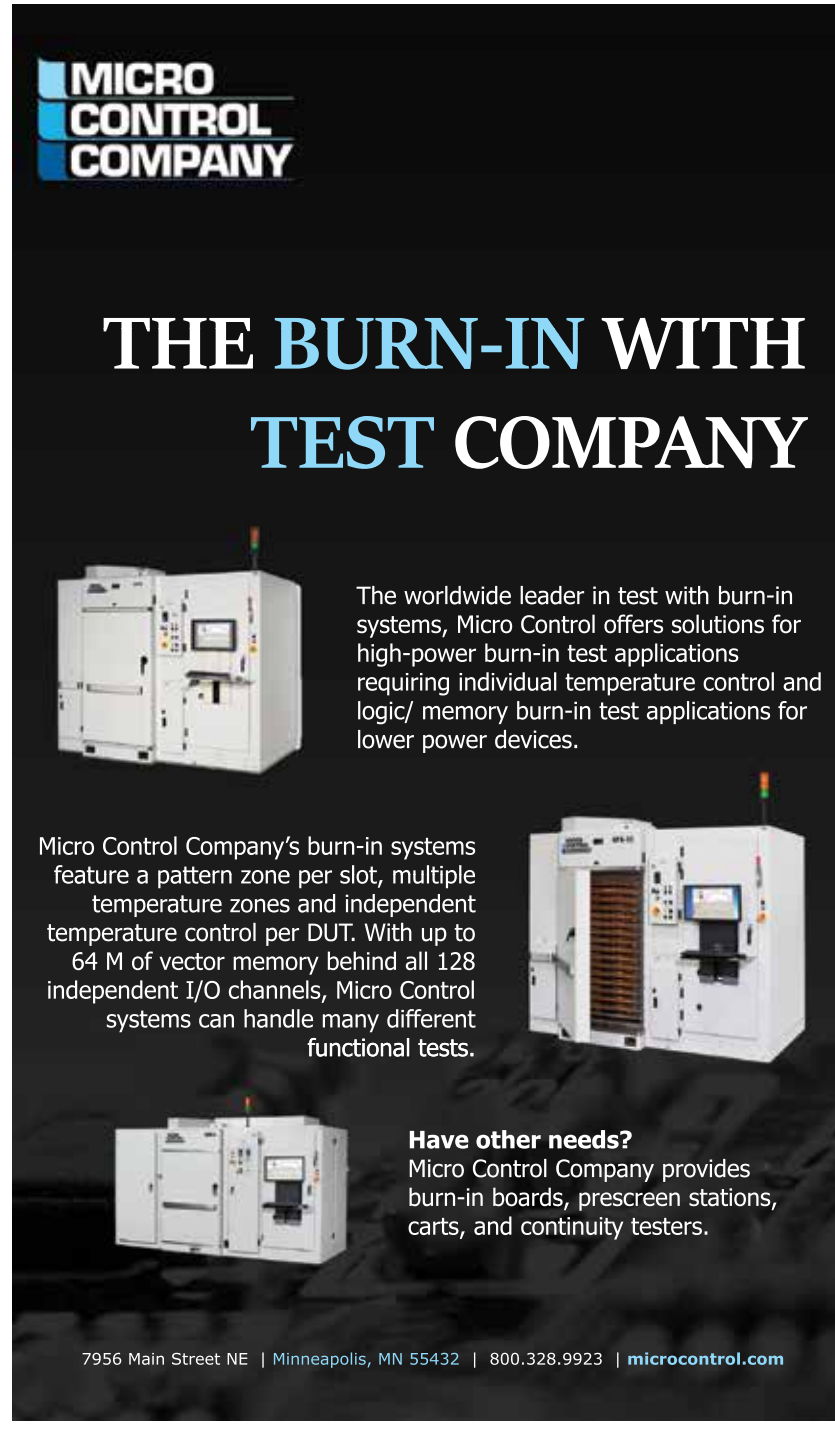
It is important that they are stored in a trusted place that cannot be modified or tampered with to ensure that you can get that initial kernel up and running in a way that you can verify that it hasn't been tampered with. And so, that means having maybe you have some boot code in ROM, then the signature and validation certificates for the rest of the code stored in a place that's immutable so that boot-ROM can validate the other code before it starts, before you start executing it. I mean, there's different ways to do that.

You could have a TPM chip or other hardware secure element in the device that enables Secure Boot and then having the software around it to enable it, as another approach that you can take. And so yeah, that has to be built in from the early stage of the hardware design. You can build Secure Boot in without some of those things, but without that root of trust, you've got a potential gap that hackers can exploit.

There are many different hardware options that you can look at. I mean, you've got things like Arm TrustZone, which is now available for their ARM's M-class MCUs. So it is available in some very low end systems. You also have your company's building hardware secure elements, like a TPM chip, but that are designed specifically for IoT use-cases. So that means they are lower cost than the TPM chip.

The TPM chip has maybe a dollar or two or something like that, which building a PC or a smartphone is a very reasonable cost to absorb. But if you're building a sensor, that's going to cost 50 cents, then obviously, that doesn't work anymore. So there are hardware devices or hardware chips built for that market, for that use-case.

***EE:* What are some of the challenges Alan, in implementing well, frankly, any type of a security solution, once I'm starting to work on it, I've got my device and okay, I'm going to be a Bluetooth chip and I'm going to do this. Are there any pitfalls I have to watch out for in selecting a security solution?**



▲ A Capt'n Crunch Whistle, made famous by John Thomas Draper, also known as Captain Crunch, an American computer programmer infamous for his past exploits as a phone hacking (phreak) pioneer. The tone from the whistle would fool the phone company's tone-driven switching system into allowing free long-distance calls.
© 1971markus

AG: Well, there's a lot of detailed ones, but at the high level, there's a couple categories that I would throw the challenges into. One is just the technical challenges. Building security is complicated and has to be done very, very carefully. Any little flaw can be discovered and exploited by hackers. And we've seen that. I mean, Cisco's got as deep of an engineering team as anybody, they've got tremendous resources and tremendous expertise, and they had a flaw in their Secure Boot implementation that some researchers discovered and found a way to exploit and it was a pretty difficult flaw to fix. It wasn't something that'd be easily updated with a simple software update.

So the technical challenges are significant. Hackers are very resourceful. They're really good at reverse engineering code and finding any little flaw and doing fuzz testing. And again, if you implemented one area great, and missed something else and left a flaw there, then they'll go exploit that. Right, they're really good at finding that low-hanging fruit.

So there's the technical challenges. And the approach there is don't try to do security all by yourself, right? Find people with expertise, leverage partners, leverage people who have expertise in security in the IoT space. The other two categories are the business challenge and regulatory challenges. The business challenge is just basically making sure that you've got the right resources allocated to solve the problem, making sure that, management has approved the budget that's necessary to really do the job right.

Sometimes it can be a significant budget, and sometimes it's not easy to get the additional budget for security approved. So there's that piece. And then the third one is, well, there's kind of regulatory. And what I mean by that is, what standards do you need to be worried about? Are there specific regulations you have to meet? Are there specific industry regulations you have to meet? What jurisdictions are you going to sell into?

So, you're kind of navigating different industry and legal standards and regulations, another challenge that has to be addressed, so if you're selling into California, and if you're building a device, California has passed some legislation saying that you have to have reasonable security. You can't have default passwords and hard-coded passwords and things like that. So at a minimum, you need to make sure that you've met that requirement. If you're in the medical space, you've got FDA cybersecurity guidelines that you have to follow. But the good news on this front is we are starting to see some organizations that are defining security requirements for different products in different markets and different solutions.

One example of that is a group called ioXt that is creating a validation process for specific products. They have defined security profiles for different products. So with that, there's a defined set of requirements and processes to kind of help provide some very good guidance for a company that is building a product. Another one that's emerging and that we're actually participating in is, something called Project CHIP, which is part of the ZigBee Alliance.

CHIP is Connected Home over IP. And what we've got there is Apple and Google and Amazon have come together, and they're trying to define their interoperability standards. So if you have some devices for each of the vendors, they'll easily work well together in the home, but in addition to it being an interoperability standard, they are looking very closely at the security. So they're going to have validation processes and testing houses as well, that will test security and interoperability in that context.

So, there are organizations that are starting to address the security challenges. It's not necessarily regulatory, it could be regulatory or standards compliance, and so it is, it's more standards compliance. But we need to have devices that have been approved by that group, which if it's successful, could really have a pretty broad reaching impact, because you do have the major players in the smart home market engaged. So it really could kind of turn the direction of the industry in that vertical market, towards building devices that are not just highly interoperable, but also have well thought-out security.

***EE:* Okay then. So now having mentioned a good partner, why don't you then tell us about your organization, a little bit of its history and where you insert yourself with value add in the stream?**

AG: Sectigo is a company that has a very, very long history in providing certificate of authority solutions or and services in the IT world. So it actually has its roots in the old Comodo CA business. It was spun out from Comodo as a standalone certificate authority company about three years ago, and rebranded as Sectigo. And one of the things that everyone in the business of issuing identities for websites, business applications, emails, has recognized, is that IoT is one of the new growth areas.

There's huge numbers of IoT devices coming online. Those devices need to have identities, or you need to be able to know for sure which one is which, that they're really authentic, and that each device is who they say they are. And PCI PKI and digital certificates are an important way of doing that. I joined Sectigo about a year and a half ago, when they acquired Icon Labs, the company that I had co-founded. And Icon Labs provides, and

developed a number of solutions for embedded security.

So software SDKs for building things like Secure Boot and embedded firewall, secure key storage into small footprints devices or other IoT devices. We can now use the PKI solutions from Sectigo to provide a well-rounded set of security solutions for IoT OEMs. Part of that is having a PKI hierarchy that spans multiple vendors. So we work with those consortiums to provide certificate solutions, PKI solutions, so that as different companies are producing products, they've all got the same PKI hierarchy. So they all can work together on the same network.

We also work with OEMs to build those same additional security solutions into the devices. We are able to provide certificate management solutions for IoT devices directly to OEMs, as well as them having capabilities like Secure Boot and better firewalls and so on. Again, working very closely with OEMs on this process.

EE: **That's pretty comprehensive. How would you end it? How would you close out a piece like this? What would you offer as advice to the audience?**

AG: Yeah so, like I said, we've covered a lot of different pieces. There's a lot out there. I mean, the one message that I repeat, and repeating for a long time as I talk to folks, is the importance, as we talked at the very beginning, about ensuring that security is a priority as a requirement in the early stages of the design. Don't wait until you're about to release the product or you're moving from a beta product to a final release product to start thinking about security. And because if you do, you're going to be trying to graft it in afterwards. And that's just much more challenging. It needs to be something that's looked at from the very early stages of design.

The other thing I was looking at, I would say is, if you're building a device, take a look around and see what the different standards and organizations are for your vertical market and, and see what's out there that you can leverage. Obviously, we talked about the new CHIPS Alliance, which has been formed in the last year or so in the smart home environment. So if you're building a device in smart home space, you need to look at Project CHIP and see what you can leverage from that.

There are other similar standards in the industrial space. So, you don't have to start from scratch, or you can look at the NIST requirements for IoT cybersecurity or their guidance for IoT cybersecurity and have a starting point. So there are different rules and legislation and industry standards that can be used as a starting point. EE

channels (DN2 80x