Embedded COMPUTING DESIGN

MAY/JUNE 2017
VOLUME 15 | 3
EMBEDDED-COMPUTING.COM

TRACKING TRENDS
Embedded systems engineers are dropping the ball in security!
PG 5

IoT INSIDER
EdgeX Foundry joins industry-wide push for IoT interoperability
PG 6

2017 TOP EMBEDDED INNOVATORS

PG 24

PRODUCT NOMINEES START ON PG 30

Embedded COMPUTING DESIGN 2017 INNOVATION AWARDS

OLIVER WINZENRIED
CEO AND FOUNDER
WIBU-SYSTEMS

KRISTIN RUSSELL
GLOBAL PRESIDENT
ARROW INTELLIGENT SYSTEMS

BILL MENSCH
CEO
THE WESTERN DESIGN CENTER

DEVELOPMENT KIT SELECTOR
Digi-Key ELECTRONICS
www.embedded-computing.com/designs/iot_dev_kits

Embedded COMPUTING DESIGN TOP INNOVATIVE PERSON

OLIVER WINZENRIED
CEO AND CO-FOUNDER, WIBU-SYSTEMS

Since co-founding Wibu-Systems in 1989, Oliver Winzenried has dedicated his career to securing embedded systems and applications, focusing primarily on software protection, licensing, and access control. With millions of devices now connecting to the Internet of Things (IoT) security has become paramount, requiring protection mechanisms that can scale from the smallest microcontroller-based (MCU-based) systems to cloud servers, as well as over time. A 2017 Embedded Computing Design Top Embedded Innovator, Winzenried offers perspective on the security "arms race," and introduces new (but old) methods of cryptography based on Kerckhoffs' principle that exponentially increase complexity for hackers.

There's no such thing as impenetrable security for connected systems, making the goal of the security professionals rather to make hacking a device so difficult that it isn't worth the time and effort. Where are we today in the arms race to secure embedded and IoT systems?

WINZENRIED: If you look at systems in the embedded and IoT space today, many of them are running without security at all. The first step towards making something secure is education and creating more awareness; making people aware that they must activate and use the security mechanisms already available in products. The second thing is that device manufacturers need to make security usable. If it's too complicated to implement a secure configuration, people will not activate it. Systems must be set up in a way that, out of the box, users are guided through a secure configuration process.

If you look back at Wi-Fi hotspots ten years ago, everyone was happy just to get the network configured and working. There was more or less no security then, but today when you set up a Wi-Fi network for the first time you are guided through a secure setup in which it's hard to disable all of the security mechanisms. There is a step-by-step process so that at the end you at least have a standard security configuration running.

Of course, there's never 100 percent security. Encryption algorithms will continue to increase in key length over time, but asymmetric and symmetric encryption mechanisms are only part of the overall security of a solution. In some cases, you don't even need to break the encryption on a device to compromise it. If you have physical access to a device and can tap into the CPU through a debug port, you don't need to break the encryption; you just wait until the encryption or decryption is finished and then access the plain code in RAM space. If you can debug, step by step, all possible parts of a program, you can successfully hack an application regardless of the encryption. It doesn't matter how good the encryption is.

With our Blurry Box cryptography mechanism one of the principles is duplicating code, such as a function that is inside an embedded device. If the function is important it can be duplicated five or ten times and then modified to deliver results based on certain input ranges. The original and duplicated functions are then encrypted, and duplicated functions containing input ranges that would never be used by the original application are marked as traps. By combining these mechanisms, someone who wants to hack a system really needs to be able to run through all possible parts of the program, and the application has been made so complex with so many different functions protected that at a certain point it's no longer worth the time required to hack it.

These three mechanisms of Blurry Box are publicly described, and we recently completed a Blurry Box hacking contest that was open to participants from all over the world. Participants were sent, free of charge, a secure element preloaded with a Windows application that included the published Blurry Box protection schemes. The contest ran from May 15th through the beginning of June, with a prize of €50,000 for anyone who was able to crack the security mechanisms. We haven't completed review of the submissions, and aren't claiming that the protections of the sample application are 100 percent secure – that's not possible. But, what our developers and scientists believe is that it is not possible to crack the Blurry Box protections within the allotted three-week period, even with all of the protection mechanisms publicly described. What we've done is really increase complexity so that it's very hard for attackers.

Of course adding protections such as those in Blurry Box, just as with longer cryptographic keys, requires more system resources. Are bigger processors and more memory an inevitable part of staying ahead of attackers?

WINZENRIED: To a certain extent, yes. Certain resources are going to be necessary.

The three mechanisms of Blurry Box mentioned previously of course cost more resources in program space. But, for example, in an embedded system based on a microcontroller (MCU) with 1 MB of flash, you would reasonably expect to use around 100 KB of memory for symmetric or asymmetric cryptography, leaving 900 KB for the application. If the actual application code space required is only 400 KB or 500 KB, the Blurry Box mechanisms described can certainly be achieved in an additional 300 KB.

Regardless, you should be able to implement sufficient protections for embedded devices within a reasonable footprint, particularly if external secure elements are used – for example, a dongle from Wibu-Systems, a trusted platform module (TPM), or a trusted execution environment (TEE) such as TrustZone from ARM or Intel Software Guard Extensions (Intel SGX) that is much more secure than running something in the normal user space of an embedded processor. Small systems such as a secure element or TEE that don't require very complex security operations, along with proven security algorithms, can still be enough for solid security. It will cost resources and performance to secure these systems, but it will be absolutely necessary that all connected devices have a minimum level of security so that the whole system runs reliably.

As noted, security is an arms race proportionately bound to computational power. However, many embedded systems are deployed long term. How will advances in cyber threats and defense impact the development of such systems moving forward?

WINZENRIED: Everybody assumes that the basic encryption algorithms – RSA, ECC, and symmetric AES – are secure. That is true today if you are using certain key lengths, but five or ten years into the future, they may no longer be valid. One reason is that computational power is increasing to the point that attackers may be able to perform brute force attacks on encryption algorithms with today's key lengths. Increasing the key lengths will help guard against this.

Another thing is that some encryption algorithms might not work anymore at all. For example, as soon as we have quantum cryptography with a certain amount of power, which IBM predicts will be available in about five years, then asymmetric encryption as it's used today with RSA or ECC can be broken independent of key length. This is an area where research into quantum cryptography is needed. Governments all over the world understand this.

If someone is developing devices that require security, they should plan to upgrade security mechanisms over the lifetime of the product, especially in industrial areas where machines can be in use for 15 to 20 years. It's not possible to implement a solution today that will be secure 20 years from now. ECD

Wibu-Systems AG
www.wibu.com

TWITTER
@WibuSystems

LINKEDIN
www.linkedin.com/company/wibu-systems-ag/

FACEBOOK
www.facebook.com/wibusystemsag

GOOGLE+
https://plus.google.com/116577147679495835957

YOU TUBE
www.youtube.com/user/WibuSystemsAG