←Rako Studios→

Security in microcontrollers

Security is an essential element in embedded hardware.

Microcomputers are used in electric meters. The chip measures electric usage and reports that usage back to the utility with a wireless connection. The micro-controller needs strong hardware security built in. An experience in my past demonstrates why.

I used to be a bad man. I used to be like Delmar in the movie "Oh Brother where art thou?" Like Delmar, I used to be a thief. Thirty five years ago I rented a house in Ann Arbor Michigan. I noticed that the electric meter was secured with a little lead tag squeezed onto a wire that looped through the meter retention ring. But over the years, the lead had corroded away and you could pull the wire out of the tag, and remove the ring that held the electric meter into the box. Well, I am an electrical engineer after all, and the temptation was too much. I yanked the glass meter from the box. On the back were four big copper prongs that plugged into the forked sockets inside the box. I was intrigued that the spacing of the four prongs was perfectly symmetrical. So, in the interest of science, I plugged the meter in upside down. It ran backwards. So began my career as a thief.

My housemates and I knew the day of the month when the meter reader came. So we would run the meter in normal mode for 20 days. Then we would flip it around and let it run backwards for 10 days, making sure we never ran the meter to a negative value from the last reading. Our 10-dollar electric bills delighted us for most of a year. Then we forgot to flip the meter back upright on the day the electric company read the meter. The very next day there was a big new strong ring with a very secure new lead tag, all properly crimped and unable to be tampered with. It was good while it lasted.

Note that we were not poor or downtrodden. I was an automotive engineer at Ford, and my housemates were a computer operator and a nurse. We did it because it was fun. We could have a party where we would run all the electric devices in the house and try and see how fast we could reduce the bill to nearly zero. The electric company was the man, and we were sticking it to da man. After all, Ann Arbor was a theme park for the 1960s, stuck in that narcissistic hippie mentality. The city council sponsored the annual Hash Bash. Frank Zappa made fun of them with the lyrics "Free is when you don't have to do nothing or pay for nothing, we want to be free, free as the wind."
We loved free electricity. Like all infantile people, we thought the world owed us free electricity. I have grown up and long since stopped living a life of crime. But there are a lot of brilliant basically honest people that still want free electricity. I have to admit, I do miss it a bit when I get a $300 PC&E bill.

Now it's 35 years later (well past the statute of limitations, I note) but there are plenty of people who will delight in stealing from you. If you design any type of embedded system or mesh network, you have to accept that there will be a lot of people that will try to subvert your design intent. Sometimes they don't even do it for free stuff. They will do it like I did, just for the sheer fun of it.

Security should move inside the microprocessor?

I got to talking about security with my consultant pal Dave Mathis. I asked if it was important to add security inside MPUs and MCUs. He told me a story. "The USB standard has a device class called DFU. That means device firmware update. The manufacturer's encrypt the firmware, since they don't want the public to understand too much about their device's hardware. That security is nearly unbreakable. But some cleaver hacker figured out that while the firmware update is secure, the USB driver has to decrypt it and send it over the USB cable. It is a trivial matter to snoop on the packets in the cable to get an un-encrypted version of the firmware. So Mathis noted "yeah, it is pretty important for us to move hardware encryption inside the processor chips."

Brian Hammel, a senior staff field applications engineer at Atmel® agrees, noting: "Crypto does not guarantee security" But having crypto-authentication can prevent similar exploits as Mathis describes. You can set lock bits, but a hacker can still replace the entire firmware code and have control of your systems. What authentication does is insure that the code in the MPU is your code, not some hacker's or electricity thief's. "Lock bits protect your software IP, but they don't make your system secure.

Hammel points out, "You can have a secure boot, where the firmware must pass authentication, but hackers can bypass that as well." The ideal solution is to have some hardware inside the micro that you can authenticate against. He points out the chip used in Atmel's smart metering applications has just such hardware.

Atmel microprocessors with internal security Embedded into the ARM® ARM926EJ-S -based SAM9CN12 are on-chip hardware accelerators with DMA support that enable high-speed data encryption and authentication of the transferred data or the application itself. The chips support standards like 256-bit AES, SHA1 and SHA256. The IC contains a true random number generator for key generation and exchange protocols. There are fuse bits for crypto key (SAM9CN12), and device configuration. No one can take over your product with malware since the parts have a Secured Boot ROM.

Atmel external security chips

If you don't want to limit your choice of MCU, you can always use one of Atmel's external security chips. Atmel offers both symmetric- and asymmetric-key algorithm-based devices. The Atmel CryptoAuthentication™ family offers you inexpensive hardware authentication capability. The parts have hardware security fortifications like full active metal shields, multiple tamper detection schemes, internal encryption, and many other features designed to thwart the most determined attacks.
Every Atmel CryptoAuthentication device contains a pre-programmed serial number that is guaranteed unique. The devices also include secure storage. Each device features a high-quality hardware random number generator. The ICs support many common serial interfaces and come in a variety of packages.

Protect yourself from bad men

Immutability and un-alterability are vital to secure systems and these chips do both. Remember there are lots of folks out there that might break into your system just to show they can. Celebrity hacker Barnaby Jack hacked cash machines live on stage in Las Vega. He went on to show how he could command implanted insulin pumps to deliver a lethal dose of medicinal. We can argue if he was a bad man or a white-hat hacker. But there are millions of potential bad people out there and both internal and external security can make sure people are not hacking into your products.

Tailpiece

.

files