ARTICLE

The “Three-Legged Stool” of Cryptography

February 15, 2016

By Dan Ujvari, Senior Field Applications Engineer

A Cryptographic Trilogy – a Three-Legged Stool Analogy

Implementing true security in IoT devices requires a three pronged approach. Like a three-legged stool, all three legs are needed to achieve security. At least two of these “legs” demand a hardware security approach. The three legs are comprised of:

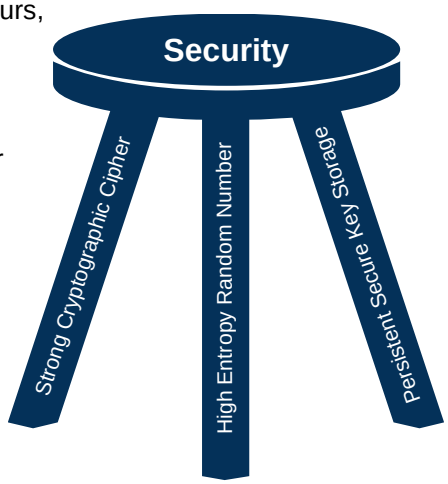
- A Strong Cryptographic Cipher for the Job
- High Entropy, Cryptographically Secure, Random Number Generator (Crypto RNG)
- Persistent Secure Key Storage with Active Tamper Detection

A Strong Cryptographic Cipher for the Job

A cipher is a cryptographic algorithm for performing encryption/decryption, authentication, key management, or other security purposes. It needs to be strong enough for the application. A one-time pad is considered the only unbreakable cipher, so theoretically, all other ciphers can eventually be broken. Time and cost are the two usual measures of breaking any cipher.

Time

The cover time of a secret is the amount of time the message needs to be kept secret. A tactical secret, such as a command to fire a particular missile at a particular target has a cover time from the moment the commander sends the message to the moment the missile strikes the target. There isn’t much value in the secret after that. If an algorithm is known to be breakable within a few hours, even that algorithm provides enough cover time for the missile firing scenario.



On the other hand, if the communication is the long term strategy of the entire war, this has a cover time significantly longer and a much stronger cipher would be required.

Cost

Generally, the time it takes to break any cipher is directly related to the computation power of the attackers system and the mathematical skills of your adversary. This usually relates directly to cost, so the value of your secret will in a large part determine how much effort is put into breaking your cryptography. Therefore, you want to select a cipher

which is well known to be strong, has been open to both academia and the public, and survived their scrutiny. Vigorously avoid proprietary algorithms claiming to be strong. The only thing which can speak to a cipher's strength is for it to be fully open to scrutiny.

These types of proven ciphers are available within the Atmel® line of microcontrollers and microprocessors and the Atmel CryptoAuthentication™ devices.

Importance of a High Entropy, Crypto RNG

The importance of a high quality RNG cannot be overstated. Some examples which rely on the randomness of the random number are:

- Key stream in one-time pads
- Private keys in asymmetric algorithms like RSA and ECC
- Initialization vectors for cipher modes
- Anti-replay nonces in virtually all secure network protocols

Any modern cipher regardless of intrinsic strength is only as strong as the random number generator used. Lack of adequate entropy in the random number significantly reduces the computational energy needed for attacks. Cryptographically secure random number generators are important in every phase of public key cryptography.

To realize a cryptographically secure random number generator, a high quality deterministic random number generator and a high entropy source(s) are employed. The resulting generator needs to produce numbers statistically independent of each other. The output needs to survive the next bit test, which tests the possibility to predict the next bit of any sequence generated, while knowing all prior numbers generated, with a probability of success not significantly greater than 0.5. This is no trivial task for randomly generated numbers as large as 2^{256}.

It is incredibly hard to create a Crypto RNG. Even if you had the processing firmware right, there is typically not enough entropy sources in an embedded system to create a cryptographically secure random number generator. Most embedded systems, especially IoT nodes are, well… boring. At least when considered in the context of entropy. 2^{256} is a larger number than the number of all the stars in the entire universe. How much entropy do you really think exists in your battery powered sensor?

Companies serious about security put a lot of effort into their Crypto RNGs and have their generators validated by the National Institute of Standards and Technology (NIST), the government body overseeing cryptographic standards in the US and Canada.

Any assurance or statements that a RNG is "compliant" or "meets standards" and is not validated by NIST is unacceptable within the cryptographic community. A Random Number Generator is either on NIST's RNG Validation List or it isn't.

Atmel is just such a serious company. The Crypto RNG Atmel used in its Atmel CryptoAuthentication devices is validated by NIST and is listed on their publically available listing: http://csrc.nist.gov/groups/STM/cavp/documents/rng/rngval.html

Persistent Secure Key Storage with Active Tamper Detection

Strong ciphers supported with high entropy random keys and nonces are used to keep adversaries away from our secrets, but their value is zero if an adversary can easily obtain the keys used to authenticate and encrypt.

System security is heavily dependent on the confidentiality of the keys. Protection and safeguarding of these keys is critically important to any cryptographic system. Your secret/private keys are, by far, the most rewarding prize to any adversary.

If your keys are compromised, an adversary will have access to every secret message you send, like a flower offering its nectar to a honeybee. To add insult to injury, nobody will inform you the keys have been compromised. You will go on sending “secret” messages, blissfully unaware your adversaries can read them at their leisure; completely unhindered.

A very well respected manager in our crypto business unit puts it this way; Keys need to be protected behind “guns, guards, and dogs.”

Holding cryptographic keys in software or firmware is akin to placing your house key under the front mat, or above the door, or in that one flowerpot nobody will ever think of looking in.

Adversaries will unleash a myriad of attacks on your system in an effort to obtain your keys. If they can get their hands on your equipment, as is often the case with IoT devices, they will rip them apart. They will employ environmental attacks such as extreme temperature, voltage or clock rates, or power consumption analysis. They will decapsulate and probe the die of your microcontrollers to disable JTAG locks or other protections. There is no limit to what they can and will do.

The Atmel line of CryptoAuthentication devices offers a long list of active defenses to these attacks, as well as providing an external tamper detect capability you can use to secure your devices from physical intrusion and warranty violation.

Summary

As stated in this brief of the three elements which enable truly secure systems, poor protection of the keys and low entropy random numbers will compromise any security system, no matter the algorithm or protocol used.

Inadequate entropy in a random number generator compromises every aspect of cryptography because it is relied upon from the generation of keys to supplying initialization vectors for cipher modes to generating anti-replay nonces in the messaging protocol. The Atmel hardware CryptoAuthentication devices ensure you have a NIST validated cryptographically secure random number generator.

Keys, signatures, and certificates require a persistent secure vault to protect them. The very elements which ensure the authority, security and integrity of your system cannot be left in the attackable open.

Keys held in software or firmware are easily recovered. Typical microcontrollers and microprocessors do not contain the protections needed to keep out adversaries. Even newer processors with secure zones have very limited key storage and are not designed to prevent aggressive attacks on the keys stored in the devices. From software protocol attacks to environmental and hardware probing, the ways and means of an adversary to recover keys from your software/firmware are nearly unlimited. This is akin to hanging your house key in a flimsy silk pouch on your front door knob.

Hardware security devices offer a number of benefits which include:

- Secure storage of private keys in the key hierarchy.
- Stop adversaries from hacking your code.
- Secure boot and program image checking to prevent execution of unauthorized code
- Read-only storage of digital signatures and certificates to prevent root store attacks
- Stop unscrupulous contract manufacturers from over building your product.
- Create new revenue streams by allowing premium services to be purchased post deployment
- Limit the life of products, such as the number of squirts an ink cartridge has, thereby thwarting refill/reuse.
- Streamline deployed product tracking and warranty services.

With regards to creating a truly secure system, active hardware protection for keys and cryptographically secure random numbers are not an option. They are a necessity. The Atmel CryptoAuthentication devices offer a high security, tamper resistant, physical environment within which to store and use keys for digital signatures, key generation/exchange/management, and perform authentication.

Atmel is very serious about security. In addition to testing, validations, and approvals by certifying entities, Atmel employs third party labs to apply the very latest attacks and intrusion methodologies to the devices. Atmel devices are extremely resilient. The methodologies and results of these tests are available to customers under non-disclosure agreement. Please visit the Atmel Security ICs webpages for more information, www.atmel.com/products/security-ics/default.aspx.

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | **www.atmel.com**