Protect the key – or don't bother encrypting your data

August 19, 2019

Brad Beutlich I Vice President Sales Western Region and LATAM

Encryption has seen quite the evolution. The technology, which can be traced back to BC Mesopotamia, is on the cusp of entering into a quantum era. The one constant? While encryption solutions will change with time, the importance of protecting the key will never change. In fact, the more effective the encryption technology, the more the key needs protecting.

Throughout history, one side in a conflict would encrypt their messages and the other side would employ people who would try to either break the encryption or steal the key. Nothing is different today. Except today, because of the strength of our encryption technologies, the other side doesn't even try to break the encryption. Rather, they steal the key by any means possible.

All of us have seen the movies where the bad guy puts a gun to the head of the good guy and says something like "decrypt the data or you'll eat a bullet." Following a feverish and typically nonsensical typing on a keyboard, the encryption is broken and the good guy (covered in sweat) pushes back from the table and says he's done it.

Hollywood doesn't do us security folks any service with this fiction. With our existing computing power, the time required to decrypt data protected by a 256 Bit AES encryption key is measured in millions of years. This is why no one tries to "brute force" attack an encryption key. As we attempt the transition to quantum encryption, this statement will be even more true.

If you've been wise enough to assume that your perimeter will be breached and you are enlightened enough to assume your uninvited hacker guest will try to steal your data and you're smart enough to encrypt the data…you still can't rest on your laurels. Based on a number of studies, the time between a hacker's penetration and detection is between 160 and 260 days. Even at the low end, that's a long time for a hacker to find your keys if you've stored them in software.

Since most hackers aren't your regular 8 am to 5 pm crowd and sometimes work in teams, those 160 days might end up being thousands of hours if the hacker is working with his buds. How hard is it to find an encryption key that's stored in software? Unfortunately for you, not very hard. Cryptographic keys use something called a Random Number Generator in their creation. As such, the resulting key, as you expect, is itself quite random.

ENTRUST

A crypto key represented in a binary data scan will look very much like ‘snow’ in that it has a varied pattern. All a hacker has to do is search through data using a relatively unsophisticated program that looks for randomness in a binary data scan. Once the random data is found, it’s highly likely it will be some type of crypto key. Seeing that a company may have a few thousand crypto keys, it doesn’t take long to try these keys against the encrypted data. To put this into perspective, a 256 Bit AES key has 1.15×1077 possible combinations. That’s 115 with 75 zeros behind it. This is a truly unfathomable number of combinations. Even if a hacker finds a few thousands keys, it won’t take them 160 days to try each of them on the encrypted data in order to unlock the data. Trying four keys per minute, a single hacker, in a 16-hour period could test over 3,840 keys. In 160 days, that’s over 614,000 keys.

To illustrate this another way; Most people lock the doors of their houses. Most houses have breakable glass windows within a few feet of the door. Smart burglars don’t like to make noise so breaking glass isn’t the best option. A burglar, however, will always check under the mat for an extra key. Storing keys in software is the physical world equivalent of leaving your front door keys under your doormat.

Entrust Hardware Security Modules (or HSMs to those in the know) are specifically designed to stop a hacker from finding crypto keys. An HSM takes the keys from ‘under the mat’ and puts them into a secure location that a hacker cannot see. If you’ve encrypted your data, the hacker will immediately go on their secondary search for those random bits of data. They cannot see the HSM and therefore they cannot see where the keys are stored. An HSM is designed using strict standards imposed by the National Institute of Standards and Technology (NIST). The protection of software stored keys aren’t certified by anyone.

The process of encryption has been around for thousands of years and there’s every indication that encryption will become even more important in the future. From a security perspective, the encryption process is important – but the security of the key is paramount. If you’re going through the trouble of encrypting your data or any other solution that requires a cryptographic component, you must make an equal effort to protect those keys. Otherwise, you’re in for a rude awakening.

Visit us at https://www.entrust.com/digital-security/hsm to learn more about Entrust’s products.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com