CIA and TPM to secure the IoT?

GUENTHER FISCHER, WIBU AND THE TRUSTED COMPUTING GROUP

0 Comments - **Leave a Comment**

CIA, TPM and IoT: You might ask what these three acronyms have in common and how they relate to each other. To make a long story short, it is all about security, trust, and reliability.

The abbreviation CIA in this context does not mean the Central Intelligence Agency. It is an abbreviation for Confidentiality, Integrity, and Authenticity. The so-called CIA principle is a simple, but widely used, security model covering three key tenets that should be guaranteed by all secure systems.

Confidentiality is intended in the sense of hiding information from people not authorized to view it. It is perhaps the most obvious aspect of the CIA model when it comes to security. At the same time, it is also the one most under attack. Cryptographic symmetric and asymmetric encryption methods are examples of means to ensure confidentiality when transmitting data from one computer system to another.
Integrity, on the other hand, represents the certainty that data is accurate and not changed on its journey from the original sender to the intended receiver. A common security attack, often called a man-in-the-middle attack, intercepts data and makes changes to it, before passing it on to the intended receiver. Cryptographic digital signature methods are one way to attest the integrity of code and data.
In addition, authenticity is needed to address the concern about genuine information. In other words, you want to make sure the information you receive actually comes from the source that claims to be its genuine origin. Cryptographic digital certificates are used to prove the authenticity of the issuer.

Now that we understand why CIA is important for a secure system, let's move to the third acronym: IoT.

After many years of being an overhyped marketing term, the so-called Internet of Things (IoT) is starting to become mature and real. Mark Weiser created the term "ubiquitous computing" first in his famous

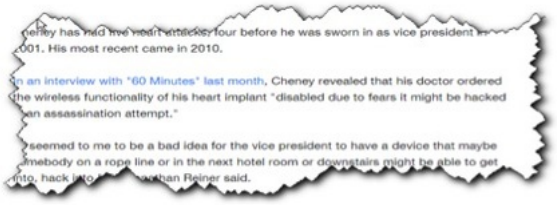
Scientific American article “The Computer for the 21st Century”, published September 1991. His thinking was so ahead of his time that it seemed like science fiction to most of his readers. In 2016, his vision has become reality. Ubiquitous computing (or ubicomp for short) became today’s – perhaps overhyped – IoT.

Weiser started his article, “The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.” He predicted that computing devices would become commonplace and part of all aspects of life, and he was right. Just consider, for example, the consumer gadgets like fitness bands, smart watches, smart phones, or navigation systems that send and receive data all day long. Or, consider the home, which is connected to a power grid where a smart meter allows the energy provider to effectively calculate the resources needed to cover the demand of all households. Interconnected computing devices are everywhere nowadays.

Shifting focus to industrial applications, today’s business IoT applications are developed together, with devices and services coming from various sectors of industry: information technology, automation, and production technology, aerospace, maritime, and naval systems, railways, car manufacturers and their suppliers, energy providers, agricultural, medical technology, and building automation. All of those share characteristics, including long life in the field: reliability and robustness in harsh environments and reliable, long-term availability.

IoT systems rely on public networks, but public networks are not secure environments. While IoT creates new capabilities and services, allows greater efficiencies, increases flexibility, and enables the customization of single production units, it also opens up previously closed systems and allows attackers to get access to those systems from the outside world.

Attackers often use reverse engineering techniques to identify software vulnerabilities, which they can exploit to create counterfeit products, steal sensitive data, or tamper with the device for sabotage and espionage purposes. This can lead to serious and dangerous hacks, as recent attacks on safety-critical automotive, aerospace, and medical components have shown.

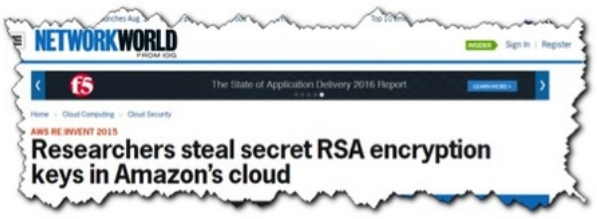


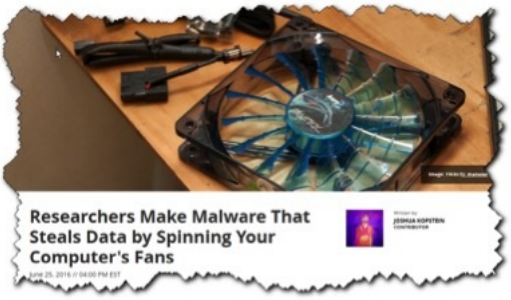
This brings us back to the CIA principle we started with. The only way to avoid situations like those listed above is to apply the CIA security model to the world of IoT devices. As we have learned, CIA is built around cryprograhic operations. Today's modern cryprography leverages standard crypto protocols. The Dutch cryptographer Auguste Kerckhoffs stated a maxim in the 19th century that would become known as Kerckhoffs' principle: A cryptosystem should be secure even if everything about the system, except for the key, is public knowledge.

I repeat, everything is public knowledge except for the key, which is needed to encrypt and decrypt the content, either directly or in a derived form. So, how do you store a key in a secure manner? This brings me to the second acronym: TPM, the Trusted Platform Module.

In the world of cryptography, there is a ton of other acronyms referring to the various protocols and methods that are used to ensure the CIA principle. To name just a few of them, you have DES, AES for symmetric cryptography and RSA, ECC for asymmetric cryptography. The list of acronyms goes on and on. The really important part, however, is that the algorithms themselves are typically not secret; they are publicly available, just as Kerckhoffs' principle demands it. The only part that really needs to be kept secret is the key itself. This sounds simple, but it is pretty hard to achieve. To keep the key secret, you need a secure place like a safe, which we will call a secure element, to securely store the key. A TPM (Trusted Platform Module) is such a secure element, and it offers a lot more, including the crypto protocols.

In a nutshell, a TPM is a specialized and dedicated device that offers crypto operations and secure storage for secret keys, all in one. This allows you to store the key in a secure place and, even more importantly, it allows the key to stay there, so it never leaves its secure location. All important crypto operations are done inside of the TPM itself, and only the results are exposed. This prevents the key from getting compromised. In case you want to know why it is important to have this dedicated functionality separated in a dedicated device, I recommend you to read the following two articles. These should make it obvious how important it is to have a dedicated, secure element like a TPM inside a computing device to make it secure, trustable, and reliable.





So how can incidents like these be prevented? Use technology that creates secured code and licenses that can be bound to a secure element in the target system, ensuring that the code and the licensed features can only be used on an individual system. License creation and deployment can be integrated into existing business processes, such as ERP systems or e-commerce platforms. This mechanism opens up new business models, such as feature-on-demand upselling and time-based or pay-per-use licenses for the IoT and other intelligent devices. The result is improved security from attacks, malware, theft, and other malfeasance for code and IP.

Guenther Fischer is a Senior Licensing and Protection Consultant at Wibu-Systems. His specialty is cybersecurity applied to the IoT world.

Wibu-Systems AG www.wibu.cm LinkedIn: www.linkedin.com/company/wibu-systems-ag Twitter: @WibuSystems YouTube: www.youtube.com/user/WibuSystemsAG Email: guenther.fischer@wibu.com

THIS ARTICLE WAS PUBLISHED ON JULY 11th, 2016.

#information technology #cybersecurity #cryptography #smart meter #IoT #tpm