University Of Agder

DAT 211

Networking and Security

Hardware based encryption devices

Author:
Bendik Egenes Dyrli

Supervisor:
Sigurd Kristian Brinch

2015

Introduction

Security in a company is a crucial thing, and by setting up policies, like to encrypt all the data on laptops thats setup to be used either at home or while traveling is something many business does now days, to ensure the security of their customers and the company itself. To be absolutely confident that the laptops are secure, there are chips on the motherboards which are used to store the cryptographic keys that are generated, there also appears to be a hardware module which is network based which also can be used to save cryptographic keys with and also used for PKI's[1]. In this essay we'll try to understand a little bit better how the keys are stored, and that they are not easily accessible for others which could potentially steal the keys for use to decrypt sensitive information.

TPM - (Trusted Platform Module)

TPM is a Computer chip , which can be used to securely store cryptographic keys, that is used to authenticate your PC. This type of chip is only found integrated on the motherboard itself, so if you don't have a TPM chip in your laptop or PC there is no really easy way of getting one, except for either getting a motherboard that have one already integrated or get a new laptop that has one. By having one of these chips you can store things like passwords, certificates or encryption keys. [1] But in 2010 there is this Black Hat hacker Christopher Tarnovsky, who managed to reverse-engineer the TPM chip first by making the chip going through different kinds of acid bath, so he could expose the chips cores. Then he could use a very tiny needle to wiretap the communication channel and then eavesdrop on all the communication which was sent back and forward by the programming instructions and the computer memory (RAM). This meant that he had made his own kind of way into the VIP-area of the TPM chip, he could by then see the data unencrypted this was because he was physically inside the chip. Tarnovsky spent over six months developing this "hack". But the makers of the TPM chip *Trusted Computing Group*, called the attack "exceedingly difficult to replicate in a real-world environment." as written in the article i'm referring to. [2]

[1] public key infrastructure

HSM - (Hardware Security Module)

HSM is more or less the same as the TPM only this is a kind of "removable device" it's a hardware that can be inserted into a server or a PC. This however means that it can only provide a limited functionality of the cryptographic functions, and these are encrypting, decrypting, generating keys and hashing. [3]

Conclusion

By diving into the world of chips that saves cryptographic keys, we've seen that here that if a potentially thief/hacker was to steal a laptop from a guy that works at 'x' corporate. That it wouldn't be possible for them to safely export the cryptographic, without having some kind of hardware experience. Though by the time they might have extracted data from example a TPM chip.. that might have been changed, so then again it's then useless. i Think the main target for the black hat hacker, was to show that even though it's a integrated chip on the motherboard that it is capable of being hacked, though this requires skill and most of all patience.

References

[1] "Trusted Computing Group - Trusted Platform Module (TPM) Summary", Trustedcomputinggroup.org [Online].
Available: http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary.
[Accessed: 10- Mar- 2016]

[2] "Supergeek pulls off 'near impossible' crypto chip hack - NZ Herald News", The New Zealand Herald, 2016. [Online].
Available: $http://www.nzherald.co.nz/technology/news/article.cfm?c_id = 5objectid = 10625082.$
$[Accessed : 12 - Mar - 2016]$

[3] Sans.org, [Online]
Available: http://www.sans.org/reading-room/whitepapers/vpns/overview-hardware-security-modules-757.
[Accessed: 13- Mar- 2016]