Segurança de Sistemas e Informação
(SEGSI)
PL05
*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**)*
{@isep.ipp.pt}

Exercise 1: Linux Disk Encryption

Hard Drive Encryption serves many purposes. The biggest advantage is to deter thieves from physically stealing your computer and extracting all data that lies in it. It also prevents malicious actors from implanting malicious files to elevate their privileges.

1. Understand what is LUKS [1] [2], [3].
2. In a Virtual Machine, use a Linux Live ISO and try to mount your existing Hard Drive. Where are you able to do it?
3. In a Virtual Machine, take a snapshot and encrypt all your hard drives.
4. Try to mount the Hard drive in the Live ISO. Where are you now able to do it?
5. Are you able to use any other forms of keys, for instance, TPM, YubyKeys, or Fingerprint together with LUKS?

Exercise 2: Windows Bitlocker

Windows also provides a subsystem to handle all storage encryption, BitLocker. This subsystem integrates well with TPM devices and protects user data from being stolen.

1. Understand what a TPM device is [4].
2. What happens if a Bitlocker encrypted device loses connection to TPM? Are you able to recover from such an error?
3. What are the typical attacks on BitLocker encryption? [5]
4. Why does Bitlocker prevent attacks such as KonBoot? [6].
5. Given the image available in Moodle how can you extract and crack the encryption of it? [7]
6. How can DMA [8] or SecureBoot [9] attacks compromise data encryption?

References

[1] "Linux hard disk encryption with luks." [Online]. Available: https://www.cyberciti.biz/security/howto-linux-hard-disk-encryption-with-luks-cryptsetup-command/

[2] RedHat, "Chapter 11 encrypting block devices using luks red hat enterprise linux 8." [Online]. Available: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/encrypting-block-devices-using-luks_security-hardening

[3] "dm-crypt/encrypting an entire system - archwiki." [Online]. Available: https://wiki.archlinux.org/title/dm-crypt/Encrypting_an_entire_system

[4] Microsoft, "Microsoft tpm." [Online]. Available: https://support.microsoft.com/pt-pt/topic/o-que-%C3%A9-o-tpm-705f241d-025d-4470-80c5-4feeb24fa1ee

[5] "Bitlocker." [Online]. Available: https://www.sstic.org/media/SSTIC2011/SSTIC-actes/bitlocker/SSTIC2011-Article-bitlocker-bordes.pdf

[6] K. Boot, "Kon boot - best tool for forgotten windows password and macos passwords (kon-boot)." [Online]. Available: https://kon-boot.com/

[7] E-Ago, "E-ago/bitcracker: Bitcracker is the first open source password cracking tool for memory units encrypted with bitlocker." [Online]. Available: https://github.com/e-ago/bitcracker

[8] J.-C. Delaunay, R. Matasse, A. Peter, and K. Denis, "Practical dma attack on windows 10." [Online]. Available: https://www.synacktiv.com/en/publications/practical-dma-attack-on-windows-10.html

[9] "Bios and secure boot attacks uncovered." [Online]. Available: https://cis.temple.edu/~qzeng/cis4360-spring17/slides/21-secured-system-boot.pdf