Argon2 security margin for disk encryption passwords

by Vojtěch Polášek <410266@mail.muni.cz>
Department of Computer Systems and Communications, Faculty of Informatics, Masaryk University
Advisor Ing. Milan Brož, Ph.D.
Spring 2019 Awarded with special prize by the dean of the Faculty of Informatics

Abstract

Passwords are a popular authentication method in the field of information technology. Passwords were created for humans to be remembered. Sometimes they are not ideal for usage in encryption software. Therefore, there exist key derivation functions, which transform a password into more suitable cryptographic key.

This thesis deals with such functions, in particular considering their usage in disk encryption. The most popular function PBKDF2 is described together with its vulnerabilities and attacks. Memory-hard functions have started being used as a mitigation of time-memory trade-off attacks. One of such functions is Argon2 selected as a winner of Password Hashing Competition. The thesis describes Argon2 in detail.

The practical part of the thesis deals with simulating of an attack on a disk encrypted with LUKS2 encryption scheme using Argon2 as PBKDF. It includes collecting Argon2 parameters benchmarked by Cryptsetup software. Attack is devised through CPUs and GPUs using high-performance hardware provided by MetaCentrum VO.

The last part of the thesis introduces a price model for an attacker using either physical hardware or on-demand allocation of computing resources in the cloud. This model is then applied to real world prices and data obtained during the attack simulation.

Summary and results

The goal of the thesis was to perform a realistic simulation of an attacker trying to guess a correct passphrase to an encrypted disk volume. Therefore, it was necessary to collect realistic data about such disk volumes. For the sake of this thesis, the only important data was the LUKS2 volume header. This header stores all metadata pertaining to an encrypted volume. These headers were generated on two very different hardware configurations; a powerful laptop and a single-board computer. A related goal was to verify if PBKDF parameters provided by the Cryptsetup disk encryption software are sufficient to withstand brute-force attacks devised with powerful hardware, possibly using parallelization. Therefore I chose two very different devices.

In later stage of the experiment, a simulation of an actual attack was performed utilizing powerful hardware. For example machines with 32 high performance CPU cores supporting AVX512F instructions and 192 GiB of RAM, as well as machines equipped with GPUs providing 12 GiB of dedicated memory were used. Attacks were devised utilizing Argon2 implementation for CPU as well as for OpenCL and CUDA parallel computing frameworks.

These results were later analyzed and two price models were created. The first model supposed that an attacker buys physical hardware for an attack, the second model assumed utilization of on-demand computing resources located in cloud.

To point out one example, cracking in ten years an eight characters long passphrase used to unlock encrypted volume in circa two seconds on Raspberry PI could take up to 1,085 Nvidia Tesla P100 GPUs costing circa 120 million dollars. Trying to crack a volume created on modern laptop would require up to 75,121 powerful machines running for ten years costing over four billion dollars.

Based on collected results the default Argon2 parameters used by Cryptsetup and LUKS2 provide sufficient security considering intended use of this software.