

NOW – ENTERPRISES DO NOT HAVE TO STORE ENCRYPTION KEYS ANYMORE

Swedish company changes the playing field for storing passwords and encryption keys.

GOTHENBURG, SWEDEN, April 23, 2019 /EINPresswire.com/ -- The Swedish based cybersecurity start-up Authentico Technologies, developed a centralized hardware unit that can be installed on an enterprise's servers. The product, named CIPHRA, is a hardware device that makes password theft essentially impossible even if a database is stolen. Passwords and other sensitive data are protected because no secret key material are stored anywhere. The device works as a plug-and-play product and, once running, it enhances security without any change in the user experience or login process.

The technology called PUF (physically unclonable functions) is used by turning this slightly noisy fingerprint of the chip into a reliable root key. Whenever the root key is needed by the system, CIPHRA reliably reconstructs it without the need for storing this root key in any form of memory and They are virtually impossible to clone or predict.

When using PUF, cryptographic keys and identities are derived from a digital fingerprint in the start-up behavior of SRAM cells. This means the secret material is never stored in memory and no physical traces can be found on a chip that lead to the secret material. Hence, using SRAM PUF protects secrets from reverse engineering attacks, simply by virtue of the fact the secrets are not present on the chip in any physical form. So, besides removing the requirement for externally provisioning keys to chip (because they are created from the silicon imperfections internally), storing keys with PUF also provides a level of security that cannot be achieved with any other form of key storage, due to the fact that keys are not physically stored on the chip.

“Our approach, to generate strong unclonable keys and not store them anywhere, makes theft of passwords and encryption keys essentially impossible,” said Philip Lundin Weinstock, chief executive officer of Authentico Technologies. “The exposure of passwords has reached alarming levels, there are approximately 8 billion stolen passwords that are accessible via the dark web today and new data breaches are reported more or less each month now”.

We guarantee our customers that passwords, or the password hashes are useless to an attacker if they get stolen, regardless of the password strength and the resources available to the hacker. This is something that can not be guaranteed by recommended hashing algorithms since the time it takes to crack a password offline, depends on the strength of the password itself. Weaker passwords get cracked very fast using sophisticated dictionary lists and brute force attacks with dedicated hardware. Besides that these kind of attacks improves all the time, hardware is also getting cheaper and more powerful every single year.



The major problem with the current approaches is that they do not stop data from being stolen in the first place. Rather it might delay the use of the stolen data for an uncertain period of time that depends on both the computational resources available to the attacker and weaknesses being found in algorithms, along with findings published by researchers.

One of the key problems is that personally identifiable information is stored using industry standard architecture which is vulnerable to various attacks. Encryption keys can usually be exploited inside code or maintained in files on servers and wherever they are stored. Hackers and insiders can infiltrate those hidden places which put the whole organization at serious risk.

Philip says: "The problem we see is that the vast majority of users do not change their behavior - How many years have the community informed people about generating strong passwords, turn on two factor authentication and use a recommended password manager?

A tiny minority does that, but the majority does not. We must ask ourselves, what can we do to improve the security for the users, not what the users can do themselves".

Philip Lundin Weinstock
Authentico Technologies
+46 73 322 10 40

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases. © 1995-2019 IPD Group, Inc. All Right Reserved.