AUTHENTICO ELIMINATE THE COSTS AND RISKS OF BULK PASSWORD AND DATABASE INFORMATION THEFTS

CIPHRA
BY AUTHENTICO
TECHNOLOGIES

"OUR MISSION IS TO BE A GLOBAL LEADER IN THE PASSWORD AND DATABASE PROTECTION INDUSTRY, WITH A SCALABLE AND COST-EFFICIENT HARDWARE SOLUTION" - MARTIN FABIANSSON, CEO

THE PROBLEM

There are more than 12 billion passwords that are hacked and for sale on the Dark Web. Software-based hashing algorithms, such as bcrypt, crypt, scrypt, PBKDF2 are not secure enough due to users' predictability of using weak passwords as well as the increasing computer processing power that enables higher success rates when it comes to password cracking.

Attackers have statistically between 191-487 days to crack the stolen password hashes before the organization has realized they´ve been breached; in many cases much longer according to an IBM Ponemon study from 2017.
Additionally, the average cost per compromised record is more than US$216 according to the Ponemon institute.

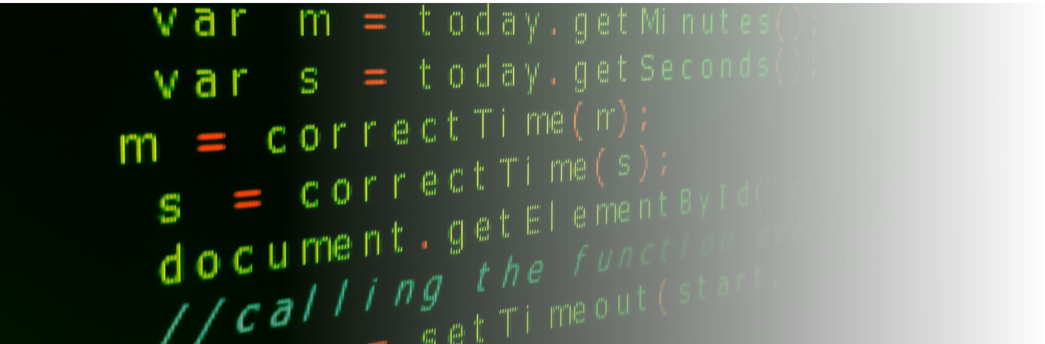
THE SOLUTION

CIPHRA is a Hardware Security Module powered by PUF (Physical Unclonable Functions) and works as a password hashing processor with encryption capabilities.
Using our patented PUF technology will enable next generation highest protection, where no root/master key is stored or backed-up anywhere, at a much lower cost than other alternatives.
The CIPHRA appliances are designed to easily scale redundancy and throughput. In other words, increasing the number of authentications per second without any major changes to the customer's existing system architecture.

Without access to the keys protected by CIPHRA, the stolen data is useless to the attacker.

Connecting the CIPHRA appliances to public web-server databases prevents the password hashes from being cracked through offline password recovery attacks such as brute force, rainbow tables etc, regardless of the password strength and computing resources available to the attacker.

Furthermore, the offline key generated during the installation process is used to scale and seamlessly maintain the redundancy and throughput required for your online service.



```
var m = today.getMinutes();
var s = today.getSeconds();
m = correctTime(m);
s = correctTime(s);
document.getElementById(
//calling the function
getTimeout(start
```

WHO SHOULD USE CIPHRA?

If your organization has multiple users/customers that authenticate with usernames and passwords, we guarantee the strongest protection for your clients.
If the customer/user database is leaked, we eliminate the risk of their accounts being hijacked.

Today we mainly offer our products to hosting and online service providers, but there are of course no limits to the type of organization who can use us.

HOW DOES CIPHRA WORK?

CIPHRA is a PUF-based password storage solution that processes user passwords (or the salted password hashes) and then stores the output. The validity of a user password is checked by processing the user password (or its salted hash) by CIPHRA's cryptographic processor and comparing the output with the corresponding stored value.
Additionally, the solution does not rely on any administrator passwords and thus makes insider threats less risky.
CIPHRA processes the passwords with a unique device key protected by a PUF-key, which is never stored except for an offline copy which can be kept in a physical valve or shared in part between administrators.

SUMMARIZATION - QUESTIONS TO ASK YOURSELF

Do all of your users have two-factor authentication turned on?

If not, the attacker is only one step from being able to access the account.
Even if two-factor authentication is turned on, it is still possible to go around.

How many of your users have very strong passwords?

As described previously, most users tend to create weak and predictable passwords which are easy to crack regardless of which software hashing algorithm that is used.

What are the major risks if your database leaks?

Think about:

- Financial impacts - Remediation costs
- Reputation costs - Customer loss
- Account takeover - Abuse
- Competitors can get access to your customers
- GDPR - Sensitive data
- PR issues

This company has received funding from the European Union's Horizon 2020 research and innovation programme