STEVEN
MEYER

Co-Founder & Co-CEO

Cracking the Code: How GPU-Accelerated Rainbow Tables Changed Password Security

June 2024, Microsoft has just announced the phasing out of NTLM, a security protocol for authenticating Windows users. But this retirement is long overdue as it has been broken for more than a decade. Let me tell you the story of how I became infamous by rendering the Windows 8-character passwords obsolete.

Breaking password is a science of itself. You can social engineer it out from someone with phishing attacks and fake websites, you can steal it with keylogger and password recovery tools (like Mimikatz), you can try to guess it by using personal and stollen information, or you can crack it.
The principle of a password is quite simple: the user and a device share a common secret (the password) and when the user want to authenticate, he input it on the device. The device will compare both of them, and then only if it is the same, the access is granted. Instead of storing actual passwords, which can be stolen, the industry uses a technique called hashing. This converts the original password into a unique set of characters (the hash), which is easy to verify but hard to reverse and reveal.

My research was about how to reverse and reveal in a much-optimized way. One option is to precalculate the 6 quadrillion 8-character passwords and their hashes. It would then be very easy to crack by doing a simple lookup, but it would require 133 PB of storage. An alternative would be to crack the password in real time, but it would take a month at each cracking operation.

The solution was to use Rainbow Tables, an ingenious solution to this problem, allowing for a time-memory compromise. We precalculate potential password hashes but store them in a way that dramatically reduces the required space and search time. The result of the research was the creation of a rainbow tables with NVIDIA Cuda GPUs that could sit in a 1TB SSD drive use 4GB of RAM and break 99% of 8-character NTLM passwords in an average of 23 sec.

This project has not only pushed the industry to use passwords beyond 8-characters, but also to add salt in passwords, and to promote Memory-hard & Time-expensive algorithm such as bcrypt for secure password storage.

> "My research was about how to reverse and reveal in a much-optimized way.
>
> Steven MEYER
> Co-CEO of ZENDATA

Always in
movement
to protect

our team.