

# CYBERSECURITY CYBER-ATTACK SERIES

## SIDE CHANNEL – RAINBOW TABLE

### ATTACKS

Prepared by David Mohajer

## What is a Rainbow Table attack?

### Technical:

A rainbow table attack is when a hacker wants to compromise the login credentials of users in an online system. This is done through the use of pre-computed hash tables that allow for reversing the hashes back to plain text in order to successfully crack hashed passwords.

### English:

The obfuscation method for login passwords can be reverse engineered using Rainbow Table attacks. The bottom line is that if a system is protected only by a password – it can probably be breached with a Rainbow Table.

## Why Rainbow Tables?

Rainbow tables are created to save time when attempting to brute force into systems protected by hashed passwords. This is done for a number of reasons:

1. “Traditional” Brute force methods can take minutes, hours, days, months or years to crack using software like [John the Ripper](#) (O'Donnell, 2016).
2. Rainbow tables can be shared, purchased, and sold. They range in the single digit Terabytes in size (O'Donnell, 2016) and can easily be placed onto cheap consumer grade hard drives.

## Have you suffered a Rainbow Table attack?

This is almost impossible to determine, as a rainbow table attack generally does not involve brute forcing a login system in order to guess passwords. All they need is a few hashed passwords and time to figure out the hashing algorithm, and then they can start building the rainbow table — or select an existing one.

It is best practice to assume that you are vulnerable to Rainbow Table attacks unless you have taken special precautions against it in your authentication scheme.

There will always be some users that have weak passwords that can be cracked using a dictionary attack, therefore the hashing and salting algorithm will be broken as a result of password selection by those users. Alternatively, if people from the wild can login and make



Your Cybersecurity Partner

their own accounts this can be a potential issue, as well as, it can facilitate the analysis needed to determine the right hashing algorithm your system is using to obfuscate passwords.

## Preventing a Rainbow Table attack

It is common practice to salt and hash passwords in databases (O'Donnell, 2016) to protect against simple data exfiltration of user databases. The risk here is if the original data exfiltration was able to recover the salts as well – then salting does not help.

Per user salting combined with bcrypt implementation is recommended (TheCodeArtist, 2010) for all user databases in a production environment.

Salting is not the be-all and end-all of protection against Rainbow Table hacking (Salt – Preventing Rainbow Attacks against Password Stores, 2014), but it can mitigate the speed at which Cyber Criminals will break into your system and reduce them to one account per week instead of all accounts in one day – so keep those hashes slow!

Do not use the same password more than once, or you will become commodified by Cyber Criminals (Salt – Preventing Rainbow Attacks against Password Stores, 2014).

XAHIVE recommends that for systems that contain PII, PHI, and Trade Secrets and have public facing portals – that there be some type of secondary Authentication such as an RSA encryption key or rapidly changing pin number sent via encrypted link to a mobile device.

## Works Cited

- Kuliukas, K. (2007, January 4). *How Rainbow Tables work*. Retrieved from Kestas: <http://kestas.kuliukas.com/RainbowTables/>
- O'Donnell, A. (2016, March 31). *Rainbow Tables: Your Password's Worst Nightmare*. Retrieved from about tech: <http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm>
- Salt – Preventing Rainbow Attacks against Password Stores*. (2014, March 31). Retrieved from sqlity.net: <http://sqlity.net/en/2309/salt/>
- Salting Passwords Thwarts Rainbow Table Attacks*. (2007, March 1). Retrieved from CSO Online: <http://www.csoonline.com/article/2121265/application-security/salting-passwords-thwarts-rainbow-table-attacks.html>
- TheCodeArtist. (2010, April 10). *Rainbow Tables: How to defend against them?* Retrieved from stack overflow: <http://stackoverflow.com/questions/2675073/rainbow-tables-how-to-defend-against-them>