Security: Some Fun with Passwords

- How to handle Passwords: the Basics
- Rainbow Attacks

Not too long ago...

Hi, I forgot my password!

Let me help you. What is your name?

My Name is John Doe.

I found you in my system. Your password is XXXYYY.

Q: What is wrong with this scenario?
### Password Hashing

Instead of storing the password on the server...

...we store an encrypted (hashed) version of the password.

Is Alice’s password = “XXXYYY”? Is Alice’s password hash = Hash(“XXXYYY”)?

### Replay Attacks and Challenge Response

Simply encrypting a request does not protect from replays.

Solution: Challenge-response.
Is Password Hashing Overrated?  
(or, hacking password files using rainbow tables)

Password Hashing:

Two approaches to “Decrypt” passwords:
1. Exhaustively generate and hash passwords and check for match.
2. Generate table for all possible passwords and their hashes. Then just look up.

Rainbow Tables: Reduction Functions

Reduction function:
\[ \text{RED}(arg) := \text{pick first numerical 6 digits of arg.} \]
**“Chains” of Hashes**

Simple Hash Chain Table:

<table>
<thead>
<tr>
<th>start</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>iaisudhui</td>
<td>4259cc34599c530b1e4a8f225d665802</td>
</tr>
<tr>
<td>oxcvioix</td>
<td>c744b1716cbf8d4dd0ff4ce31a177151</td>
</tr>
<tr>
<td>9da8dasf</td>
<td>3cd696a8571a843cda453a229d741843</td>
</tr>
<tr>
<td>[...]</td>
<td></td>
</tr>
<tr>
<td>sodifo8sf</td>
<td>7ad7d6fa6bb4fd28ab98b3dd33261e8f</td>
</tr>
</tbody>
</table>

**Problems with Hash Chains**

- **Chains can collide:**
  - When hash function or reduction values collide, hash chains **merge**.
  - Hash function values are unlikely to collide
  - Reduction function values are **likely** to collide

- Reduction function should map back to **likely subset** of passwords.
  - If not, we are spending time scanning the entire space.
How to Counter such Attacks? Salting

Instead of storing the hash

\[ \text{hash(password)} \]

we store the salted hash

\[ \text{hash(password + salt)} \]

where salt is a very large number.