Practical Application of Hashing

Objectives

- Understand how hashing should be used
- Discuss where hashing is used today
- Discuss how failures of implementation lead to data breaches

Technology today

- Websites want you to register
  - How many accounts do you have?
  - Each site stores your password in some sense
- Your phone
  - Pin
  - Password
  - Fingerprint
- Your computer
  - Stored password?
- Your car
  - Keys are coded to only work with your car

Logins

- Windows uses NTLM to store hashes
  - The password is padded with NULL bytes to exactly 14 characters. If the password is longer than 14 characters, it is replaced with 14 NULL bytes for the remaining operations.
  - The password is converted to all uppercase.
  - The password is split into two 7-byte (56-bit) keys.
  - Each key is used to encrypt a fixed string.
  - The two results from step 4 are concatenated and stored as the LM hash.
- Linux, BSD use various hashing algorithms, however most are “salted”

Databases

- Microsoft produced a study around 10 years ago, the results were that an average user only uses 5 to 6 unique passwords for all of their accounts
- What if your data is breached on one website?
- Databases should store your password as an encrypted password. This should be a function of the database implementation on the server side.

Rainbow tables

- Used to store many hashes for a certain type of hashing algorithm
- Precomputed to easily find password
- Some are small, most are not
- Types: wireless, NTLM
- Can use online crackers or use a graphics card to compute

Intrusion/AV Detection

- Many AV companies use hashes to detect malicious software
- Same with intrusion detection
- In 2016, Verizon DBIR, shown 99% of malware is only up for 58 seconds
- That means a lot of hashing
- There are evasion techniques
- Best AV/IDS/IPS uses machine learning or other heuristics to detect maliciousness

Data Breaches

- Yahoo! – 1billion accounts secured with only MD5 hash
- Cupid Media – 42 million accounts, no encryption
- LinkedIn – 6.5 million accounts – but encrypted, without salts