Cybersecurity

Database Security

CYBER.ORG

Tokens

- Access token
  - An object that specifies access rights
    - Keys are an example of a token
      - But what if a key is compromised?
      - You have to change the locks/keys
    - Tokens can be changed frequently
      - Does not matter if a token is compromised if it changes
- Hardware Tokens
  - A proximity card, USB tokens, key fobs, etc…
- Software Tokens
  - Provide two-factor authentication
  - Password and the token

Hashing and Salting

- Hashing a database
  - Creates a unique string of text
  - If altered, a completely new string of text

- Salting a database
  - Adding a string before hashing
  - Extra layer of security
  - Creates different outputs for same database

Hashing Example

Notice, Boise has been changed to Sandpoint

Original Database

	A	B	C	D	E
1	**First Name**	**Last Name**	**City**	**State**	
2	Francis	Shelton	Boise	Idaho	
3	Judith	Moreno	Newark	New Jersey	
4	Kenny	Goodwin	Buffalo	New York	
5	Betty	Miles	Reno	Nevada	
6	Wilson	Vega	Colorado Springs	Colorado	
7	Danielle	Tyler	Akron	Ohio	
8	David	Haynes	Milwaukee	Wisconsin	
9	Velma	Sanchez	Indianapolis	Indiana	
10	Noel	Sharp	Denver	Colorado	
11	Frances	Park	Riverside	California	
12					

Altered Database

	A	B	C	D	E
1	**First Name**	**Last Name**	**City**	**State**	
2	Francis	Shelton	Sandpoint	Idaho	
3	Judith	Moreno	Newark	New Jersey	
4	Kenny	Goodwin	Buffalo	New York	
5	Betty	Miles	Reno	Nevada	
6	Wilson	Vega	Colorado Springs	Colorado	
7	Danielle	Tyler	Akron	Ohio	
8	David	Haynes	Milwaukee	Wisconsin	
9	Velma	Sanchez	Indianapolis	Indiana	
10	Noel	Sharp	Denver	Colorado	
11	Frances	Park	Riverside	California	
12					

SHA256 Checksum

900949c6d5f422adba9be331eb4c5e05ae8c4d5cc
00de335d60985e167726fe8

SHA256 Checksum

d0f48f6a3f2135de451ab470bfaa04f24717291147
342d17bcab70e66d54e1dd

Notice, they have completely different checksums, thus, the database has been altered/tampered with