Alice gives me your PK

PK_B, cert

wet = sign(SK_CA, Bank has PK_B, expiry)

CA

Better than TD:
+ can contact Bank (or anyone) to obtain PK

Certificate hierarchies & chains

Verisign CA

UC President

David

Raluca

Stanford President

\[ C_U = sign(SK_CA, \text{"UC Pre. has PK}_U\text{"}, expiry) \]

\[ C_S = sign(SK_V, \text{"David has PK}_D\text{"}, expiry) \]

Certificate chain

When I ask for David's PK, I will receive PK_D, C_1, C_2,
- check PK_U using C_1 using PK_CA
- check PK_D using C_2 and knowledge of PK_U

David, berkeley.edu

Path of authority
Root servers serve cert.edu

Revocation

How can we revoke a certificate that has not yet expired?

- Wait till expiry, make expiry shorter

- Revocation lists: CA could push revocation
  sign (SKCA, "Revoke cert") into browsers; not ideal solution because
  browsers might not be downloading lists

Long-term problem with CAs:

CAs can be compromised or could be deceived
  to sign incorrect certificates

- Transparency logs promise to address this problem
Passwords

Tension between usability and security

- choose memorable passwords
- choose random and long passwords (hard to guess)
Attack mechanisms

• Online guessing attacks
  – Attacker tries to login by trying different user passwords in the live system
• Social engineering and phishing
  – Attacker fools user into revealing password
• Eavesdropping
  – Network attacker intercepts plaintext password on the connection
• Client-side malware
  – Key-logger/malware captures password when inserted and sends to attacker
• Server compromise
  – Attacker compromises server, reads storage and learns passwords
Defences/mitigations

Network eavesdropper:
• Encrypt traffic using TLS (will discuss later)

Client-side malware: hard to defend
• Intrusion detection mechanisms – detect malware when it is being inserted into the network
• Various security software (e.g., anti-virus)
• Use two-factor authentication
Mitigations for online-guessing attacks

• Rate-limiting
  – Impose limit on number of passwords attempts

• CAPTCHAs: to prevent automated password guessing

• Password requirements: length, capital letters, characters, etc.
Mitigations for server compromise

• Suppose attacker steals the database at the server including all password information
• Storing passwords in plaintext makes them easy to steal
• Further problem: users reuse passwords at different sites!

Don’t store passwords in plaintext at server!
Hashing passwords

• Server stores hash(password) for each user using a cryptographic hash function
  – hash is a one-way function

<table>
<thead>
<tr>
<th>username</th>
<th>hash of password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>hash(Alice’s password)</td>
</tr>
<tr>
<td>Bob</td>
<td>hash(Bob’s password)</td>
</tr>
</tbody>
</table>

• When Alice logs in with password w (and provides w to server), server computes hash(w) and compares to Alice’s record
Password hashing: problems

• Offline password guessing
  – Dictionary attack: attacker tries all passwords against each hash(w)
  – If D is dictionary size, n number of hashes passwords, attack takes Dn
  – Study shows that a dictionary of $2^{20}$ passwords can guess 50% of passwords

• Amortized password hashing
  – Idea: One brute force scan for all/many hashes (D+n time)
  – Build table (H(password), password) for all $2^{20}$ passwords
  – Crack 50% of passwords in this one pass
LinkedIn was storing h(password)

"Link" was the number one hacked password, according to Rapid7. But many other LinkedIn users also picked passwords — "work" and "job" for example — that were associated with the career site's content.

Religion was also a popular password topic — "god," "angel" and "jesus" also made the top 15. Number sequences such as "1234" and "12345" also made the list.
Prevent amortized guessing attack

- Randomize hashes with salt
- Server stores \((\text{salt}, \text{hash(password, salt)})\), salt is random
- Two equal passwords have different hashes now
- Dictionary attack still possible, BUT need to do one brute force attack per hash now, not one brute force attack for many hashes at once
- Attacks takes Dn time instead of D+n time
## Salted hash example

<table>
<thead>
<tr>
<th>username</th>
<th>salt</th>
<th>hash of password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>235545235</td>
<td>hash(Alice’s password, 235545235)</td>
</tr>
<tr>
<td>Bob</td>
<td>678632523</td>
<td>hash(Bob’s password, 678632523)</td>
</tr>
</tbody>
</table>

Attacker tries to guess Alice’s password:
Computes table
- ‘aaaaaa’  | hash(‘aaaaaa’, 235545235),
- ‘aaaaab’  | hash(‘aaaaab’, 235545235),
- …
- ‘zzzzzzz’ | hash(‘zzzzzzz’, 235545235)

This table is useless for Bob’s password because of different salt
Increase security further

• Would like to slow down attacker in doing a dictionary attack
• Use slow hashes = takes a while to compute the hash
• Define
  \[ H(x) = \text{hash(hash(hash(…hash(x))))} \]
  use with \( x = \text{password} || \text{salt} \)

• Tension: time for user to authenticate & login vs attacker time
• If \( H \) is 1000 times slower and attack takes a day with \( H \), attack now takes 3 years with \( F \)
Conclusions

- Do not store passwords in cleartext
- Store them hashed with salts, slower hash functions better