Network Security

User and Network Authentication

Christopher Kruegel
Spring 2020
UC Santa Barbara
Passwords
User Authentication

- Authentication is the process of proving identity within an access control framework
  - Trusted system checks credentials presented by users
  - “Something you have, know, or are”
  - Unguessable, unforgeable, revocable
- Passwords are the de facto single-factor credential

Passwords fail in numerous ways
Password Attacks

- Passwords can be guessed
  - Passwords should have high entropy
  - People are bad at choosing high-entropy passwords
  - Machines can very quickly test password guesses
- Passwords must be protected at rest and in transit
  - Developers are bad at ensuring these properties
Attacker simply guesses passwords until a correct guess is made

- Authentication systems should limit rate and total number of guesses
- Prevent, or make more difficult, automated interactions
- Apply same principles to any secrets (complete mediation) e.g., password recovery mechanisms
Password Strength

\[ H = \log_2 N^L = L \log_2 N = L \frac{\log_i N}{\log_i 2} \]

- Entropy (H) is the usual password quality metric
  - \( N \) = number of possible symbols, \( L \) = length of password
  - Measure of unpredictability or average information content
- How to increase password strength in terms of \( N, L \)?
- What assumptions underlie entropy as a strength metric?
Table 1: Humans are notoriously bad at generating memorable random strings [1]

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>–</td>
</tr>
<tr>
<td>2</td>
<td>password</td>
<td>–</td>
</tr>
<tr>
<td>3</td>
<td>12345678</td>
<td>+1</td>
</tr>
<tr>
<td>4</td>
<td>qwerty</td>
<td>+2</td>
</tr>
<tr>
<td>5</td>
<td>12345</td>
<td>-2</td>
</tr>
<tr>
<td>6</td>
<td>123456789</td>
<td>NEW</td>
</tr>
<tr>
<td>7</td>
<td>letmein</td>
<td>NEW</td>
</tr>
<tr>
<td>8</td>
<td>1234567</td>
<td>–</td>
</tr>
<tr>
<td>9</td>
<td>football</td>
<td>-2</td>
</tr>
<tr>
<td>10</td>
<td>iloveyou</td>
<td>NEW</td>
</tr>
</tbody>
</table>
';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username

264 pwned websites
4,859,717,682 pwned accounts
61,409 pastes
59,821,668 paste accounts

Top 10 breaches

711,477,622 Onliner Spambot accounts
593,427,119 Exploit.In accounts
457,962,538 Anti Public Combo List
There’s a lot of advice on how to select good passwords. Most of it is bad.
Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
Password Strength Meters

If people can’t select good passwords, let’s help them

– Meter gives immediate feedback on how strong a password is
– Ideally, should give *suggestions* on how to improve candidate passwords
– Requires a realistic model for what makes a password strong
<table>
<thead>
<tr>
<th></th>
<th>qwER43@!</th>
<th>Tr0ub4dour&amp;3</th>
<th>correcthorsebatterystaple</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>zxcvbn</strong></td>
<td><strong>Weak</strong></td>
<td><strong>So-so</strong></td>
<td><strong>Great!</strong></td>
</tr>
<tr>
<td><strong>Dropbox (old)</strong></td>
<td><strong>Great!</strong></td>
<td><strong>Great!</strong></td>
<td><strong>So-so</strong></td>
</tr>
<tr>
<td><strong>Citibank</strong></td>
<td><strong>Medium</strong></td>
<td><strong>Strong</strong></td>
<td>1 number required</td>
</tr>
<tr>
<td><strong>Bank of America</strong></td>
<td>(not allowed)</td>
<td>(not allowed)</td>
<td>(not allowed)</td>
</tr>
<tr>
<td><strong>Twitter</strong></td>
<td>✔ Password is perfect!</td>
<td>✔ Password is perfect!</td>
<td>✔ Password is perfect!</td>
</tr>
</tbody>
</table>
Password Selection Guidelines

- Avoid common passwords
- Avoid personal information
- Use a large symbol alphabet and long strings
- Don’t reuse passwords
- *Use a password manager*
Offline Password Attacks

Attacker captures password database and directly attacks it

– Obviously if passwords are in cleartext, the game is over
– Passwords are cryptographically hashed (not encrypted)
– Passwords checked by comparing hashes

\[ h_{\text{stored}} = H(p_{\text{provided}}) \]
Historical Password Hashing

$ man 3 crypt

– 25 iterations of DES on a zeroed vector
– First eight bytes of the password used as the key
– 12-bit salt to hinder dictionary attacks

What is wrong with this method?
Key Derivation

- Key derivation function (KDF) produces a secret key from a secret input using a pseudorandom function (PRF)
- *Salt* is a nonce intended to prevent precomputation attacks
- *Key stretching* adds salt and iterations to slow each KDF application
- *Key strengthening* is similar but deletes the salt
Modern Password Hashing

```
$ man 3 crypt
```

- Modular crypt format: $scheme$rounds$salt$hash
- $10^3$ – $10^8$ iterations of SHA-2
- Full password is used
- Up to 16 bytes of salt
- See PBKDF2 [2]

**Goals:** Enlarge the search space, slow the guess rate
Modern Password Crackers are Fast

Hashcat Benchmark, 8x Nvidia GTX 1080, MD5

Speed.Dev.#1.: 24943.1 MH/s (97.53ms)
Speed.Dev.#2.: 24788.6 MH/s (96.69ms)
Speed.Dev.#3.: 25022.2 MH/s (97.76ms)
Speed.Dev.#4.: 25106.6 MH/s (97.42ms)
Speed.Dev.#5.: 25114.1 MH/s (97.42ms)
Speed.Dev.#6.: 24924.1 MH/s (97.30ms)
Speed.Dev.#7.: 25197.9 MH/s (97.30ms)
Speed.Dev.#8.: 25246.4 MH/s (97.00ms)
Speed.Dev.#*.: 200.3 GH/s
Memory-Hard Password Hashing

```rust
let block_size_factor = 8;
let block_size = 128 * block_size_factor;
let blocks = pbkdf2_hmac_sha256(passphrase, salt, 1, block_size * pf);
for i in 0..p { blocks[i] = ro_mix(blocks[i], 2^cost_factor); }
let expensive_salt = blocks.into_iter().join();
return pbkdf2_hmac_sha256(passphrase, expensive_salt, 1, key_length);
```

- scrypt [3] password-based key derivation function (PBKDF)
- Renders hardware-based attacks difficult by requiring large amounts of memory
- Also see Argon2 [4]
Password Search Strategies

- Precomputation
- Brute-force search
- Dictionary attacks
- Mutation rules
- Generative models
- Combinations of the above
Precomputation Attacks

Given a password space $P$, hash digest space $D$, and hash function $H : P \mapsto D$, precompute an inverse mapping $H' : D \mapsto P$

- Naïve precomputation requires $\Theta(|P|^n)$ bits
- Hash chains can be used to balance the time-space tradeoff between run-time guessing and computing $H'$
Precompute a list of password–hash digest mappings, but only store the start and end values

- Hash chains define a reduction $R : D \mapsto P$
- Reductions are not inverse mappings!
- Instead, $R$ cover the space of likely passwords
Computing Hash Chains

\[ p_{i,0} \xrightarrow{H} h_{i,0} \xrightarrow{R} p_{i,1} \xrightarrow{\sim} h_{i,k-m} \xrightarrow{R} p_{i,k} \xrightarrow{H} h_{i,k} \]

- Chains are computed by selecting an initial password \( p_i \) and alternating applications of \( H, R \) up to length \( k \)
- Chain \( i \) becomes \((p_{i,0}, h_{i,k})\)
Using Hash Chains

\[ h_{i, j} \xrightarrow{R} p_{i, j} \rightleftharpoons h_{i, k-1} \xrightarrow{R} p_{i, k} \xrightarrow{H} h_{i, k} \]

\[ \Downarrow \]

\[ p_{i, 0} \xrightarrow{H} h_{i, 0} \xrightarrow{R} p_{i, 1} \rightleftharpoons h_{i, j-1} \xrightarrow{R} p_{i, j} \xrightarrow{H} h_{i, j} \]

- To use given a hash \( h_j \), apply \( R, H \) until a chain end value \( h_{i, k} \) is found
- Then take \( p_{i, 0} \) and recompute the chain to find \( H(p_{i, k}) = h_j \)
Hash Chain Collisions

\[ R("123456") = h_i = R("iloveyou") \]

- Hash chains are prone to collisions \(\Rightarrow\) false positives
- Very difficult to make \(R\) collision resistant since it must map into space of likely passwords
- Collisions cause chain merges that reduce coverage of \(P\)
- Merges \(\Rightarrow\) chains might not contain a password even if an end value matches (Why?)
Rainbow Tables

- Rainbow tables reduce collision likelihood by using a reduction family $\mathbf{R} = \{R_1, R_2, \ldots, R_k\}$
- Instead of repeated applications of $H$, $R$, rainbow tables use $H, R_1, H, R_2, \ldots, H, R_k$ (Why?)
Rainbow Tables

- Rainbow tables reduce collision likelihood by using a reduction family $\mathbf{R} = \{R_1, R_2, \ldots, R_k\}$
- Instead of repeated applications of $H, R$, rainbow tables use $H, R_1, H, R_2, \ldots, H, R_k$ (Why?)

Collisions only occur between two chains if reduction functions are aligned!
Hash Chain Caveats

- Tables must be built for each hash function and symbol alphabet
- Salting and key stretching defeats efficiency gains
- Expensive to build
Brute-Force Search

// Try "aaaaaaaa", "aaaaaaab", "aaaaaaac", ...
let initial_guess = "aaaaaaaaa";
for guess in password_space_iterator(initial_guess) {
    if hash(guess) == target_hash {
        println!("H({guess}) = {target_hash}");
        break;
    }
}

Dictionary Attacks

// Just try every entry in some provided dictionary

for guess in read_lines(dict_path) {
    if hash(guess) == target_hash {
        println!("H({guess}) = {target_hash}"s);
        break;
    }
}
// Example rule: Change all instances of 'e' to '3'
for guess in read_lines(dict_path) {
    for rule in rules {
        let mutated_guess = rule(guess);
        if hash(guess) == target_hash {
            println!("H({guess}) = {target_hash}");
            break;
        }
    }
}
One-Time Passwords

```javascript
let counter = floor((now() - epoch()) / interval);
let hotp = select_bytes(hmac_sha1(secret, counter));
let totp = hotp(secret, time_counter) % 10^d
```

- A one-time password (OTP) is only valid for one authentication attempt and cannot be replayed
- SMS codes (undesirable, why?)
- Time-based One-Time Password algorithm (TOTP) [5]
  - Mostly used as a second factor
Universal Second Factor (U2F) [6]

- Adds a second factor *bound to a counterparty*
- Requires use of a hardware module with trusted element
- Requires user interaction, but prevents phishing/MitM attacks
U2F device is enrolled for client at relying party

h, a; c = (challenge, origin, channel)

Check a

Resolve k_priv for h, increment counter

counter, {a, c, counter}

Resolve k_pub for h, check s using k_pub, verify origin, channel, counter
Kerberos
Protocol for mutual authentication over untrusted networks
  – Used for network single sign-on (SSO) (e.g., AD)
  – Centralized principal and policy management
  – Securely establishes session keys between clients and servers
Kerberos Terms

- Realm
- Authentication server (AS)
- Key distribution center (KDC)
- Ticket-granting ticket (TGT)
- Ticket-granting service (TGS)
Client and AS establish shared secret out-of-band

Service and AS establish shared secret out-of-band

AuthRequest(P)

Server checks client principal and credentials

AuthResponse(TGT)

Client requests access to service

AccessRequest(TGT, S)

AS checks TGT and service principal

AccessResponse(T, SK)

Client sends ticket with session key

ServiceRequest(T, SK)

Service checks ticket

ServiceResponse(...)

Client and AS establish shared secret out-of-band
In the following, let Alice $A$ and Bob $B$ be two parties that trust server $S$ but not each other. Alice wants to prove her identity to Bob. Let $K_{A,S}, K_{B,S}$ be shared secrets between $A, S$ and $B, S$; $N_A, N_B$ be nonces generated by $A, B$; and $K_{A,B}$ be a negotiated session key between $A, B$. 
Needham-Schroeder Protocol

\[ A \rightarrow S : A, B, N_A \]

\[ S \rightarrow A : \left\{ N_A, K_A, B, B, \{ K_A, B, A \} \right\}_{K_{B,S}}^{K_{A,S}} \]

\[ A \rightarrow B : \{ K_A, B, A \}^{K_{B,S}}_{K_{A,S}} \]

\[ B \rightarrow A : \{ N_B \}^{K_{A,B}}_{K_{A,B}} \]

\[ A \rightarrow B : \{ N_B - 1 \}^{K_{A,B}}_{K_{A,B}} \]
Needham-Schroeder Attack

\[ A \rightarrow S : A, B, N_A \]

\[ S \rightarrow A : \left\{ N_A, K_{A,B}, B, \left\{ K_{A,B}, A \right\}_{K_{B,S}} \right\}_{K_{A,S}} \]

\[ M \rightarrow B : \left\{ K_{A,B}, A \right\}_{K_{B,S}} \]

\[ B \rightarrow M : \left\{ N_B \right\}_{K_{A,B}} \]

\[ M \rightarrow B : \left\{ N_B - 1 \right\}_{K_{A,B}} \]
Needham-Schroeder Attack (cont.)

\[ A \rightarrow S : A, B, N_A \]
\[ S \rightarrow A : \left\{ N_A, K_{A,B}, B, \{ K_{A,B}, A, T \}_K \right\}_{K_{B,S}}^{K_{A,S}} \]
\[ A \rightarrow B : \{ K_{A,B}, A, T \}_{K_{B,S}} \]
\[ B \rightarrow A : \{ N_B \}_{K_{A,B}} \]
\[ A \rightarrow B : \{ N_B - 1 \}_{K_{A,B}} \]
Kerberos Vulnerabilities

- Time synchronization is important!
  - Tickets are only valid for a specific time window
  - Desynchronization leads to
    i. denial-of-service
    ii. replay of captured tickets
- The KDC is a central point of failure
  - What happens if it is compromised?
NT Lan Manager (NTLM) [7]

NTLM is an authentication protocol suite for Microsoft OSes

– Challenge-response protocol for client authentication over untrusted networks
– NTLM suffers from several serious design flaws
NTLMv1

\[ C \rightarrow S : \text{NEGOTIATE} \{ \ldots \} \]

\[ S \rightarrow C : \text{CHALLENGE} \{ N \} \]

\[ C \rightarrow S : \text{AUTHENTICATE} \left\{ \text{DESL}_N(\text{LMOWFv1}(P)), \text{DESL}_N(\text{NTOWFv1}(P)) \right\} \]
NTLM hashes are *password-equivalent*

- LMOWFv1, NTOWFv1 only depend on the password
  - i.e., no nonces, timestamps
- Hashes can be used instead of passwords to authenticate as a victim user
- Hashes are valid until the next password change
Hash Harvesting

Multiple sources for NTLM hashes

– In-memory extraction from `lsass.exe` on compromised machines (any locally-authenticated user)
– Dumping the Security Accounts Manager (SAM) database (local users only)
– Extracting cached hashes from the SAM
– Sniffing NTLM sessions from the network
PtH Mitigations

- Login restrictions on privileged accounts
- LSA protection
- Protected users group
- Disable NTLM (but, “pass-the-ticket” still works)
Conclusions
Conclusions

In this module, we covered:

(1) Passwords
(2) Kerberos
(3) NTLM
References


