CSCI 1515 Applied Cryptography

This Lecture:

- Password-Based Authentication (Continued)
- Putting it Together: Secure Authentication
- Case Study: Group Chat
One-Sided Secure Authentication

\[(V_K, S_K) \leftarrow \text{Gen}(1^\lambda)\]

User

\[\downarrow\]

\[g^a\]

\[\text{Diffie-Hellman Key Exchange}\]

Server

\[\downarrow\]

\[g^b, gb\]

\[\text{VK}_b, X.509\]

\[\downarrow\]

\[g^{ab}\]

\[\text{Hash}\]

\[K\]

\[(K_1, K_2)\]

\[\text{Authenticated Encryption}\]

\[(\text{Encrypt-then-MAC})\]

\[\downarrow\]
Certificate Chain

Root CA

(cert1: \(6 \leftarrow \text{Sign}_{sk}(VK_1)\))

Intermediate CA1

(cert2 = \((VK_1, 6 \leftarrow \text{Sign}_{sk}(VK_1))\))

Intermediate CA2

(cert_{Bob} = \((VK_1, 6 \leftarrow \text{Sign}_{sk}(VK_1))\))

Bob

\((VK_B, SK_B) \leftarrow \text{Gen}(1^\lambda)\)

Short-lived certificates?
Password-Based Authentication

User

Server

ID, password

$h = H(\text{password})$

Signup

$ID, h$

Store $(ID, h)$

Login

Check

$ID, h$

Attacks?
Online Dictionary Attack

User

ID, password

$h = H(\text{password})$

Server

Signup

ID, h

Store (ID, h)

Login

ID, $h'$

$h' = H(\text{pwd}')$
Offline Dictionary Attack

User

ID, password

$h = H(\text{password})$

Signup

Server

ID, $h$

Store $(ID, h)$

$pwd'$

$h' = H(pwd')$

(preprocessing)
Salting

User

ID, password

Server

Signup

ID

Salt $\in \{0, 1\}$

Store $(ID, \text{Salt}, h)$

Login?

ID

Salt

$h = H(\text{password} || \text{salt})$

$h = H(\text{password} || \text{salt})$

$h' = H(\text{pwd}' || \text{salt})$

Why does it help?
Salt & Pepper

User

ID, password

Sign Up

Server

ID

0

O

↑

A

Signup

A

ID

-128

ID, salt

0

O

13

h = H(password || salt)

h

pepper

\[ h^* = H(h || pepper) \]

Login?

Store (ID, salt, h*)

ID

Salt

\[ h = H(password || salt) \]

h

H(h' = H(password || salt) || pepper*)

Why does it help?
Slow Hash Functions

- Computation-heavy hash function
  - Compose SHA256 in a certain way.

Application-Specific Integrated Circuit (ASIC) -> blockchain mining

- Memory-hard hash functions
  - Scrypt
Two-Factor Authentication (2FA)

- **User**
  - ID, password

- **Server**
  - ID
  - \( \text{Salt} \leftarrow \{0, 1\}^s \)
  - pepper \( \leftarrow \{0, 1\}^p \)

- **Signup**
  - \( h = H(\text{password} || \text{salt}) \)
  - phone #
  - Store (ID, Salt, h*, phone #)

- **How would you design it?**

- **Additional Notes**
  - 0 SMS
  - 2 app-generated code

- **Pseudorandom Function**
  - \( F_{\text{seed}}(\text{time}) \rightarrow \text{output} \)
  - \( \uparrow \) pseudorandom function
Putting it Together: Secure Authentication

Server
(public X.509 certificate)

\((V_{Ks}, S_{Ks}) \leftarrow \text{Gen}(1^\lambda)\)

Alice

\((V_{KA}, S_{KA}) \leftarrow \text{Gen}(1^\lambda)\)

Cert\(_A\)

Bob

\((V_{KB}, S_{KB}) \leftarrow \text{Gen}(1^\lambda)\)

Cert\(_B\)

Authenticated Key Exchange

Signup

Login

Signup

Login
One-Sided Secure Authentication

\[ (VK_s, SK_s) \leftarrow \text{Gen}(1^n) \]

Alice

\[ g^a \]

Diffie-Hellman Key Exchange

\[ gb, bs \]

\[ gab \]

\[ \text{Hash} \]

\[ k \]

\[ (k_1, k_2) \]

Authenticated Encryption

Signup/Login

\[ (VK_a, SK_a) \leftarrow \text{Gen}(1^n) \]

\[ VK_a \]

\[ \text{cert}_A \leftarrow \text{Sign}_{SK_a}(VK_a) \]
Two-Sided Authenticated Key Exchange

\[(VK_A, SK_A) \leftarrow \text{Gen}(1^\lambda); \text{cert}_A\]

Alice

\[6_A \leftarrow \text{Sign}_{SK_A}(g^a)\]

\[g^a, 6_A\]

Diffie-Hellman Key Exchange

Bob

\[g^b, 6_B\]

\[g^{ab}\]

\[\text{Vrfy}_{VK_A}(g^a, 6_A) = 1, \text{Vrfy}_{VK_B}(g^b, 6_B) = 1, \text{Vrfy}_{VK_A}(g^a, 6_B) = 1\]

\[g^{ab}\]

\[\text{cert}_A, \text{cert}_B\]

\[\text{Hash} \downarrow \text{Hash} \downarrow \text{Hash}\]

\[K\]

\[(K_1, K_2)\]

Authenticated Encryption

\[(\text{Encrypt-then-MAC})\]
Secure Messaging

\[ AE_{k_{bs}}(AE_{gab}(m)) \]

Server

public (X.509 certificate)

\((V_k, S_k) \leftarrow \text{Gen}(1^k)\)

Alice

\[ \downarrow g_{ab} \]

Bob

\[ \downarrow g_{ab} \]

How would you design it?
Group Chat?

Server:

\[(V_{ks}, SK_{s}) \leftarrow \text{Gen}(1^\lambda)\]

Public (X.509 certificate)

How would you design it?