CSCI 1515 Applied Cryptography

This Lecture:

- Public Key Infrastructure (PKI)
- Case Study: Secure Shell Protocol (SSH)
- Case Study: Secure Messaging / Group Chats
- Case Study: Single Sign-On (SSO) Authentication

ANNOUNCEMENTS:

1. Thank you for uploading your intro videos!
2. Get a Dean's Note or doctor's note if you need extensions.
Putting it All Together: Secure Authentication

Server

Where does it come from?

\((V_{K_S}, S_{K_S}) \leftarrow \text{Gen}(1^n)\)

Alice

\(\leftarrow \text{Seqn}_{SK_S}(\text{Alice}, V_{KA})\)

Bob

\(\leftarrow \text{Seqn}_{SK_S}(\text{Bob}, V_{KB})\)

Authenticated Key Exchange

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

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

Signup

Login

Signup

Login
Two-Sided Authenticated Key Exchange

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

Alice

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

\[g^a, 6_A\]

Bob

\[Vrfy_{VK_A}(g^a, 6_A) = 1\]

\[Vrfy_{VK_A}(g^a, 6_A) = 1\]

Diffie-Hellman Key Exchange

\[\downarrow\]

\[g^ab\]

\[\downarrow\text{Hash}\]

\[Vrfy_{VK_B}(g^b, 6_B) = 1\]

\[Vrfy_{VK_B}(g^b, 6_B) = 1\]

\[6_B \leftarrow \text{Sign}_{SK_B}(g^b)\]

\[g^ab\]

\[\downarrow\text{Hash}\]

\[K\]

\[K_1, K_2\]

Authenticated Encryption

\[(\text{Encrypt-then-MAC})\]
Public Key Infrastructure (PKI)

Certificate Authority (CA)

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

Certificate Request

Google

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

Cert_{A} \leftarrow \text{Sign}_{SK_{A}}(Google, V_{KA})

Amazon

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

Cert_{B} \leftarrow \text{Sign}_{SK_{B}}(Amazon, V_{KB})
Public Key Infrastructure (PKI)

\[(VK_b, SK_b) \leftarrow \text{Gen}(1^n)\]

Bob

Certificate Signing Request (CSR)

“bob.com” \leftarrow (bob.com; VK_b), σ \leftarrow \text{Sign}_{SK}(bob.com, VK_b)

“Certificate”

Certificate Authority (CA)

Standard: X.509 certificate
Figure 13.4: An example X.509 certificate
Certificate Chain

Root CA

\[ (VK_1, SK_1) \leftarrow \text{Gen}(1^\lambda) \]

6₁ \leftarrow \text{Sign}_{SK_1}(VK_1)

Intermediate CA1

\[ (VK_1, SK_1) \leftarrow \text{Gen}(1^\lambda) \]

VK₁, 6₁
6₂ \leftarrow \text{Sign}_{SK_1}(VK_2)

Intermediate CA2

\[ (VK_2, SK_2) \leftarrow \text{Gen}(1^\lambda) \]

VK₁, 6₁
VK₂, 6₂
6₂ \leftarrow \text{Sign}_{VK_2}(VK_B, 0)

Bob

\[ (VK_B, SK_B) \leftarrow \text{Gen}(1^\lambda) \]
Certificate Revocation

- Short-lived certificates
- Certificate revocation lists (CRLs)
Case Study: Secure Shell Protocol (SSH)

Known to each other

\((V_{KA}, SK_A) \leftarrow \text{Gen}(1^n)\)

\((V_{KB}, SK_B) \leftarrow \text{Gen}(1^n)\)

Client

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

\(g^a, 6_A\)

\(\text{Vrfy}_{V_{KA}}(g^a, 6_A) = 1\)

Diffie-Hellman Key Exchange

\(g^b, 6_B\)

\(6_B \leftarrow \text{Sign}_{SK_B}(g^b)\)

Server

\(\downarrow \text{Hash}\)

\(K\)

\((K_1, K_2)\)

\(\downarrow \text{Hash}\)

\(K\)

\((K_1, K_2)\)

Authenticated Encryption

\((\text{Encrypt-then-MAC})\)
Generating a new SSH key

You can generate a new SSH key on your local machine. After you generate the key, you can add the key to your account on GitHub.com to enable authentication for Git operations over SSH.

Note: GitHub improved security by dropping older, insecure key types on March 15, 2022.

As of that date, DSA keys (ssh-dss) are no longer supported. You cannot add new DSA keys to your personal account on GitHub.com.

RSA keys (ssh-rsa) with a valid_after before November 2, 2021 may continue to use any signature algorithm. RSA keys generated after that date must use a SHA-2 signature algorithm. Some older clients may need to be upgraded in order to use SHA-2 signatures.

1 Open Terminal.

2 Paste the text below, substituting in your GitHub email address.

```
$ ssh-keygen -t ed25519 -C "your_email@example.com"
```

Note: If you are using a legacy system that doesn't support the Ed25519 algorithm, use:

```
$ ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

This creates a new SSH key, using the provided email as a label.

> Generating public/private ALGORITHM key pair.

When you're prompted to "Enter a file in which to save the key", you can press Enter to accept the default file location. Please note that if you created SSH keys previously, ssh-keygen may ask you to rewrite another key, in which case we recommend creating a custom-named SSH key. To do so, type the default file location and replace id_ssh_keyname with your custom key name.

> Enter a file in which to save the key (/Users/YOU/.ssh/id_ALGORITHM: [Press enter])

3 At the prompt, type a secure passphrase. For more information, see "Working with SSH key passphrases."

> Enter passphrase (empty for no passphrase): [Type a passphrase]
> Enter same passphrase again: [Type passphrase again]
Copy the SSH public key to your clipboard.

If your SSH public key file has a different name than the example code, modify the filename to match your current setup. When copying your key, don't add any newlines or whitespace.

```
$ pbcopy < ~/.ssh/id_ed25519.pub

# Copies the contents of the id_ed25519.pub file to your clipboard
```

Tip: If `pbcopy` isn't working, you can locate the hidden .ssh folder, open the file in your favorite text editor, and copy it to your clipboard.

In the upper-right corner of any page, click your profile photo, then click Settings.

In the "Access" section of the sidebar, click ⚛ SSH and GPG keys.
4. Click **New SSH key** or **Add SSH key**.

5. In the "Title" field, add a descriptive label for the new key. For example, if you're using a personal laptop, you might call this key "Personal laptop".

6. Select the type of key, either authentication or signing. For more information about commit signing, see "About commit signature verification."

7. **Paste your public key into the "Key" field.**

8. **Click Add SSH key.**

9. If prompted, confirm access to your account on GitHub. For more information, see "Sudo mode."
Testing your SSH connection

After you've set up your SSH key and added it to your account on GitHub.com, you can test your connection.

Mac  Windows  Linux

Before testing your SSH connection, you should have:

- Checked for existing SSH keys
- Generated a new SSH key
- Added a new SSH key to your GitHub account

When you test your connection, you'll need to authenticate this action using your password, which is the SSH key passphrase you created earlier. For more information on working with SSH key passphrases, see "Working with SSH key passphrases".

1. Open Terminal.

2. Enter the following:

   $ ssh -T git@github.com
   # Attempts to ssh to GitHub

   You may see a warning like this:

   > The authenticity of host 'github.com (IP ADDRESS)' can't be established.
   > RSA key fingerprint is SHA256:nThbg6kXUpJWGl7E11G0CspRomTxdCARLviKw6E5SY8.
   > Are you sure you want to continue connecting (yes/no)?

3. Verify that the fingerprint in the message you see matches GitHub's public key fingerprint. If it does, then type yes:

   > Hi USERNAME! You've successfully authenticated, but GitHub does not
   > provide shell access.

   Note: The remote command should exit with code 1.

4. Verify that the resulting message contains your username. If you receive a "permission denied" message, see "Error: Permission denied (publickey)".
Case Study: Secure Messaging

Server

public (X.509 certificate)

(\(\text{VKS, SKS} \leftarrow \text{Gen(1}^n\right)\))

1. \(\text{Encrypt}(g^a, \text{Bob})\)
2. \(\text{Encrypt}(g^b, \text{Alice})\)
3. \(\text{Server} \xrightarrow{\text{Signup}} \text{Login} \xrightarrow{\text{Login}} \text{Secure Messaging} \xrightarrow{\text{Encrypt}(ct, \text{Alice})}\)

Alice

Bob

\(\downarrow \quad \text{g}^a \quad \downarrow \text{HKDF} \quad \downarrow k\)

\(\downarrow \quad \text{g}^b \quad \downarrow \text{HKDF} \quad \downarrow k\)

How would you design it?

6. \(ct \leftarrow \text{Enc}_k(m)\)
Group Chat?

Server

```
(public (X.509 certificate))
```

```
(VKs, SKs) ← Gen(1^n)
```

```
- m revealed to server?
- group structure revealed to server?
- all same key / pairwise keys?
```

Alice

```
Signup
Login
```

```
Signup
Login
```

Charlie

```
Signup
Login
```

```
Signup
Login
```

Bob

How would you design it?
Figure 5. Schematic depiction of traffic, generated for a message $m$ from sender $A$ to receivers $B, C$ in group $gr$ with $\mathcal{G}_{gr} = \{A, B, C\}$ in WhatsApp.
Figure 3. Schematic depiction of Signal’s traffic, generated for a message $m$ from sender $A$ to receivers $B$ and $C$ in group $gr$ with $G_{gr} = \{A, B, C\}$. Transport layer protection is not in the analysis scope (gray).
Case Study: Single Sign-On (SSO) Authentication

User → Password-Based Authentication ← Server

Request "token"

"token" (Signature / MAC)

MAC → Signature

Service Provider

"token"

k → VK

- OAuth / OpenID: Sign-in with Google / Apple / Brown /...
- Kerberos: enterprises
Zero-Knowledge Proofs

Prover

Verifier

Coke & Pepsi
taste differently

There is a bug in your code

I have the secret key for this ciphertext

What is a proof?

What does zero-knowledge mean?
What is a "proof system"?

<table>
<thead>
<tr>
<th>Statement: _____</th>
</tr>
</thead>
<tbody>
<tr>
<td>proof: __________</td>
</tr>
</tbody>
</table>
| _________________ ☐

- Completeness: If the statement is true, then \( \exists \text{ proof that proves it's true} \).
- Soundness: If the statement is false, then \( \forall \text{ proof can't prove it's true} \).
Zero-Knowledge Proof (ZKP)

Let \((P, V)\) be a pair of probabilistic poly-time (PPT) interactive machines. \((P, V)\) is a zero-knowledge proof system for a language \(L\) with associated relation \(R_L\) if

- **Completeness:** \(\forall (x, w) \in R_L, \Pr[P(x, w) \leftrightarrow V(x) \text{ outputs } 1] = 1\).
  \[\forall (x, w) \in R_L, \text{ P can prove it.}\]

- **Soundness:** \(\forall x \notin L, \forall p^*, \Pr[P^*(x) \leftrightarrow V(x) \text{ outputs } 1] \approx 0\).
  \[\forall x \notin L, \text{ any } p^* \text{ cannot prove it.}\]