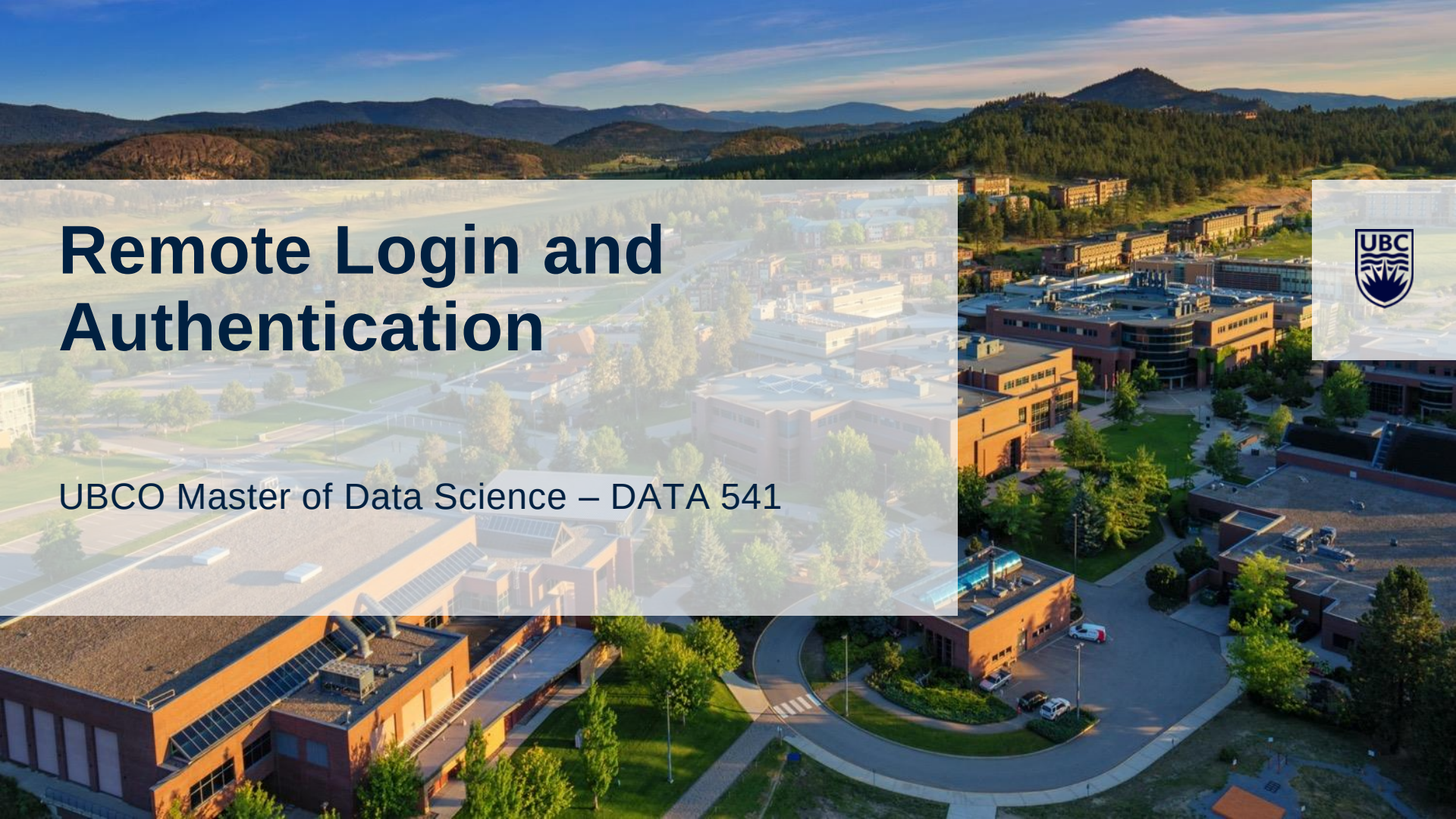


Remote Login and Authentication

UBCO Master of Data Science – DATA 541

Today's Class

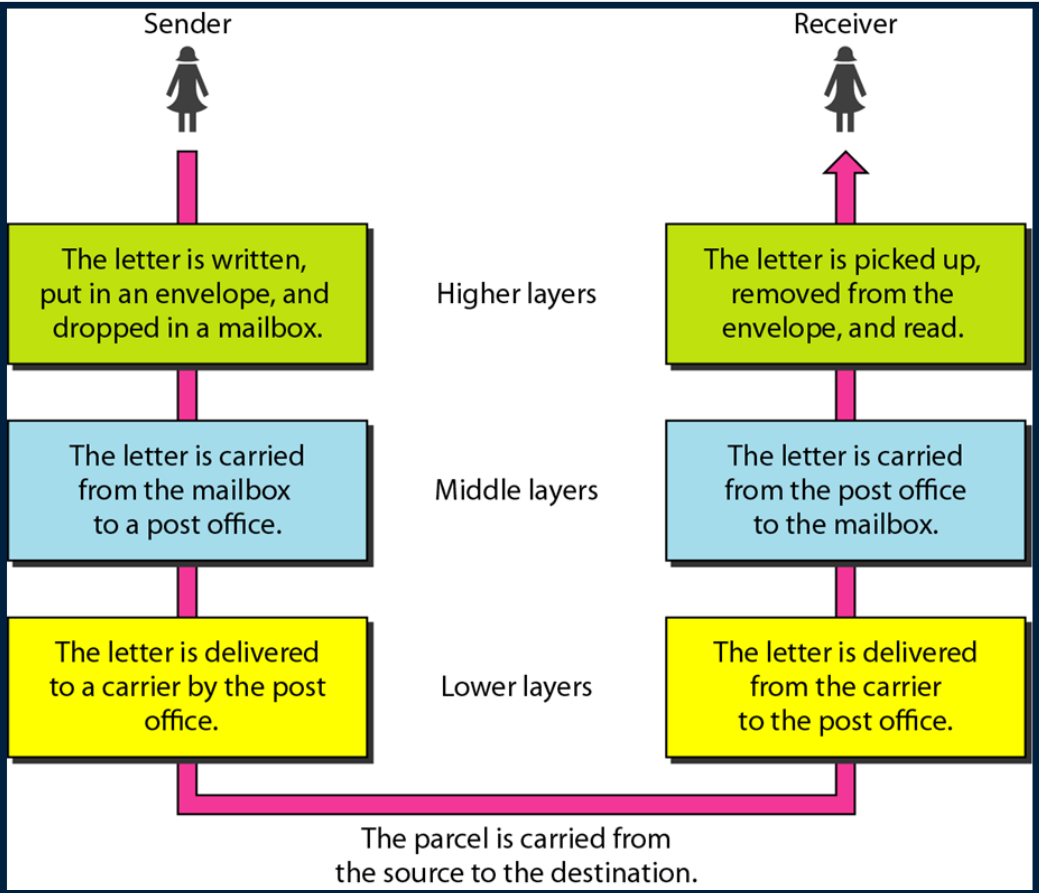
Brief History

Remote Login with SSH

Public Key, Private Key

Security Mechanism

Tasks involved in sending a letter



Remote Access

Computers can communicate between themselves

Each computer has a unique ID (e.g., IP Address, MAC/Physical Address)

Addresses

Physical Address: Media Access Control (MAC) address

Logical Address: IP address

Post address: TCP/UDP, Port number

Physical address

12-digit hexadecimal number assigned to each device connected to the network

MAC address is often found on a device's network interface card

Every byte (2 hexadecimal digits) is separated by a colon or dash, as shown below:

07-01-02-01-2C-4B

12 hexadecimal digits physical address.

How to find the MAC address

Windows

- Go to command prompt
- Type ipconfig/all, and hit Enter
- look for a value description of the Physical Address field

Mac

- Click on the Apple icon, and select System Preferences.
- Select Network
- Select the list the interface and click on Advanced.
- Click on the Hardware tab, and find the MAC address.

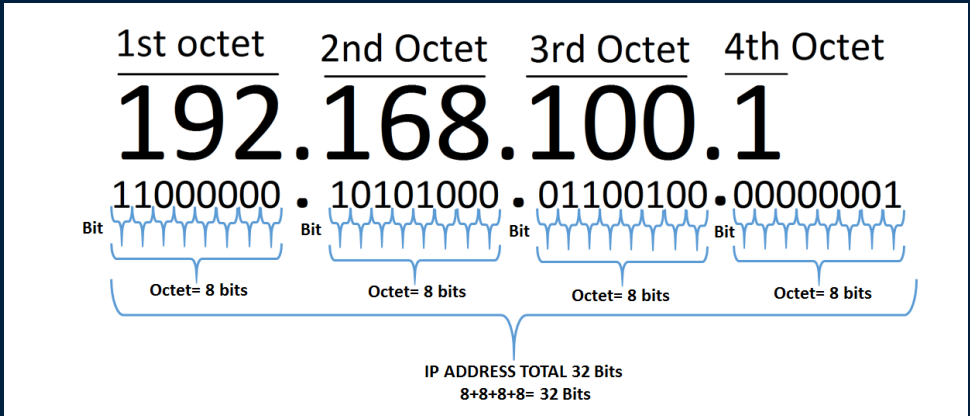
Linux

- Open a terminal or console window.
- Type ifconfig.
- The MAC address is listed as ether

IP Address

IPv4

- An IP address consists of 4 “octets”
- Each “octet” consists of numbers between 0 and 255
  - Example: 206.87.25.100
- It works like the phone system, with “area codes” to the left, then “prefix” etc
- A computer knows that “206.87.38.” means “UBC Okanagan”



IP Address Question

Question: Find the correct dotted-decimal notation for the following IPv4 addresses presented in binary notation:

10000001 00001011 00001011 11101111

A) 129.11.11.240

B) 129.11.11.239

C) 129.11.11.238

D) 129.11.11.236

E) None of the above

IP Address

Question: How many of the following are **CORRECT** IP addresses?

1) 111.56.278.78
2) 221.34.7.8.20
3) 75.45.301.14
4) 11101110.23.14.67

A) 0 **B)** 1 **C)** 2 **D)** 3 **E)** 4

Network classes

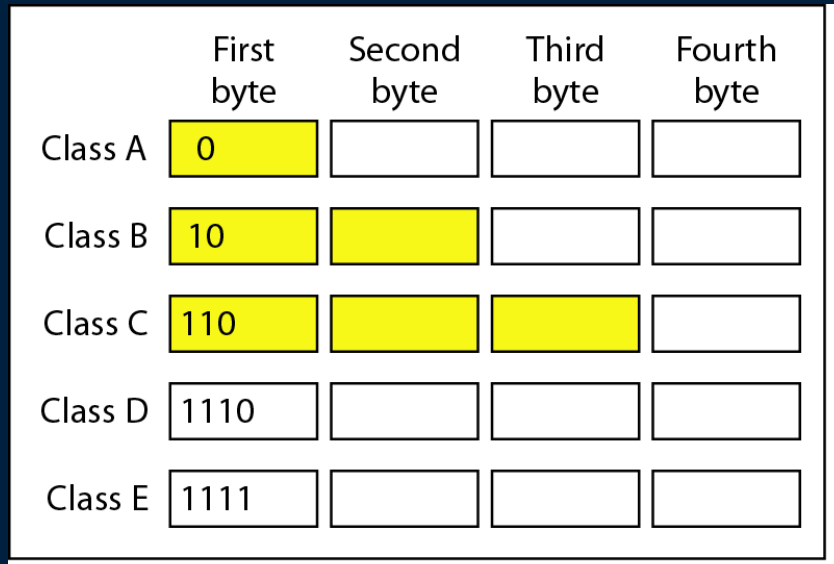
IP addresses are divided into classes.

The most common of them are classes A, B, and C. Classes D and E exist, but aren't used by end users.

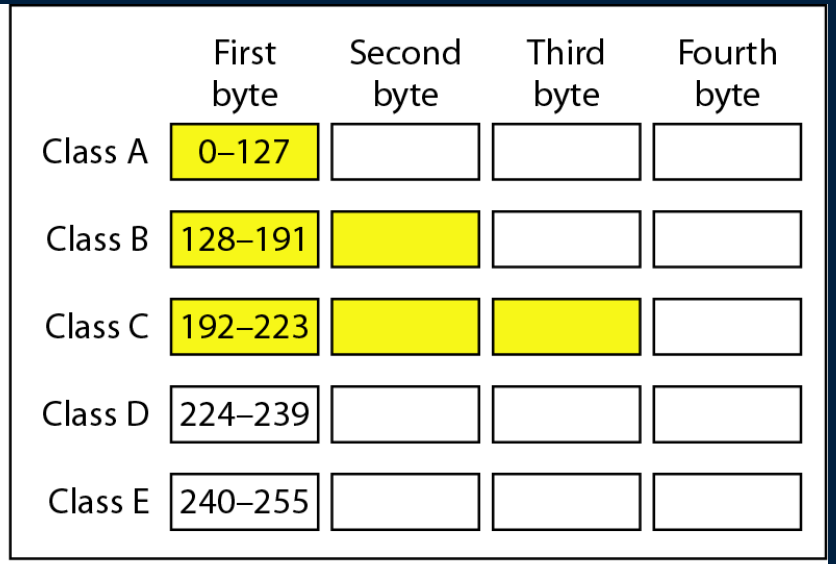
Following are the ranges of Class A, B, and C Internet addresses

- Class A networks have 0-127 as their first octet. The address 10.52.36.11 is a class A address.
- Class B networks have 128-191 as their first octet. The address 172.16.52.63 is a class B address.
- Class C networks have 192-223 as their first octet. The address 192.168.123.132 is a class C address.

Finding the classes in binary and dotted-decimal notation



a. Binary notation



b. Dotted-decimal notation

Class D: multicast
Class E: reserved

Classless addressing

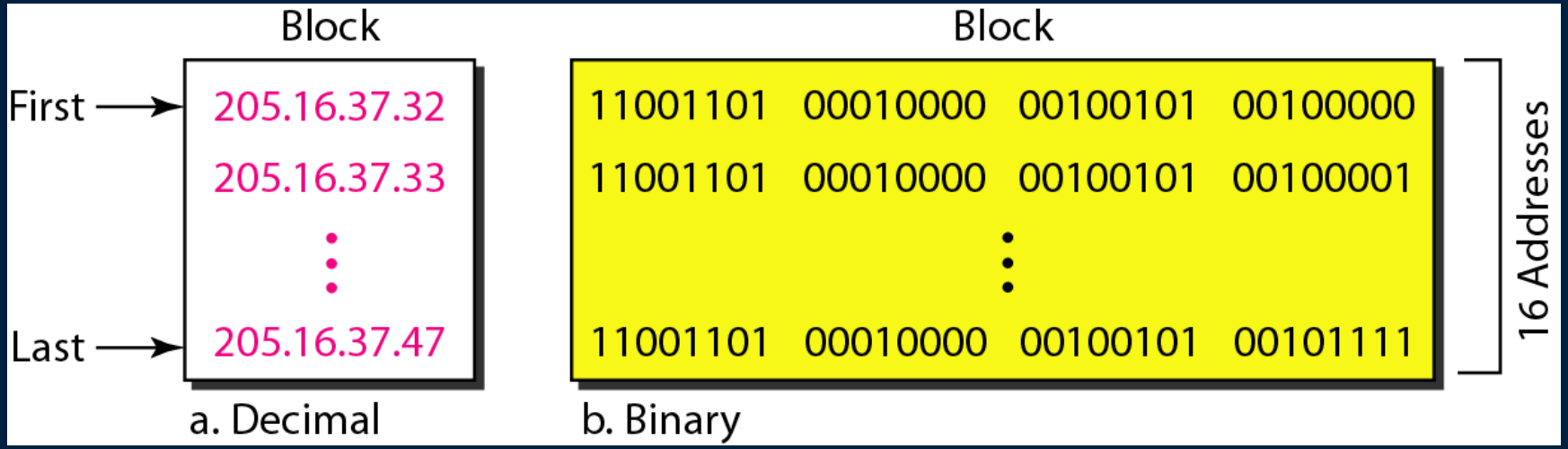
In classful addressing, a large part of the available addresses were wasted.

Classful addressing, which is almost obsolete, is replaced with classless addressing.

In IPv4 addressing, a block of addresses can be defined as x.y.z.t /n in which x.y.z.t defines one of the addresses and the /n defines the mask.

Classless addressing

A block of 16 addresses granted to a small organization



Question

A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first address in the block?

Solution

The binary representation of the given address is

- 11001101 00010000 00100101 00100111

If we set 32−28 rightmost bits to 0, we get

- 11001101 00010000 00100101 0010000
- or 205.16.37.32.

Question

205.16.37.39 = 11001101 00010000 00100101 00100111 (represented in binary)

/28 can be = 11111111 11111111 11111111 11110000 (represented in binary)

The first address can be found by AND-ing the given addresses with the mask.

ANDing here is done bit by bit.

The result of AND-ing 2 bits is 1 if both bits are 1s;

the result is 0 otherwise.

Address:	11001101	00010000	00100101	00100111
Mask:	**11111111**	**11111111**	**11111111**	**11110000**
First address:	11001101	00010000	00100101	00100000

Question

The last address can be found by ORing the given addresses with the complement of the mask.

The complement of a number is found by changing each 1 to 0 and each 0 to 1.

OR-ing here is done bit by bit.

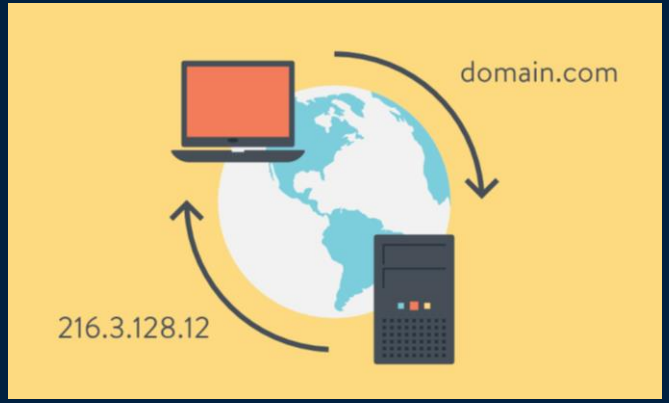
The result of ORing 2 bits is 0 if both bits are 0s; the result is 1 otherwise.

Address:	11001101	00010000	00100101	00100111
Mask complement:	**00000000**	**00000000**	**00000000**	**00001111**
Last address:	11001101	00010000	00100101	00101111

Domain Name System (DNS)

DNS

- People find it easier to remember names instead of numbers
- A DNS associates an IP address to a name.
- DNS servers are responsible for translating textual Internet addresses into numeric Internet addresses.
- nslookup is used to find DNS records



Networking Basic Question

Question: How many of the following statements are **TRUE**?

1) DNS converts a name into an IP address
2) 236.276.201.32 is a valid IP address
3) An IP address consists of 32 bits
4) MAC address is unique for every device

A) 0 **B)** 1 **C)** 2 **D)** 3 **E)** 4

Remote Login

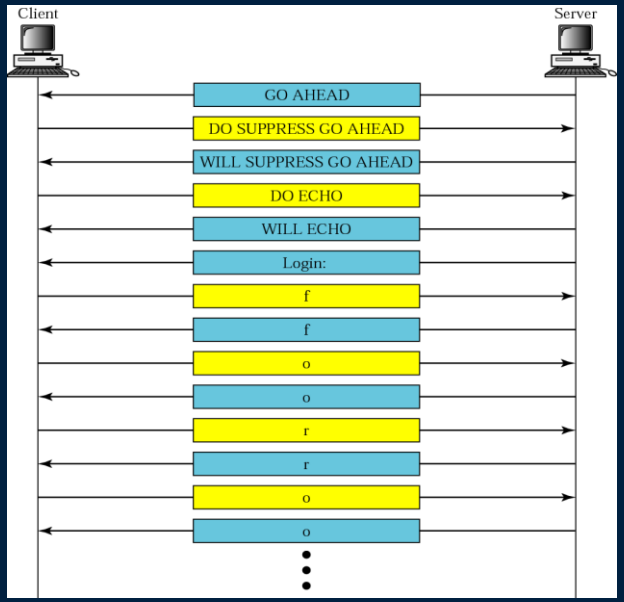
There are many utilities to login through a network in Unix environment

- Example: telnet
- Limitation: information are transmitted as clear text

Telnet connection is unencrypted

- So easy for eavesdropper!

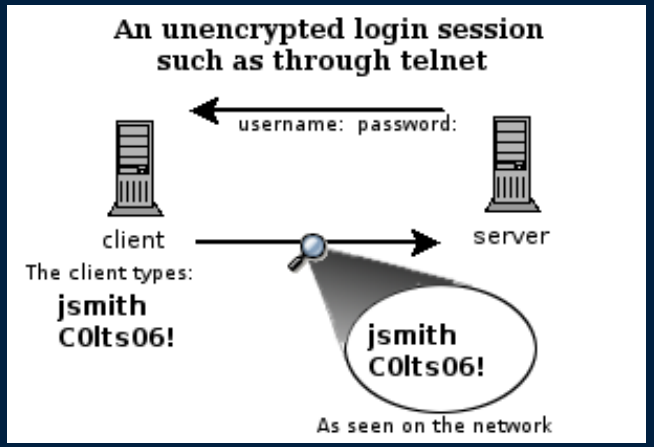
In most cases, telnet is a remote terminal. Each character is transmitted in a separated packet

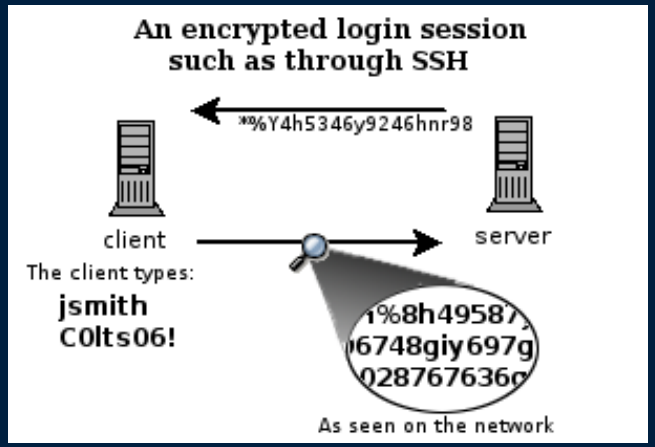


History

Secure Shell was created in 1995 by Tatu Ylönen

- In response to a password-sniffing attack at his university
- To eliminate the flaws in plain text communication
- A strong emphasis on encryption and security





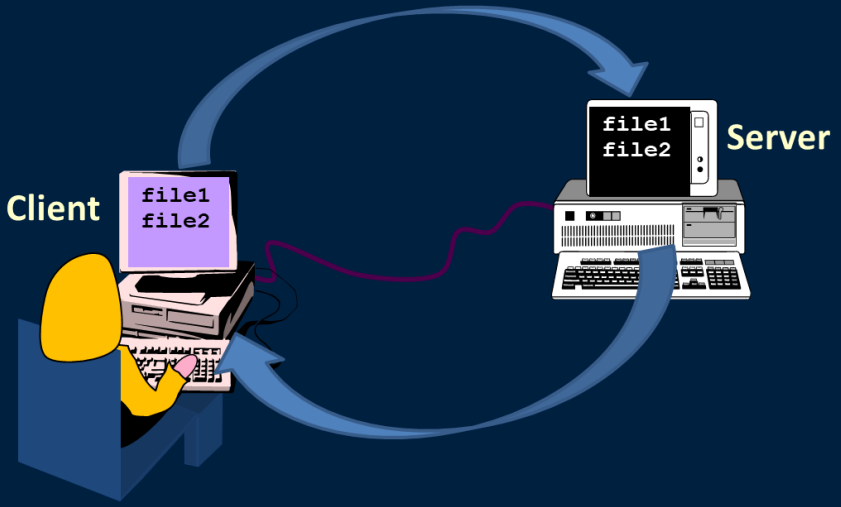
Accessing Computer Remotely

SSH which is an acronym for Secure SHell

Designed to provide the best security when accessing another computer remotely

It provides

- Secure remote logins
- Secure remote command execution
- Secure file transfers
- Better authentication facilities



Secure CoPy (SCP)

- A method of securely transferring files between computers which uses SSH for data transfer and authentication

SSH – Secure Shell

Replacement of old unsecure Telnet program

Both ends authenticate with each other

Rely on public key cryptography

All communication messages are encrypted

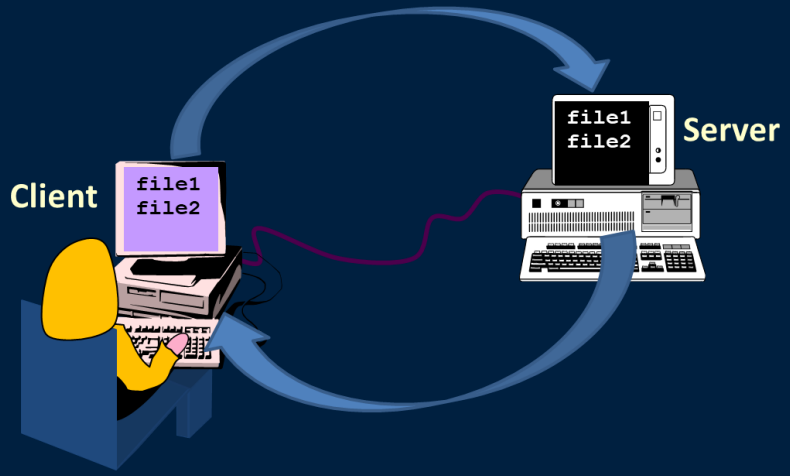
SSH is used also as a secure tunneling channel for other applications

- File transfer
- Virtual private network (VPN)

Client vs. Server

Server

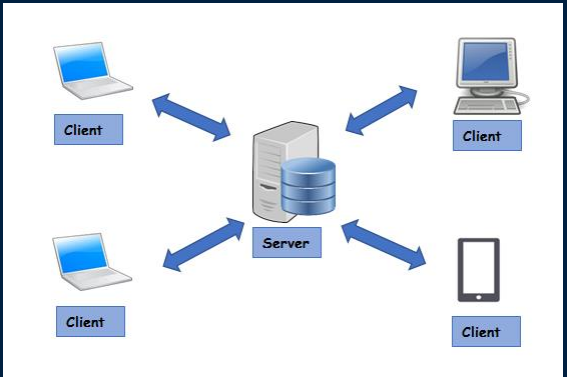
- A remote that your computer can ask questions to, and obtain answers from.
- A system that provides services to other systems in its network
- There are file servers, database servers, license servers, print servers, and even servers for particular applications.



Client vs. Server

Client

- Usually your local machine. The client initiates contact with the server.
- A system that uses remote services from a server.
- E.g., Some clients have limited disk storage capacity and they have to rely on remote file systems from a server to function.



Password-Based Authentication

Passwords are short and tend to be somewhat easy to "break" (guess).

- Say your password contains 12 characters
- Each character is one of 26 uppercase letters, 26 lowercase letters, 10 digits, or ~10 special characters
- Total probably around ~70 possibilities per character
- https://projects.lambry.com/elpassword/
- This is a HUGE number, except that there are patterns within passwords that make them easier to guess

Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345

SSH Key-Based Authentication

SSH key pairs are two cryptographically secure keys that can be used to authenticate a client to an SSH server.

Each key pair consists of a public key and a private key to encrypt and decrypt data.

SSH Key-Based Authentication

Public Key:

- Used to encrypt data that only the private key can decrypt
- Commonly uploaded to a remote server

Private Key:

- Used to encrypt and decrypt code
- Kept at the client side

SSH and Client-Server Question

Question: How many of the following statements are **TRUE**?

1) SSH transmits data as clear text
2) Secure CoPy (SCP) is primarily used for login to a remote computer
3) Server machine is usually your local machine
4) SSH was created in response to a password-sniffing attack

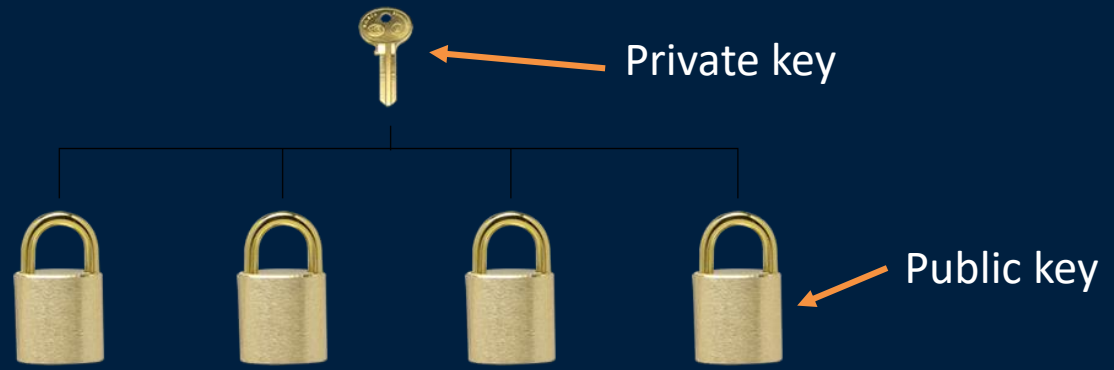
A) 0 **B)** 1 **C)** 2 **D)** 3 **E)** 4

Understanding Key Concepts

Think of a public key, not as a key, but as a padlock that you can make copies of and put anywhere you want.

To put your padlock on another machine, you would copy it to `authorized_keys` in the `~/.ssh` folder.

Think of a private key as an actual key, it can open the padlock that is stored on the other machine.



How The Lock Works

Keys are generated using `ssh-keygen -t rsa`

A private key, usually called `id_rsa` and a public key, usually called `id_rsa.pub`

You can make copies of `id_rsa.pub` (public key/padlock) and distribute them to other machines

The other machine uses the public key to encrypt a challenge message

You need to show that you can decrypt the message to demonstrate that you are in possession of the associated private key

Creating Keys

Use the following command to create a key pair

```
ssh-keygen -t rsa
```

```
khalad@A4005069:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/khalad/.ssh/id_rsa):
/home/khalad/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/khalad/.ssh/id_rsa.
Your public key has been saved in /home/khalad/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:u1D9uff8hvL1Tkb0VN6aBkffYLjRJH3bDNZOoaDhYMY khalad@A4005069
The key's randomart image is:
+---[RSA 2048]----+
|      .+ . ..==oo|
|      oEo o ++*+B|
|         o  .=.*X|
|          .  .o *=|
|        S .   + o|
|       . . . o . |
|      . .   o  .+|
|       . .  ..o=o|
|         .   .+.+B|
+----[SHA256]-----+
```

File Location

Creating Keys

Command to check all folder (including hidden): ls -a

Navigate to the SSH folder : `cd ~/.ssh/`

- `id_*` - private authentication keys
- `id_*.pub` – public authentication keys
- `known_hosts` – list of known public host keys
- `authorized_keys` – list of allowed public authentication keys

Creating Keys

Public Key: `id_rsa`: Contains your private key

```
cat id_rsa
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC1QyK5UsoMttRS0OThYEQOquZO/+rFBMvSC4Qaa
Q9laytPxiiILW4LLM5MTtJ/QxeEmMA6Uvmufo24IH2jhCr9BlVpdpv1pSK7cWJPcGmmRPu00CXp8M
```

Private Key: `id_rsa.pub`: Contains your public key

```
cat id_rsa.pub
```

```
MIIEowIBAAKCAQEAtUMiuVLKDLbUUtDk4WBEDqrmTv/qxQTL0guEGmoWJueHk6Fm
Nw2Vc/FX2MBR2HSJvVMU3QEbDfEbaANoV0PZWsrT8YoiC1uCyzOTE7Sf0MXhJjAO
lL5rn6NuCB9o4Qq/QZVaXab9aUiu3FiT3BppkT7tNAl6fDMYvX/s1D6qM0xIjhab
```

Installing Public Key on the Server

We can use either the following commands to copy the public key file on the remote server.

```
ssh-copy-id RemoteServer
```

```
khalad@A4005069:~$ ssh-copy-id mkhasan@s159.ok.ubc.ca
```

or

```
scp $HOME/id_rsa.pub RemoteServer :~/.ssh/authorized_keys
```

*** RemoteServer is user@hostname.example.com

Login and File Transfer

Login to the server

```
$ ssh username@remotehost
```

Allows encrypted transfer of files between machines

Download files from server:

```
$ scp username@remotehost.edu:file.txt /some/local/directory
```

Copy a file from a local host to a remote host (Upload files to a server)

```
$ scp file.txt rsername@remotehost.edu:/some/remote/directory
```

Public and Private Keys Question

Question: How many of the following statements are **TRUE**?

1) A public Key is used to encrypt data

2) A private key kept at client side

3) It's safe to distribute the `id_rsa` key to other machines

4) A private key, usually called `id_rsa` and a public key, usually called `id_rsa.pub`

A) 0 **B)** 1 **C)** 2 **D)** 3 **E)** 4

Try it: SSH Key-Based Authentication

1. Generate a key pair using the command `ssh-keygen`
2. Install the public key on the remote machine

   Server IP address: 159.203.60.51
3. Login to the server using SSH
4. Write and execute a script on the server machine
5. Download the script to your local machine

Objectives

- Understand networking basics
- Understand public and private key concepts
- Access a remote machine with SSH
- Authenticate a client to a remote server
- Understand secure file transfer mechanisms


UBC
THE UNIVERSITY OF BRITISH COLUMBIA