COSC 301
Network Management and Security

Lecture 13: Remote Terminal Services and SSH

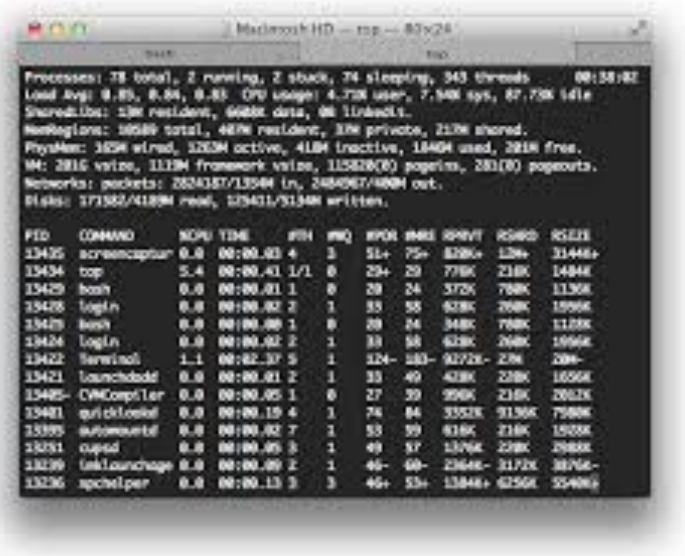
What is a terminal?

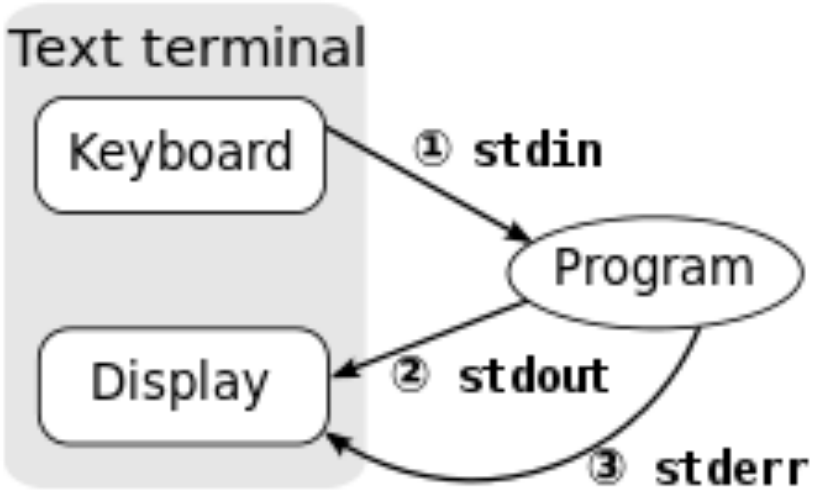
- Original terminals
  - TeleTYpewriter (TTY)

  - DEC VT-100 terminal

What is a terminal? (cont.)

- Terminal emulator
  - a program that does what an original terminal used to do
  - Terminal window





Remote TTY after Internet

- Berkeley ‘r’-commands
  - rsh remote shell commands
  - rlogin remote terminal
  - rcp remote copy
  - No password needed as the authentication is host-based
- Telnet
  - Remote terminal, similar to rlogin
  - User-based authentication
  - Clear text password

Problems

- Everything sent in clear-text, no encryption
- Weak Host-based authentication
  - Exploitable trust relationships
  - Privileged ports offer little protection
- Server not authenticated
  - Man-in-the-middle (MITM) attack potential

Solutions

- Encrypt all traffic
- Authenticate both user and server
- This is where SSH comes in

Secure SHell (SSH)

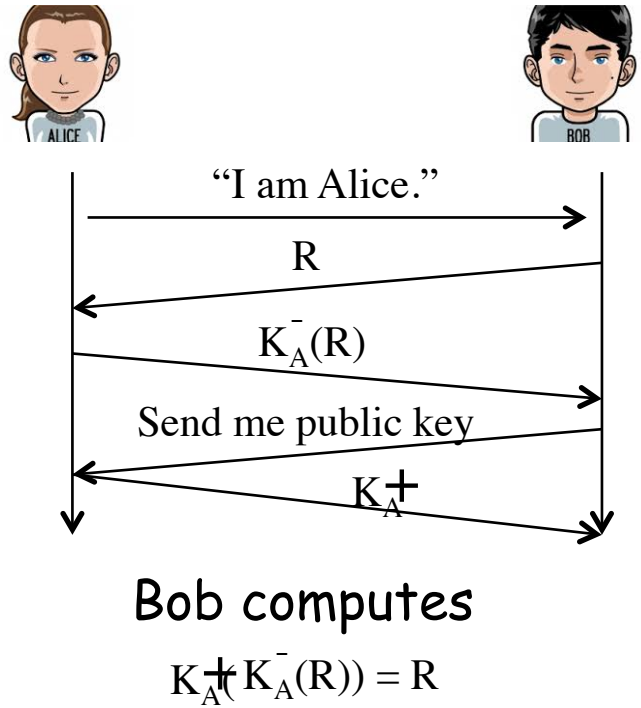
- SSH provides secure versions of the ‘r’-commands and telnet
- Encrypts all traffic
  - Public/Private Key for authentication
  - Fast block cipher for data transfer
- Authenticate both server and client/user

Public Key Encryption

- Choose two prime numbers p and q, N=p x q
- Generate e and d according to p and q so that
  - For any message/number M,
  - M^{exd} mod N = M
- Modulo property
  - M^{exd} mod N = $(M^e \text{ mod } N)^d$ mod N = M
- Encryption: e is public key, N is publicly known
  - C = M^e mod N
- Decryption: d is private key
  - C^d mod N = $(M^e \text{ mod } N)^d$ mod N = M
- N is a very large number so factor N is time consuming.

Authentication with PKI

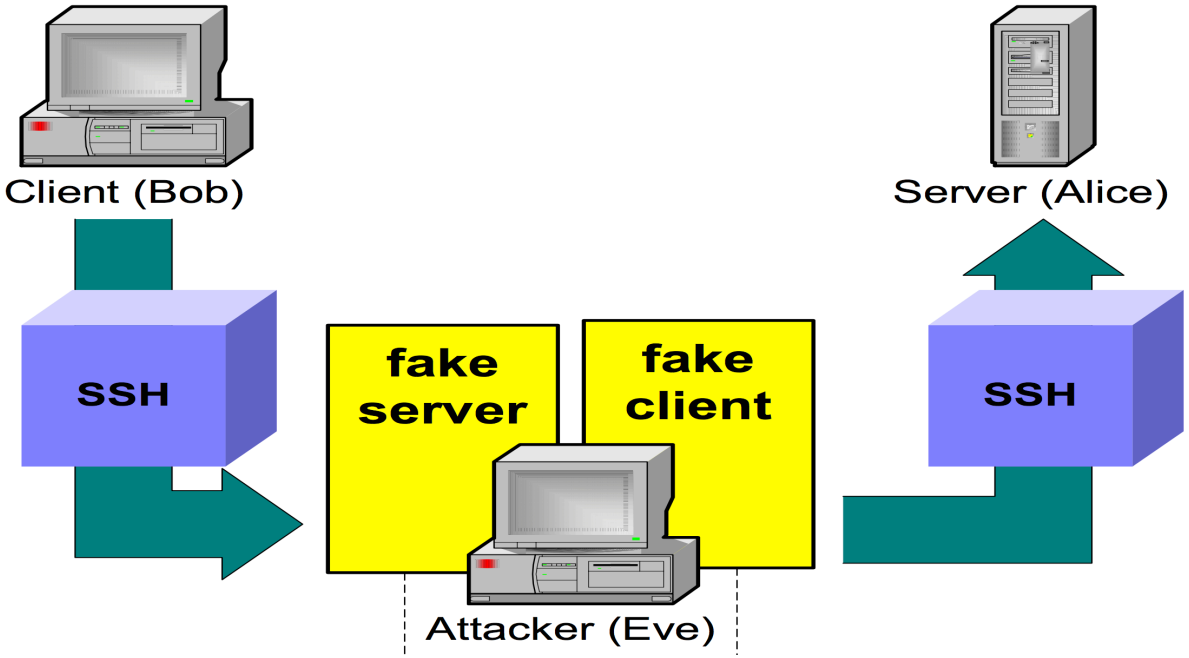
- AP5.0
  - Use the public key encryption in AP4.0
  - The protocol has the following procedures
    - Alice sends "I am Alice", to Bob
    - Bob sends a nonce, R, to Alice
    - Alice encrypts the nonce using Alice's private key A and sends the encrypted nonce back to Bob
    - Bob decrypts the received message using Alice public key. If the decrypted nonce equals the nonce he sent Alice, then Alice is authenticated.



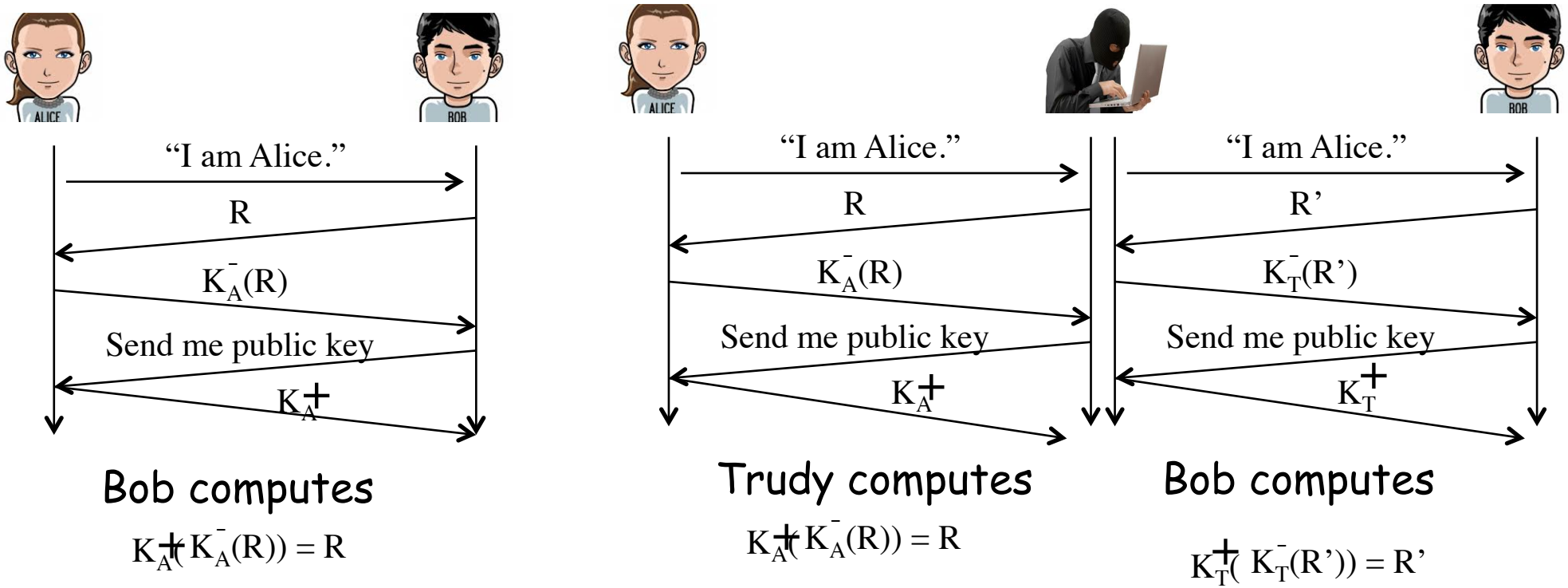
The retrieval of the public key could be a security hole

MITM

- Man-in-the-middle attack (MITM)
  - Can it happen with public key encryption?
  - If so, how?



MITM under PKI



If Bob does not verify the public key sent by Trudy, MITM attack establishes

How to prevent MITM?

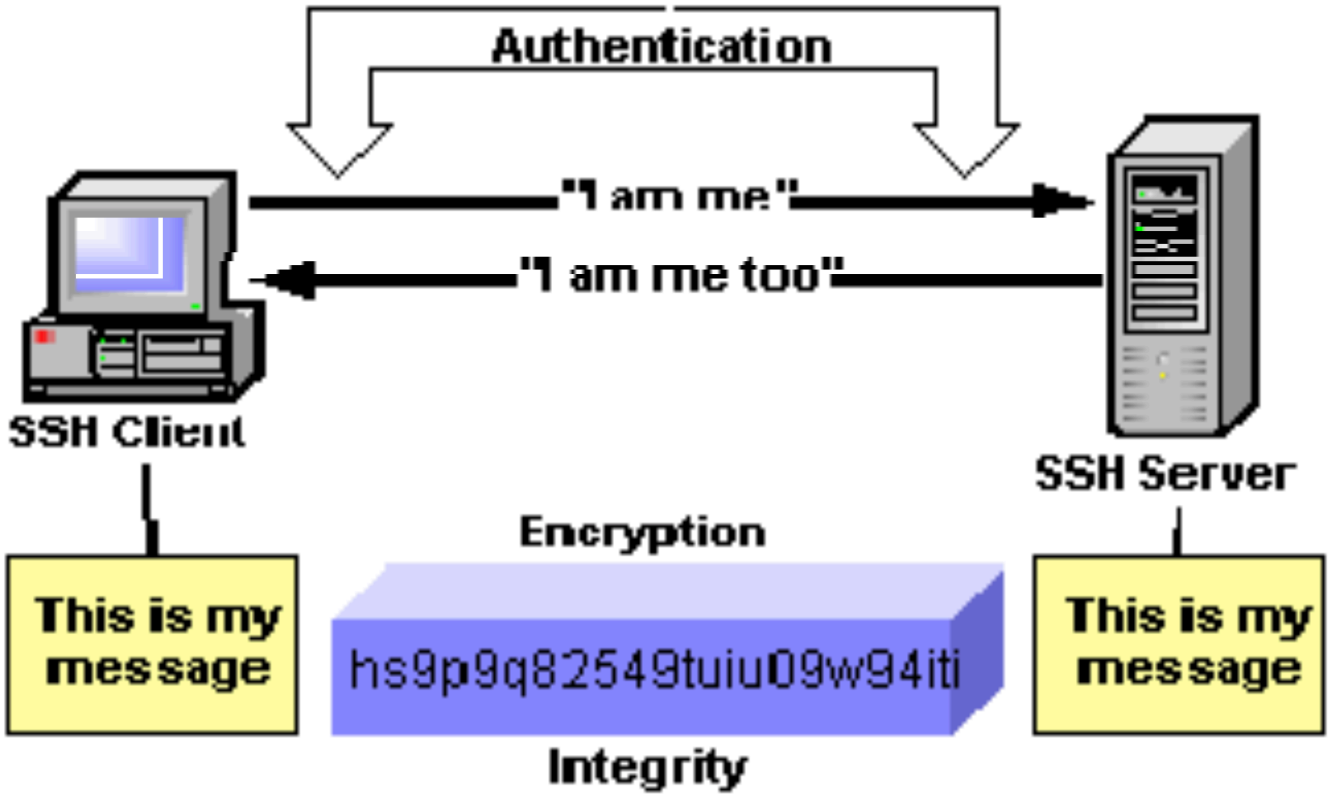
- Verify the host/user public key

```
-bash-4.2$ ssh hzy@vertex.otago.ac.nz
The authenticity of host 'vertex.otago.ac.nz (10.81.166.21)' can't be established.
ECDSA key fingerprint is SHA256:z9M2TMCOyl0hCrcsvMcxLevUs7xEs0Pw/bsA7Fg94GU.
ECDSA key fingerprint is MD5:72:5f:bd:d4:e2:21:87:c6:b1:51:65:18:a9:1f:09:ea.
Are you sure you want to continue connecting (yes/no)?
```

  - You can use ssh-keygen to find out the fingerprint of a public key
  - E.g. ssh-keygen –lf ssh_host_dsa_key.pub
- Store the public key of your trusted server into the known_hosts file under .ssh directory

Basics of SSH

- User Authentication
- Host Authentication
- Data Encryption
- Data Integrity



Keys in SSH

- User Key
  - A persistent, asymmetric key used by clients as proof of a user's identity.
  - A single user may have multiple keys
- Host Key
  - A persistent, asymmetric key used by a server as proof of its identity
  - Used by a client when proving its host's identity as part of trusted-host authentication
- Session Key
  - A randomly generated, symmetric key for encrypting the communication between an SSH client and server.
  - It can be changed during a session

Data Encryption/Integrity

- Encryption
  - Use ciphers to encrypt and decrypt data being send over the wire
  - Block cipher such as DES, 3DES, use a shared key (session key)
  - Agree which cipher use during connection setup
  - Session keys are randomly generated by both the client and server, after host authentication and before user authentication
- Integrity
  - Message Authentication Code (MAC) in SSH2
  - Simple 32-bit CRC in SSH1

User Authentication

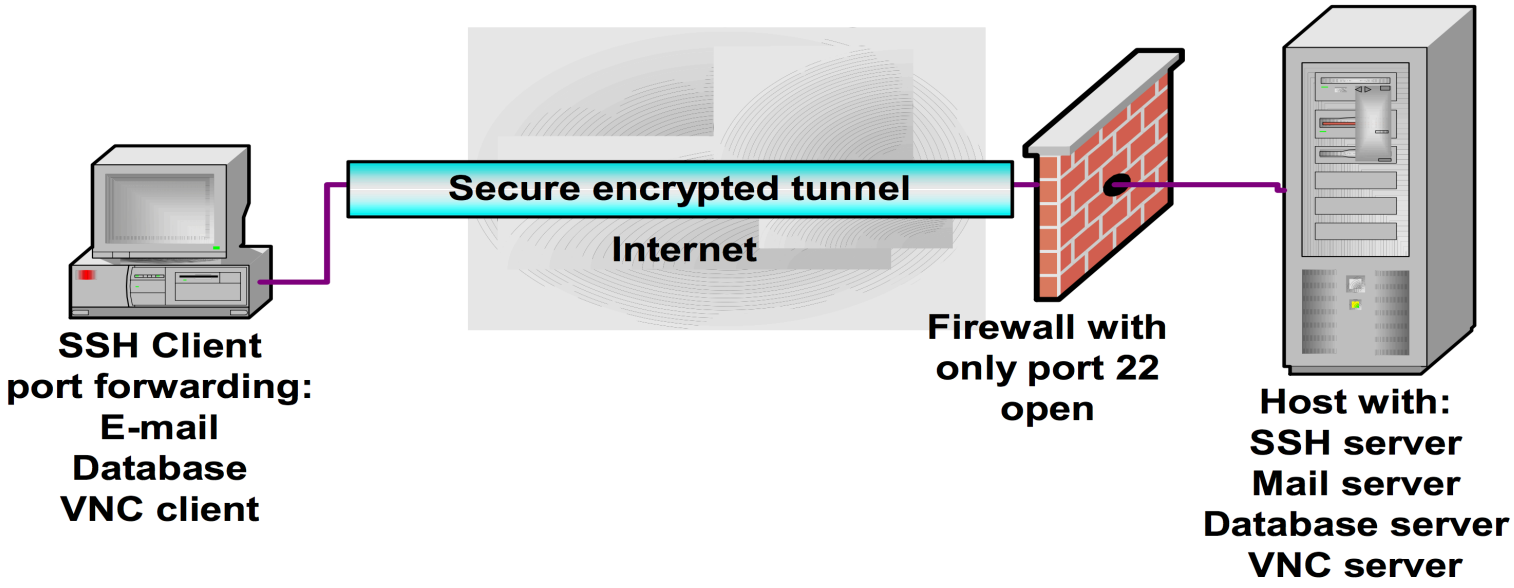
- Password authentication
  - The username and password are encrypted before transmission.
  - Inherently vulnerable in that they can be guessed
- Public key authentication
  - Public key and private key: generated using ssh-keygen
  - Private key should never be distributed, and should be protected by “passphrase”

Functionality of SSH (1)

- Secure Command Shell: anything that can be done at a local machine can be done securely remotely

Functionality of SSH (2)

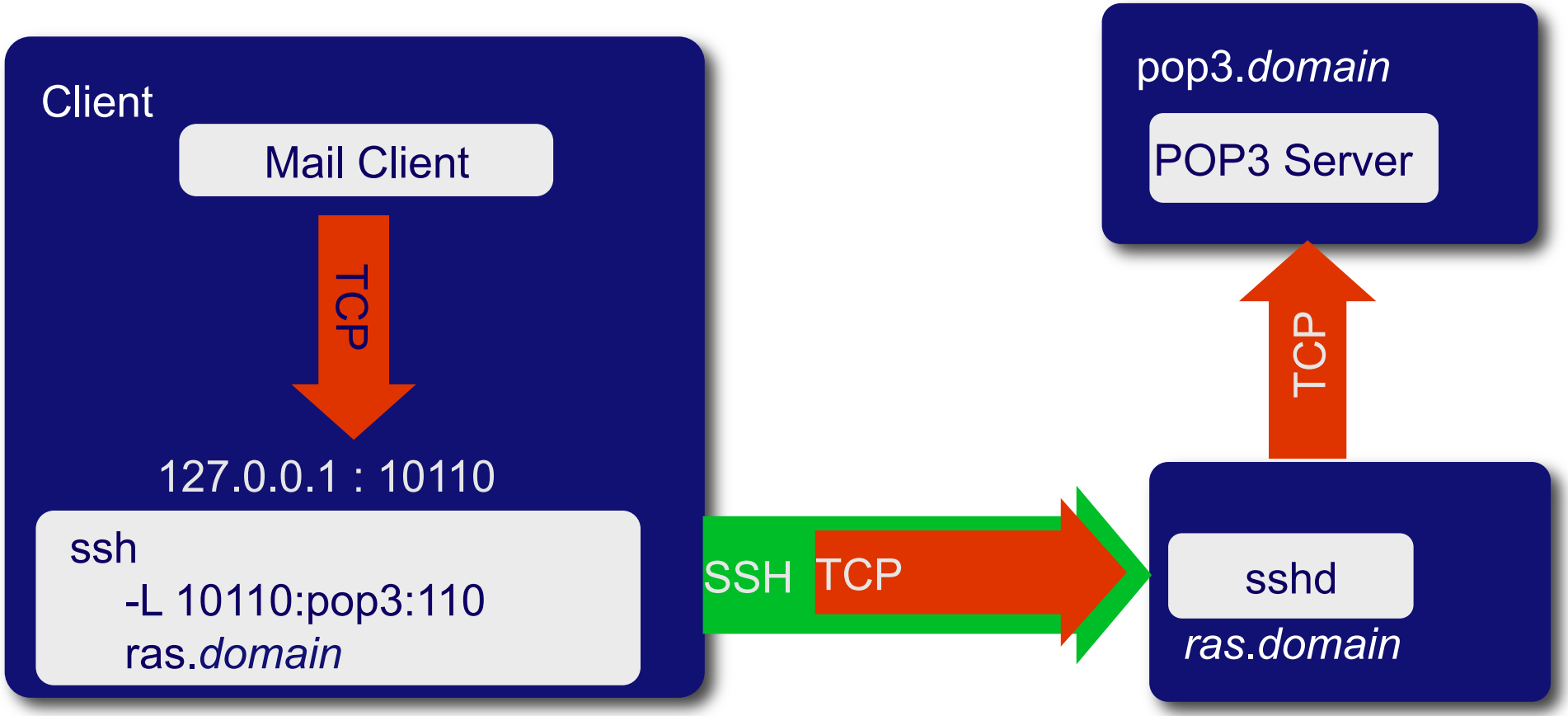
- Port forwarding
  - allows data from normally unsecured TCP/IP applications to be securely sent across the encrypted tunnel,
  - multiple applications can transmit data over a single multiplexed channel.



Ref: An Overview of the Secure Shell (SSH), Vandyke Software

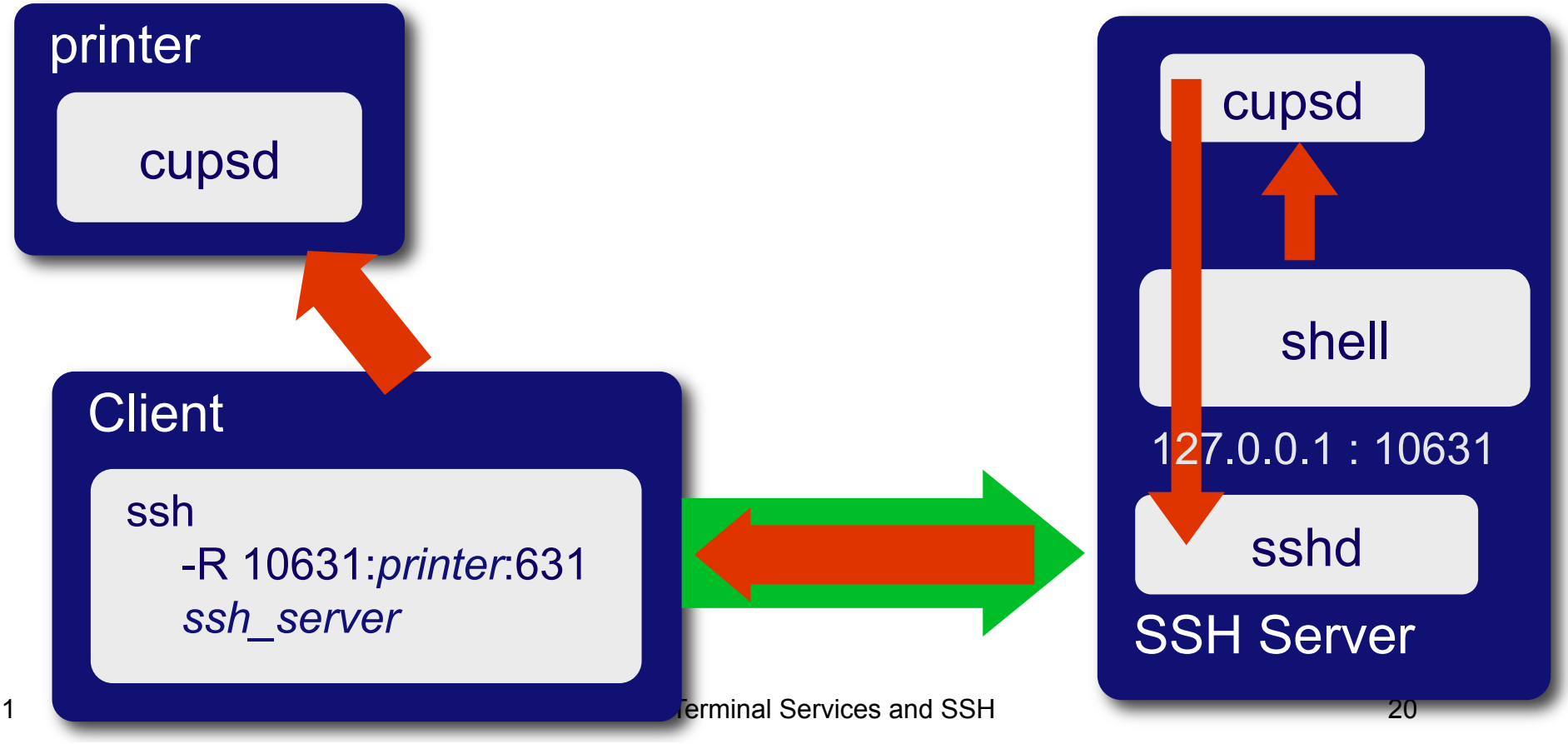
Functionality of SSH (3)

- Port forwarding
  - Local port forwarding: forward data securely from another client application running on the same computer as the Secure Shell Client



Functionality of SSH (4)

- Port forwarding
  - Remote port forwarding: enables applications on the server side of a Secure Shell connection to access services residing on the SSH's client side.



Functionality of SSH (5)

- Secure File Transfer
  - Secure copy (SCP): RCP protocol over SSH.
  - Rsync: intended to be more efficient than SCP
  - SSH File Transfer Protocol (SFTP): a secure alternative to FTP (not to be confused with FTP over SSH)
  - Files transferred over shell protocol (FISH): evolved from Unix shell command over SSH

Threats Addressed by SSH

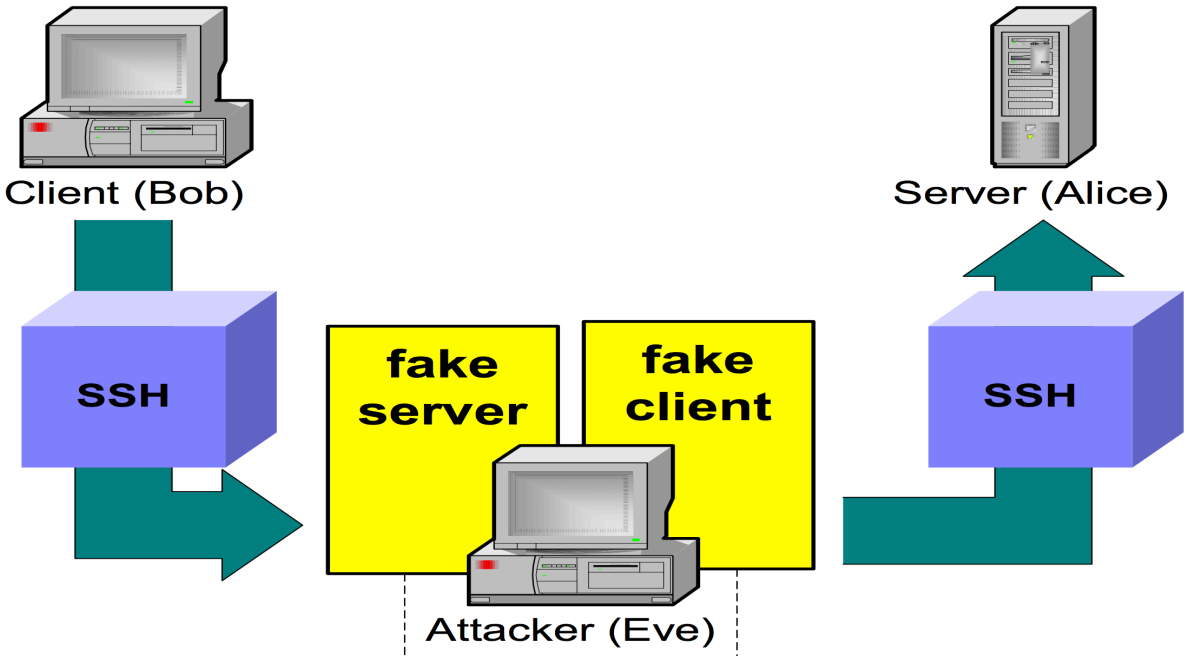
- Insertion and Replay attack
  - Attacker is not only monitoring the SSH session, but is also observing the encrypted keystrokes
  - The attacker could replay the activities of the whole session, even they are encrypted.
  - But authentication and digital signature prevent such attacks.

SSH Doesn't Prevent

- Password Cracking
- IP and TCP attacks
- Traffic Analysis

Threats Addressed by SSH

- Eavesdropping or Password Sniffing
  - All transmitted data is encrypted
- Man-in-the-middle attack (MITM)
  - Cannot happen unless the hosts involved have been compromised or accept a public key without verifying it.



Summary

- SSH port forwarding: local and remote
- Can MITM attack happen with SSH? If so, how?