COSC301
Network Management and Security

Lecture 13: Remote Terminal Services

Today's Focus
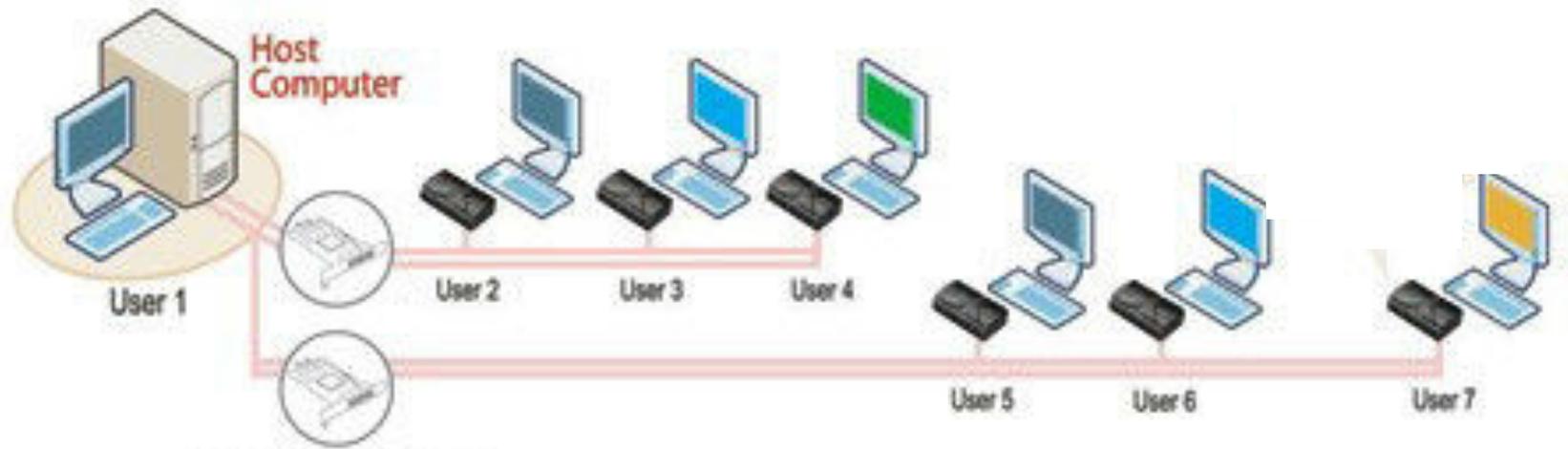

Remote Terminal Services
-- What is a remote terminal?
-- Secure SHell (SSH)

What is a terminal?

- An electronic device used for entering data into, and displaying data from a computer
  - Dumb terminal (thin client): no local processing ability
  - Smart terminal (fat client): has local processing ability

What is a terminal?
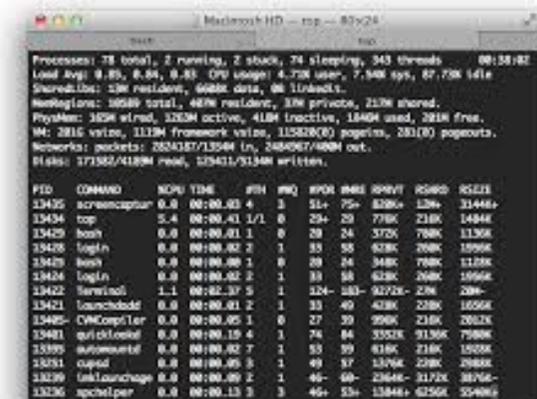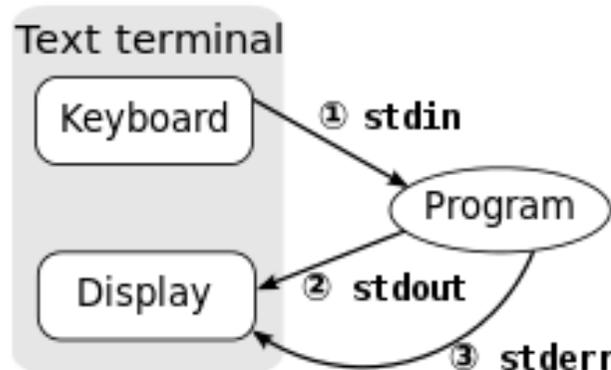
- ## Hard-copy terminals

  TeleTYpewriter (TTY)   DEC VT-100 terminal

- ## Terminal emulator
  – a program that does what a dumb terminal used to do
  – Terminal window

TTY Remote History

- **Berkeley 'r'-commands**
  - rsh   remote shell commands
  - rlogin   remote terminal
  - rcp   remote copy

> **Weak host-based authentication**
> **Privileged ports, .rhosts, no password**

- **Telnet**
  - Remote terminal, similar to rlogin
  - User-based authentication

Past Problems & Solutions

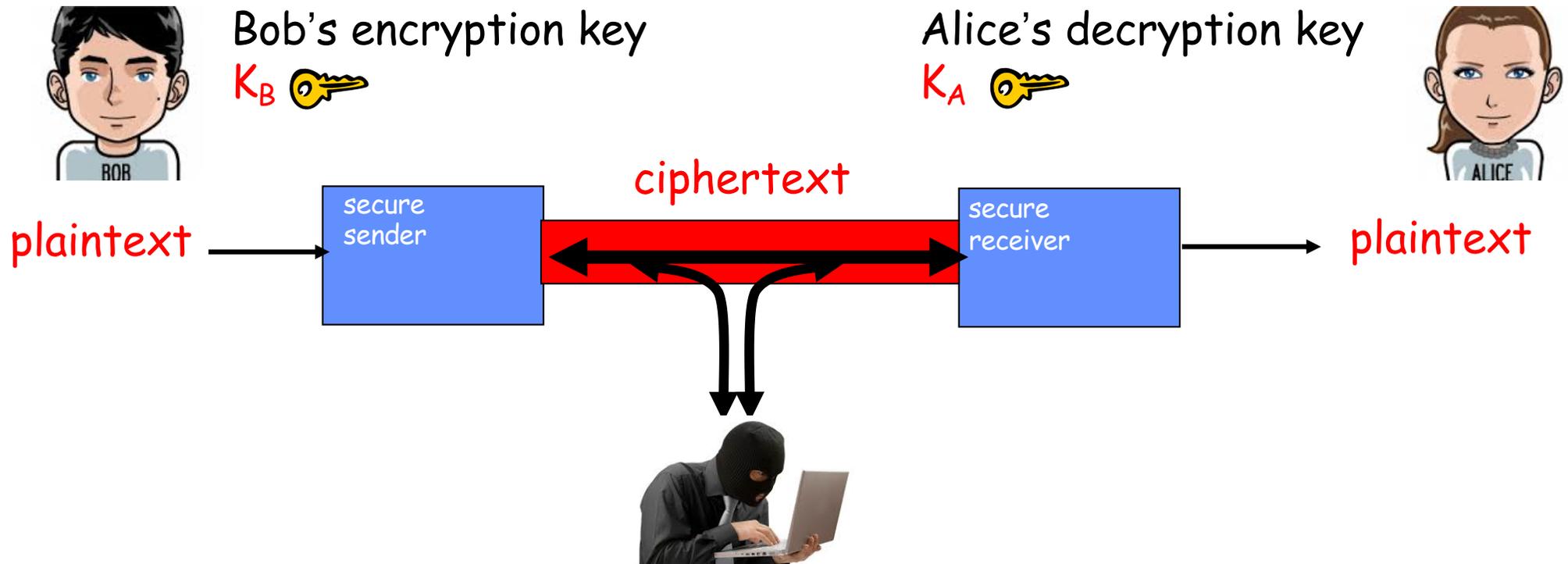- Everything sent in clear-text, no encryption

Encrypt all traffic

- Weak Host-based authentication
  - Exploitable trust relationships
  - Privileged ports offer little protection

Port forwarding

- Server is not authenticated
  - Potential Man-in-the-middle (MITM) attack

Authenticate both user and server

Principle of Cryptography

Bob's encryption key K_B 🔑

Alice's decryption key K_A 🔑

plaintext → secure sender

ciphertext

secure receiver → plaintext

symmetric key crypto: identical sender and receiver keys ($K_B = K_A$)

public-key crypto: encryption key *public*, decryption key *private*

   - public key is shared with the sender

   - private key should not be known by any except the owner

Principle of Authentication

- **Purpose**: sender and receiver confirm identity of each other.
- Methods
  - Password based authentication
    - The username and password are encrypted before transmission.
    - Inherently vulnerable in that they can be guessed
  - Public key based authentication

"I am Alice."

R

$K_A^-(R)$

Send me public key

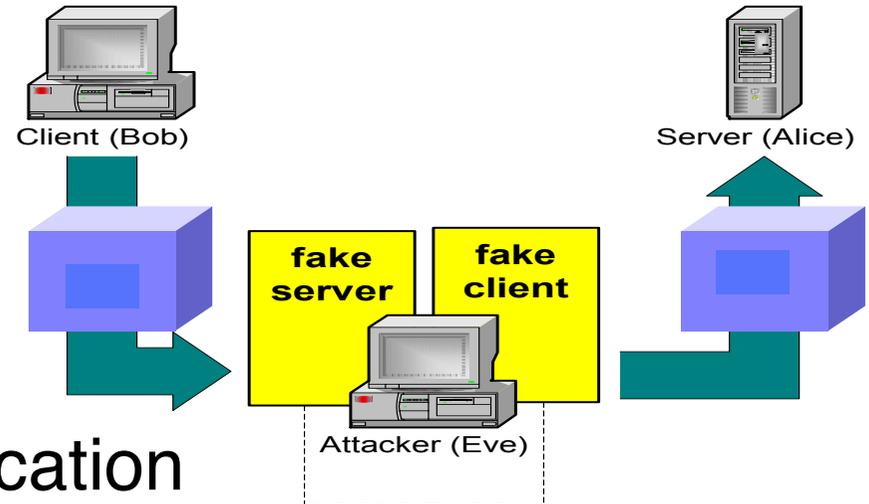K_A^+
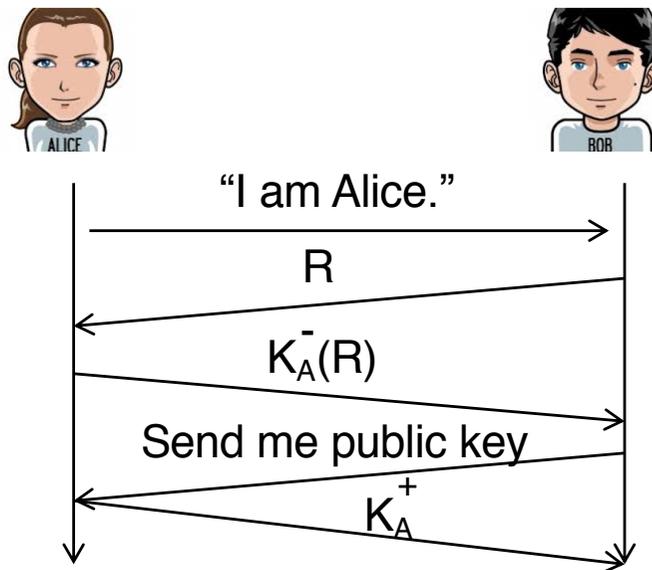
Bob computes

$$K_A^+(K_A^-(R)) = R$$

Retrieval of the public key could be a security hole!

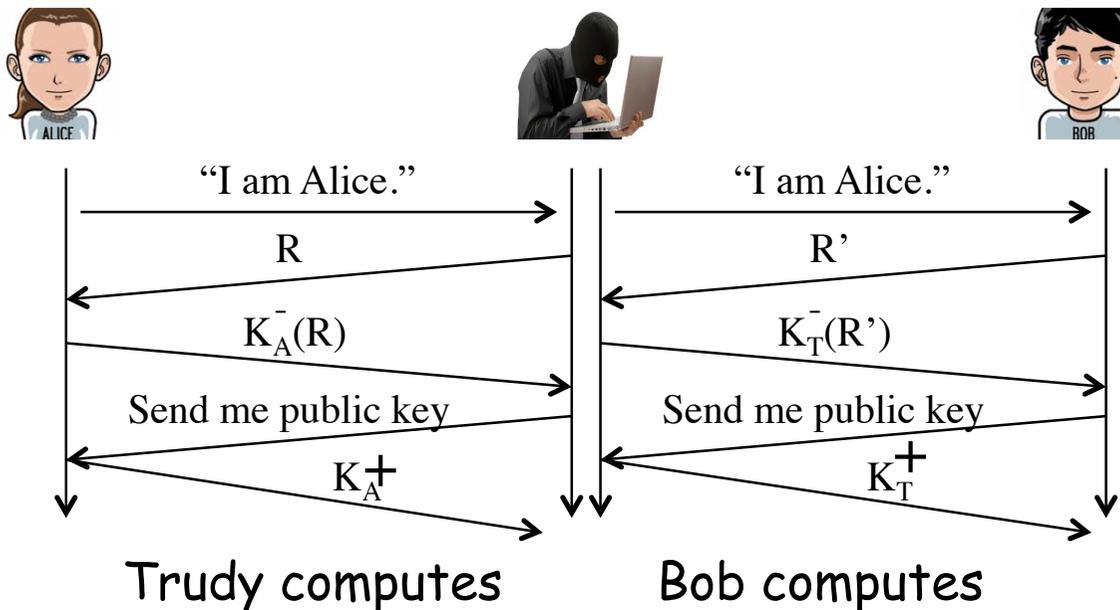Note: K_A^+ means applying RSA algorithm with the key K_A^+. The rest are similar.

Man-in-the-middle attack (MITM)

- ## What is MITM?

  The attacker secretly relays or possibly
  alters the communication

- ## MITM under public-key authentication

Client (Bob)

Server (Alice)

fake
server

fake
client

Attacker (Eve)

"I am Alice."

"I am Alice."

R

R'

$K_A^-(R)$

$K_T^-(R')$

Send me public key

Send me public key

K_A^+

K_T^+

If Bob doesn't verify
the public key sent
by Trudy, MITM attack
establishes!

Trudy computes

Bob computes

$K_A^+(K_A^-(R)) = R$

$K_T^+(K_T^-(R')) = R'$

How to prevent MITM

- Verify the host/user public key

```
Zhiyi:~ hzy$ ssh hzy@oucs1476.staff.uod.otago.ac.nz
The authenticity of host 'oucs1476.staff.uod.otago.ac.nz (10.96.224.233)' can't
be established.
ECDSA key fingerprint is SHA256:I4AA47nI2DdhK6iHcUydQWSFoMnpDeKtivdnqrplCUQ.
Are you sure you want to continue connecting (yes/no)? yes
```

- You can use ssh-keygen to find out the fingerprint of a public key

```
(base) hzy@oucs1476:~$ ssh-keygen -lf /etc/ssh/ssh_host_ecdsa_key.pub
256 SHA256:I4AA47nI2DdhK6iHcUydQWSFoMnpDeKtivdnqrplCUQ root@oucs1476 (ECDSA)
(base) hzy@oucs1476:~$ 
```

- Store the public key of your trusted server into the known_hosts file under .ssh directory

Secure SHell (SSH)

- SSH provides secure versions of the 'r'- commands and telnet
- Encrypt all traffic
  - Public/Private Key for authentication
  - Fast block cipher for data transfer
- Authenticate both host and user
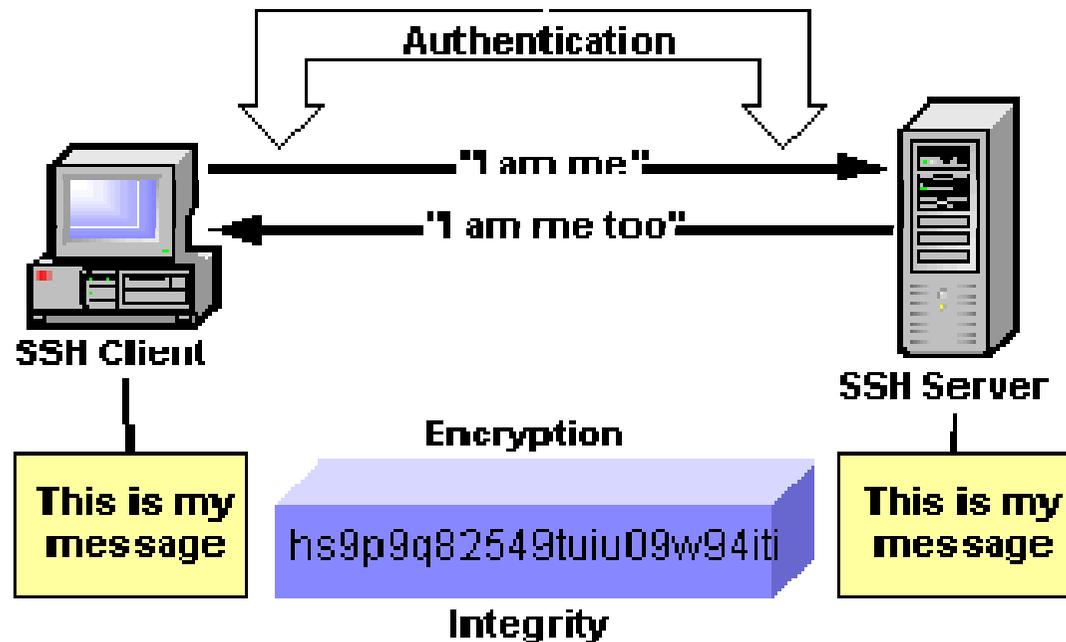
Keys, Keys, Keys

- ## 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

- ## Server Key
  - A temporary, asymmetric key used in the SSH-1 protocol.
  - It is regenerated by the server at regular intervals (by default every hour) and protects the session key

- ## Session Key
  - A randomly generated, symmetric key for encrypting the communication between an SSH client and server.
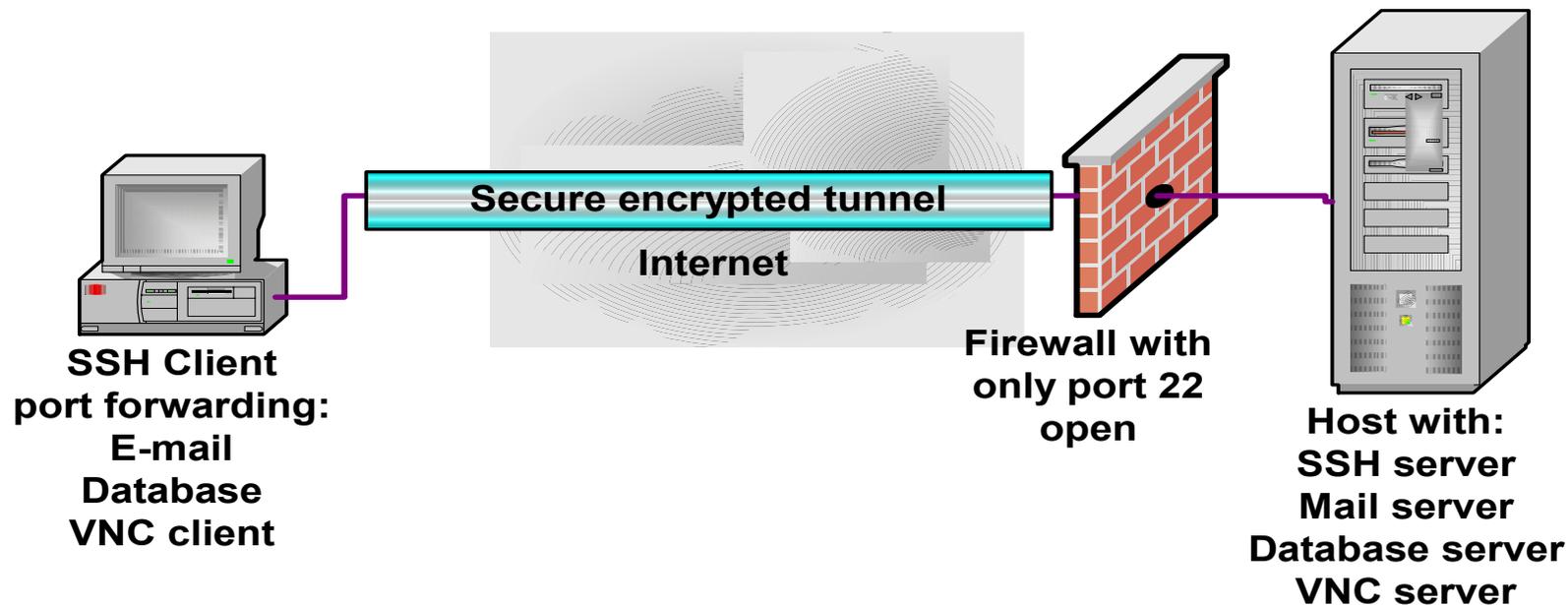
Data Encryption/Integrity

- 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
  - Simple 32-bit CRC in SSH1
  - Message Authentication Code (MAC) in SSH2

Authentication

- User authentication
  - Password authentication
  - Public key authentication using User Key

- Host authentication using Host key
  - Used by a server to prove its identity to a client
  - Used by a client to verify its "known" host
  - Persistent (change infrequently) and asymmetric
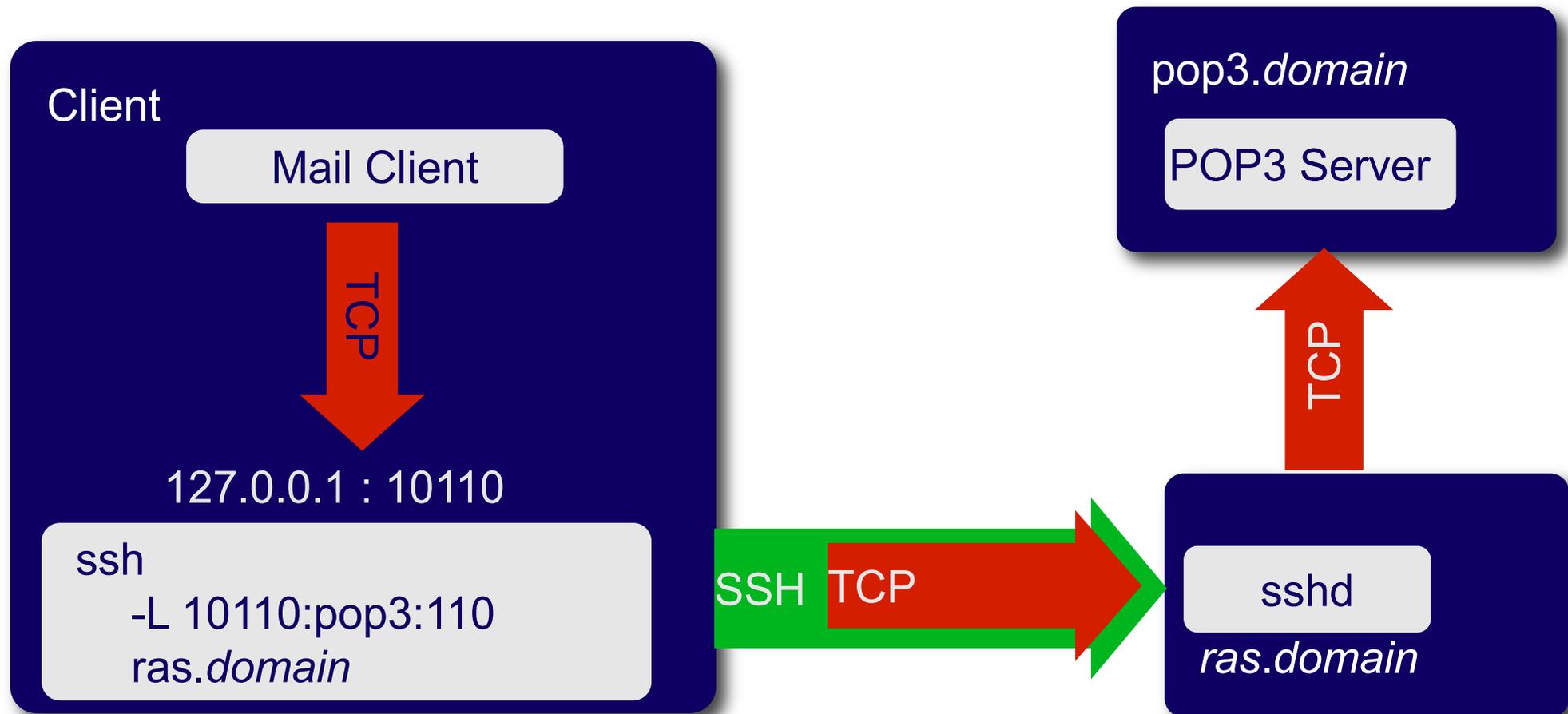 - Guards against the Man-in-the-Middle attack

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.

Secure encrypted tunnel

Internet

SSH Client port forwarding:
E-mail
Database
VNC client

Firewall with only port 22 open

Host with:
SSH server
Mail server
Database server
VNC server

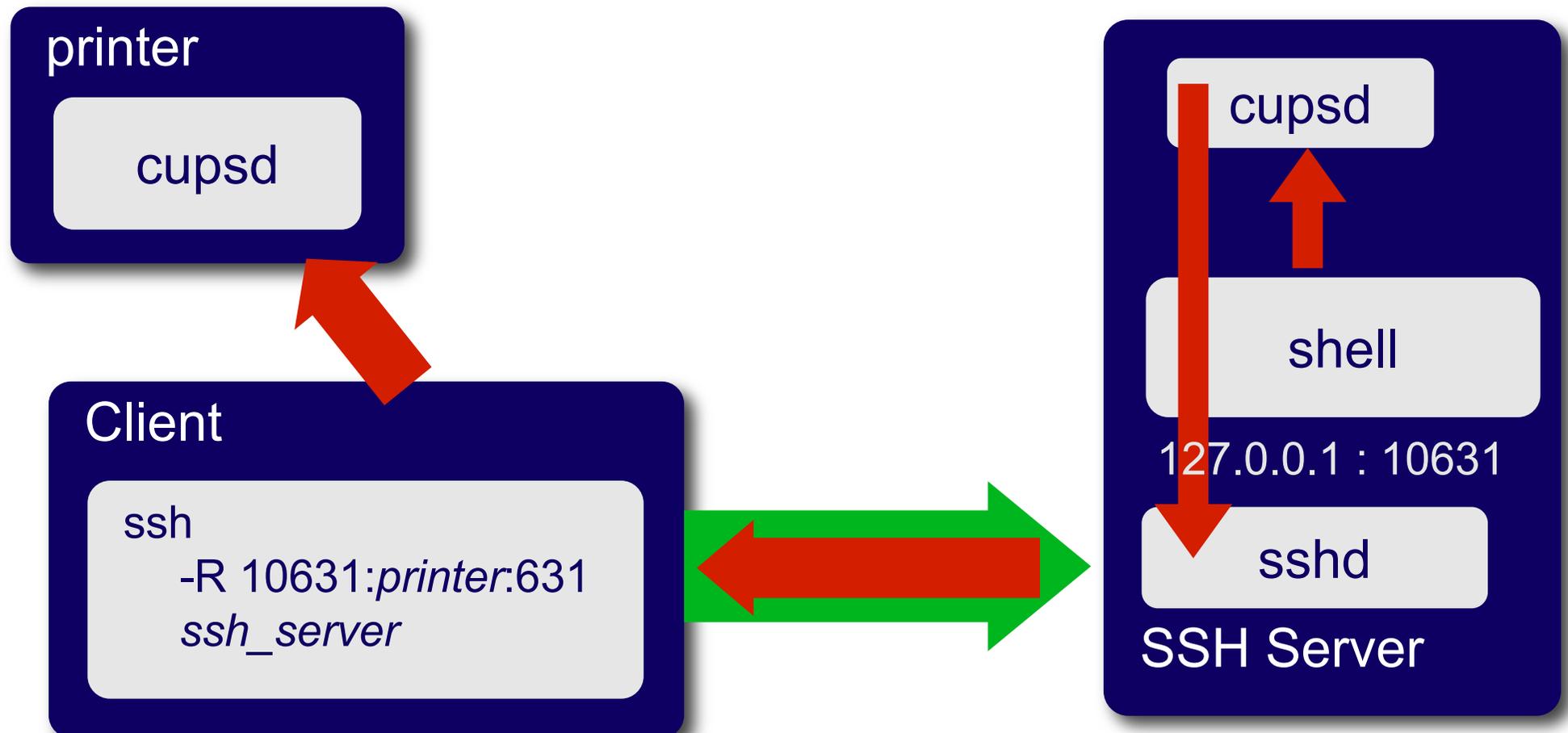Ref: An Overview of the Secure Shell (SSH), Vandyke Software

Port Forwarding

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

Client

Mail Client

TCP

127.0.0.1 : 10110

ssh
    -L 10110:pop3:110
ras.*domain*

SSH TCP

pop3.*domain*

POP3 Server

TCP

sshd

ras.domain

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.

printer

cupsd

Client

ssh
    -R 10631:*printer*:631
    ssh_server

cupsd

shell

127.0.0.1 : 10631

sshd

SSH Server

Threats Addressed by SSH

- Eavesdropping or Password Sniffing
  - All transmitted data is encrypted
- Man-in-the-middle attack (MITM)
  - Host authentication
  - Can not happen unless the host itself has been compromised
- Insertion and Replay attack
  - Attacker is not only monitoring the SSH session, but is also observing the keystrokes
  - By comparing what is typed with the traffic in the SSH stream, the attacker can deduce the packet containing a particular command, and replay the command at a particularly inappropriate time during the session.
  - Message authentication code prevents such attacks.

Threats Not Addressed by SSH

- ## Password Cracking
  - recovering passwords from data that has been stored or transmitted

- ## IP and TCP attacks
  - Syn Flood
  - IP Fragment Attacks
  - ...

- ## Traffic Analysis
  - deduce information from patterns in communication
  - can be performed even when the messages are encrypted

Summary

- Remote terminal (pseudo terminal)

- Secure SHell (SSH)

  - Data Encryption

  - Authentication

  - Port forwarding (how and why)

  - Could MIMT happen with SSH?