COSC301
Network Management and Security

Lecture 13: Remote Terminal Services

Haibo Zhang

Computer Science, University of Otago

Today's Focus

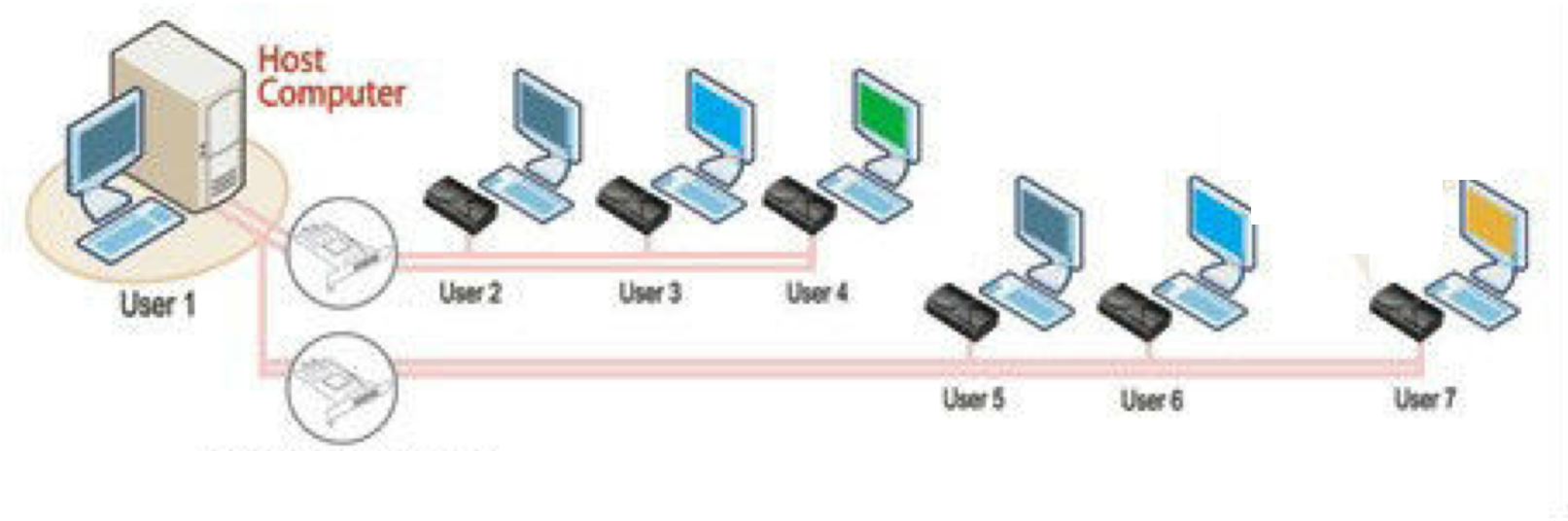
Remote Terminal Services

-- 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



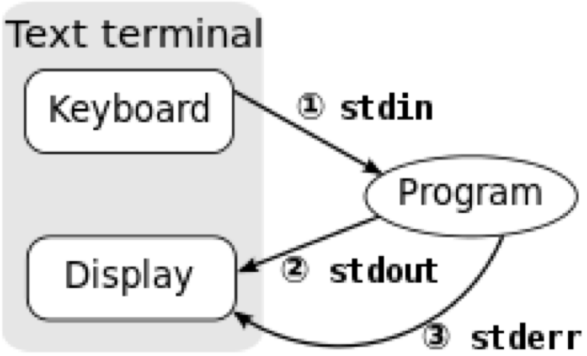
What is a terminal?

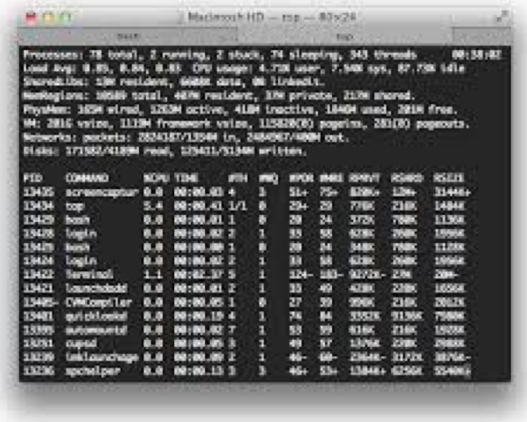
- Hard-copy terminals

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

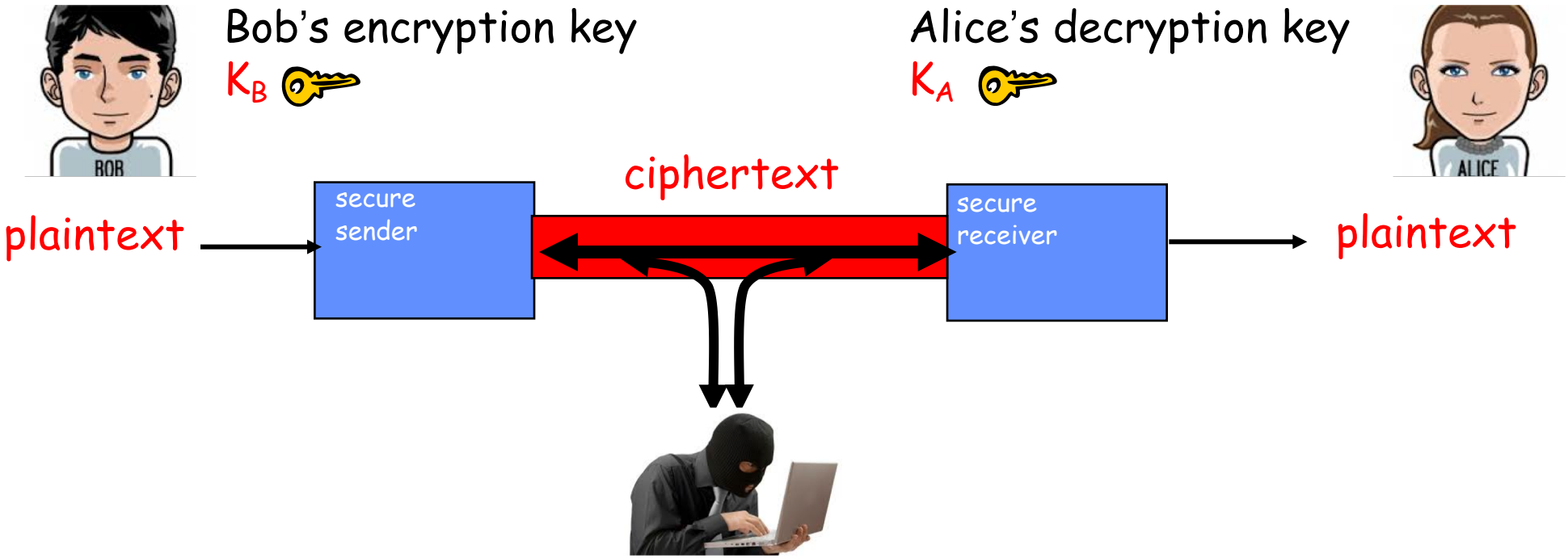
- Weak Host-based authentication
  - Exploitable trust relationships
  - Privileged ports offer little protection

Port forwarding

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

Authenticate both user and server

Principle of Cryptography



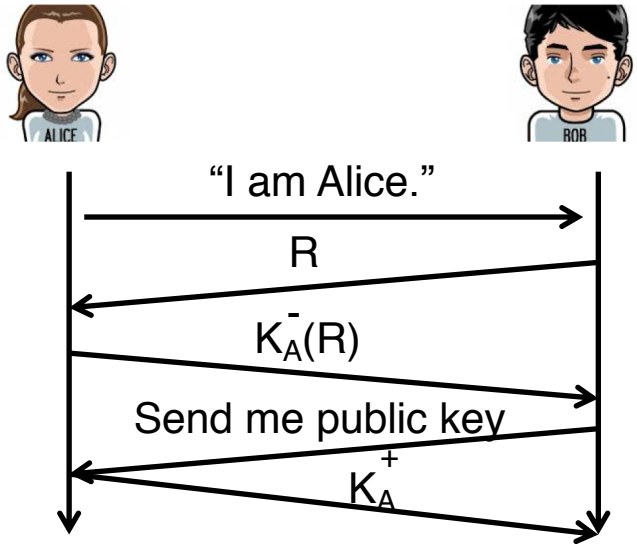
symmetric key crypto: identical sender and receiver keys (K_B=K_A)

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



Bob computes

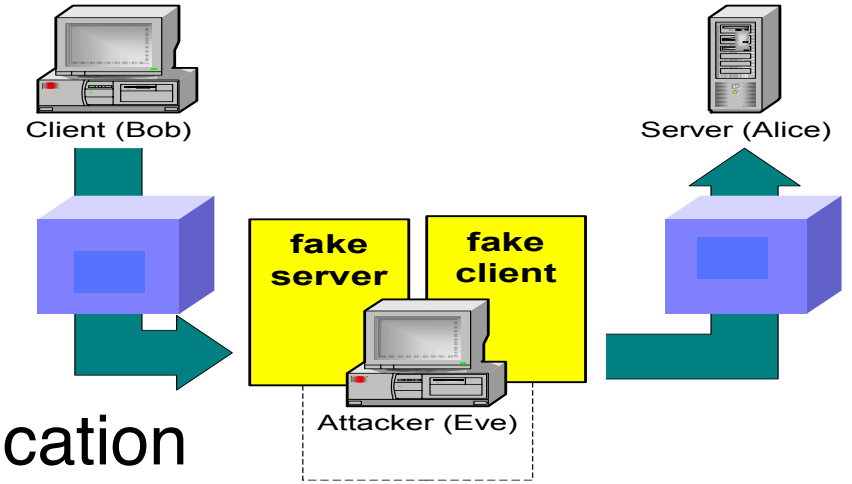
$K_A^+(K_A^-(R)) = R$

Retrieval of the public key could be a security hole!

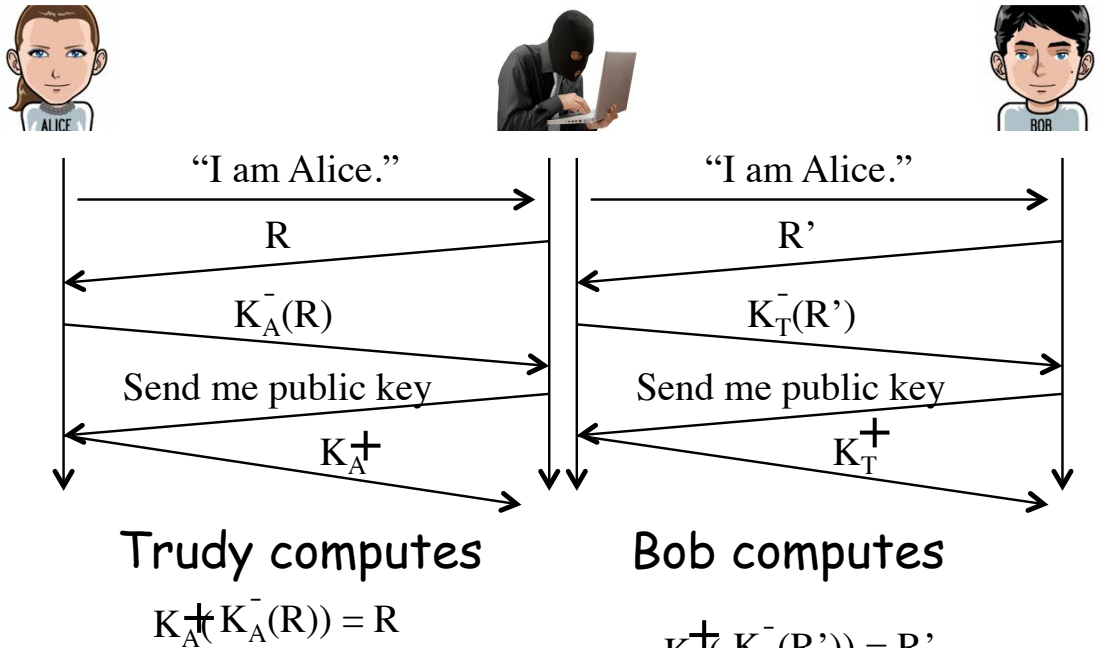
Man-in-the-middle attack (MITM)

- What is MITM?

  The attacker secretly relays or possibly alters the communication



- MITM under public-key authentication



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

How to prevent MITM

- Verify the host/user public key

```
[haibo@hextreme ~]$ ssh haibo@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.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

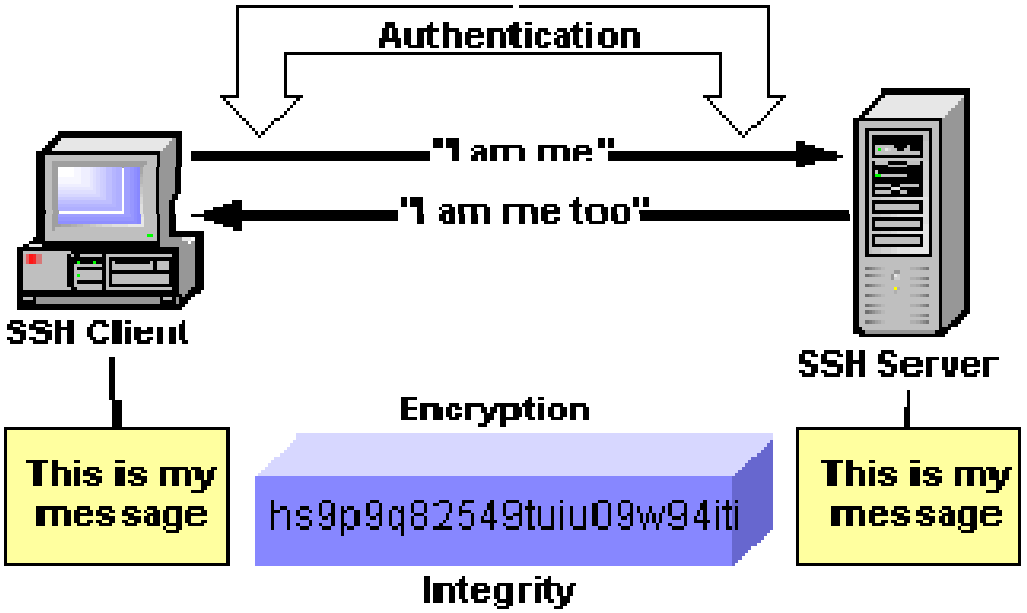
  - You can use ssh-keygen to find out the fingerprint of a public key

```
H-MacBook-Pro:.ssh haibo$ ssh-keygen -lf id_dsa.pub
1024 SHA256:OY/QGASzF5KW0GV2Z8VgEDmoa3btXDOn1SeelsLuFgM haibo@admins-MBP
-3.staff.uod.otago.ac.nz (DSA)
```

- 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

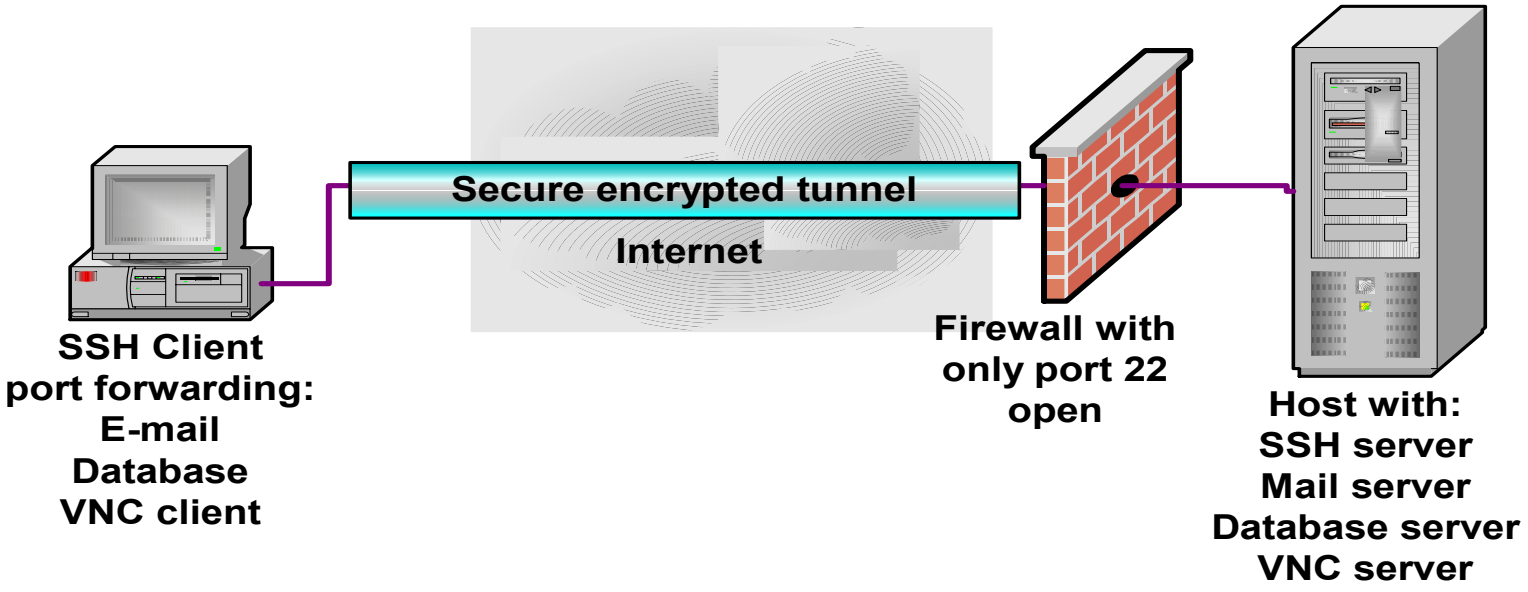
Authentication

- 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

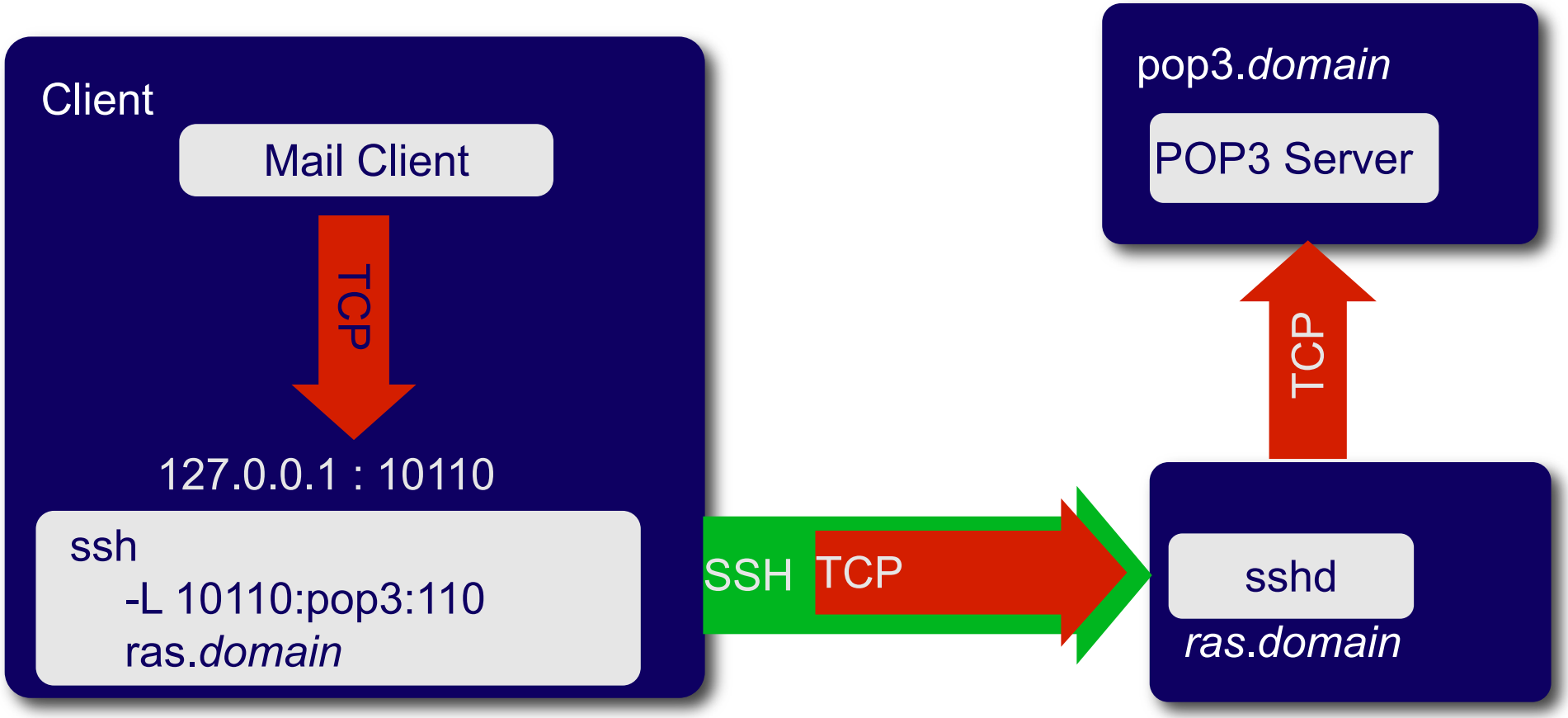
- Allows data from normally unsecured TCP/IP applications to be securely sent across the encrypted tunnel
- Multiple applications can transmit data over a single multiplexed channel.



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

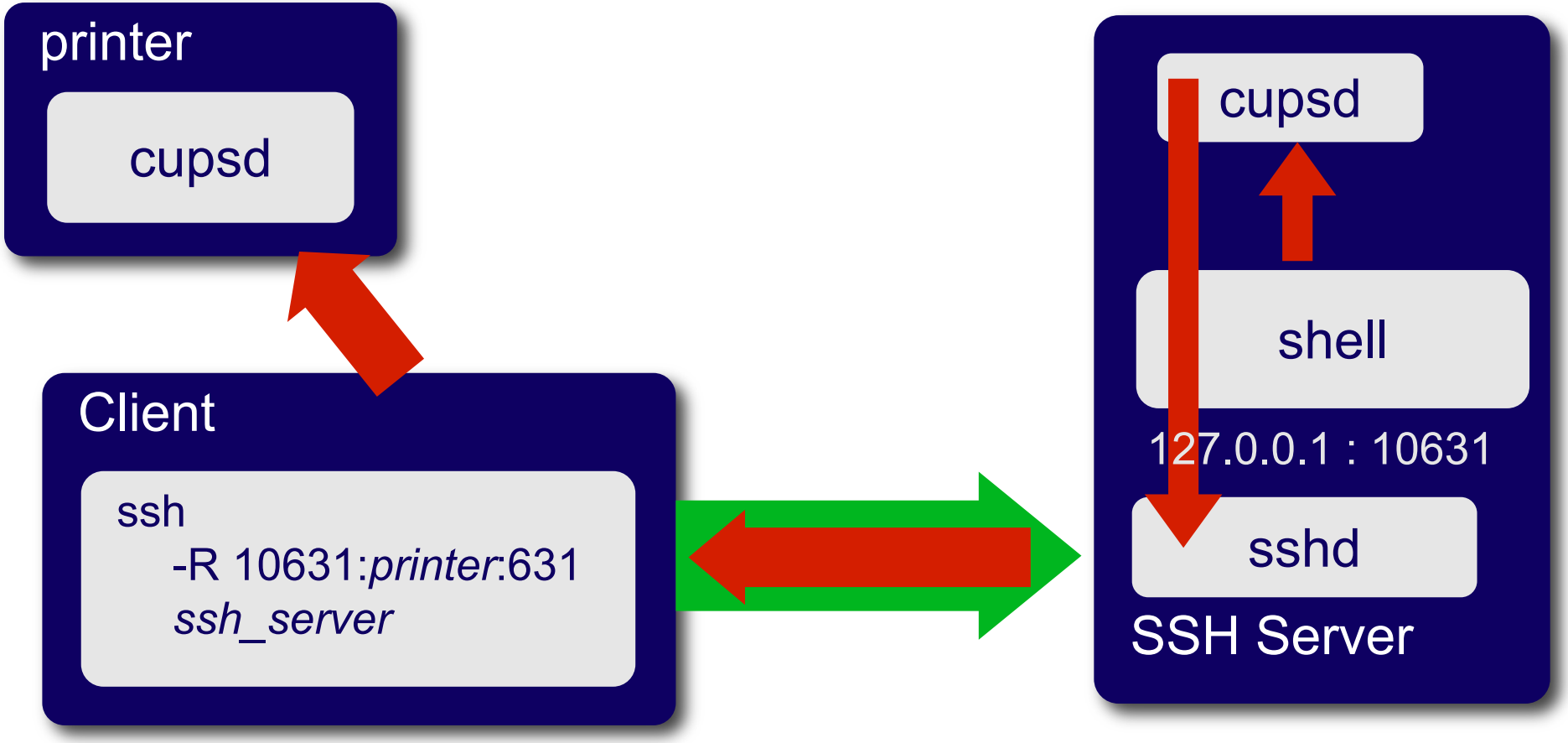
Port Forwarding

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



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.



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 reply 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
- Principle of Cryptography
- Principle of Authentication
- Secure SHell (SSH)
  - Data Encryption
  - Authentication
  - Port forwarding