

Security

Terminology
TCP Wrapper
Cryptography
Kerberos

Terminology

- ◆ Authentication: identifying someone (or something) reliably. *Proving you are who you say you are.*
- ◆ Authorization: permission to access a resource.

Terminology

- ◆ Encryption: Scramble data so that only someone with a secret can make sense of the data.
- ◆ Decryption: Descrambling encrypted data.
- ◆ DES: Data Encryption Standard: secret key cryptographic function standardized by NBS (NIST).

Terminology

- ◆ Secret Key Cryptography: a cryptographic scheme where the same key is used to encrypt and decrypt.
- ◆ Public Key Cryptography: a cryptographic scheme where different keys are used for encryption and decryption.

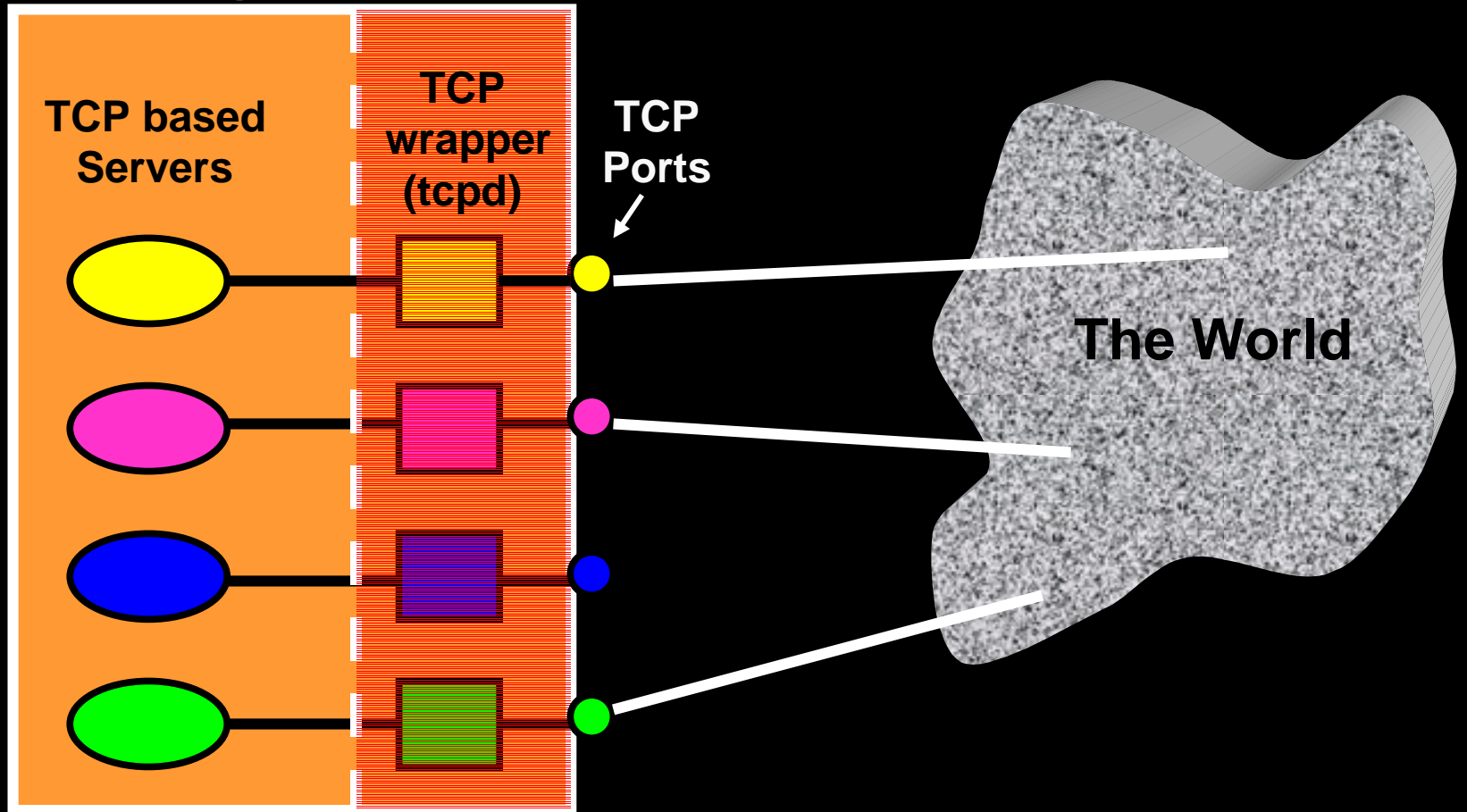
Terminology

- ◆ Firewall: a network component that separates two networks and (typically) operates in the upper layers of the OSI reference model (Application layer).
- ◆ Screening Router: a discriminating router that filters packets based on network layer (and sometimes transport layer) protocols and addresses.

TCP Wrapper

- ◆ TCP wrapper is a simple system that provides some firewall-like functionality.
- ◆ In this case a single host (really just a few services) is isolated from the rest of the world.
- ◆ Functionality includes logging of requests for service and access control.


Single Host



tcpd

- ◆ The `tcpd` daemon checks out incoming TCP connections before the real server gets the connection.
- ◆ A log message can be generated indicating the service name, client address and time of connection.
- ◆ `tcpd` can use client addresses to authorize each service request.

Typical tcpd setup

- ◆ `inetd` (the ) is told to start `tcpd` instead of the real server.
- ◆ `tcpd` checks out the client by calling `getpeername` on descriptor 0.
- ◆ `tcpd` decides whether or not to start the real server (by calling `exec`).

tcpd configuration

- ◆ The configuration files for tcpd specify which hosts are allowed/denied which services.
- ◆ Entire *domains* or IP networks can be permitted or denied easily.
- ◆ tcpd can be told to perform RFC931 lookup to get a username.