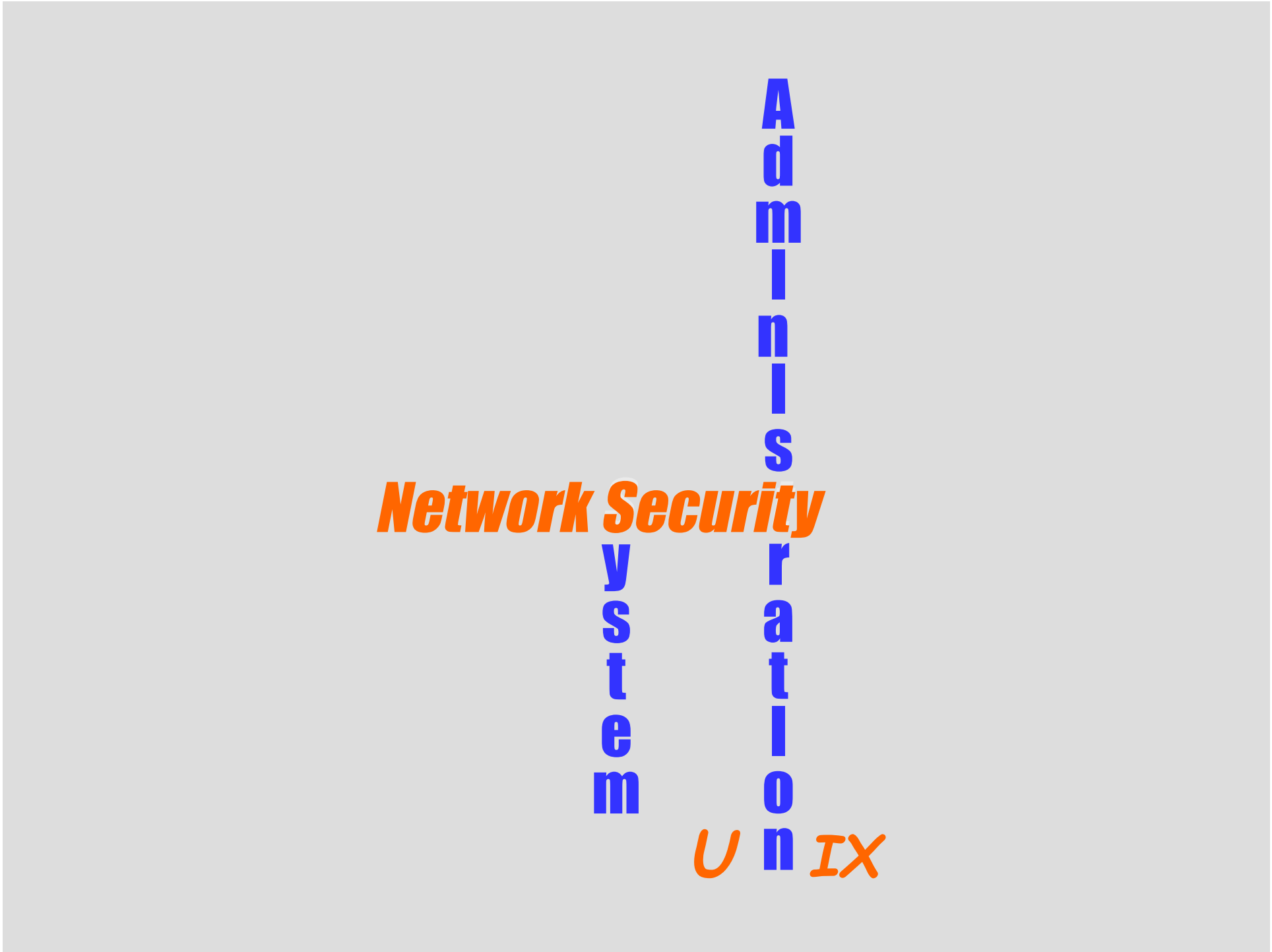
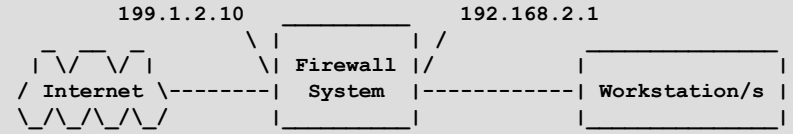

System Administration
Network Security
UNIX

Network Security

- covered some of this already
  - tcp wrappers, SATAN, COPS
- still to come:
  - firewalls
  - S/Keys
  - SSL
  - SSH
  - PGP
- the Linux Security-HOWTO is a useful reference for this area

Firewalls



- **a complex topic**
  - worthy of a course in itself!
- **a firewall is:**
  - a device that protects a private network from the public part (the internet as a whole)
  - *(see p.633, Frisch)*
- **two types of firewall (often used together):**
  - filtering: block all but selected network traffic
    - *filtering firewalls inhibit access to your network from the internet. Only services on systems that have pass filters can be accessed*
    - *all or nothing solution*
      - can't restrict to specific users for example
  - proxy servers: allows indirect internet access through the firewall
    - *with a proxy server users can login to the firewall and then access any system within the private network they have access to*
    - *can log everything they do*
    - *very configurable filtering capabilities*
      - selective transparency based on packet type, source, destination, port, etc.

More Firewalls

- firewalls require kernel support
  - number of parameters to select when making a custom kernel, including (there are more):
    - *CONFIG_IP_FIREWALL*
    - *CONFIG_IP_ALWAYS_DEFRAG*
    - *CONFIG_SYN_COOKIES*
    - *ONFIG_IP_FIREWALL_NETLINK*
- also need the ipfwadm command
  - typically used at boot time in an rc.* file

```
#
# setup IP packet Accounting and Forwarding
#
# By default DENY all services
ipfwadm -F -p deny
# Flush all commands
ipfwadm -F -f
ipfwadm -I -f
ipfwadm -O -f
# Forward email to the server
ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535 -D 192.1.2.10 25
# Forward email connections to outside email servers
ipfwadm -F -a accept -b -P tcp -S 196.1.2.10 25 -D 0.0.0.0/0 1024:65535
# Forward Web connections to the Web Server
/sbin/ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535 -D 196.1.2.11 80
# Forward Web connections to outside Web Server
/sbin/ipfwadm -F -a accept -b -P tcp -S 196.1.2.* 80 -D 0.0.0.0/0 1024:65535
# Forward DNS traffic
/sbin/ipfwadm -F -a accept -b -P udp -S 0.0.0.0/0 53 -D 196.1.2.0/24
# Flush the current accounting rules
/sbin/ipfwadm -A -f
# Do accounting
/sbin/ipfwadm -A out -i -S 196.1.2.0/24 -D 0.0.0.0/0
/sbin/ipfwadm -A out -i -S 0.0.0.0/0 -D 196.1.2.0/24
/sbin/ipfwadm -A in -i -S 196.1.2.0/24 -D 0.0.0.0/0
/sbin/ipfwadm -A in -i -S 0.0.0.0/0 -D 196.1.2.0/24
```

The TIS Firewall Toolkit

- one of the best examples of a proxy server firewall
  - http://www.tis.com/
    - *although recently taken over by Network Associates*
  - configured via
    - */etc/services*
    - */etc/inetd.conf*
    - */usr/local/etc/netperm-table*
      - controls who can access the services of the TIS FWTK
      - uses a program called authsrv to keep a database of user IDs and passwords
        - these must be given whenever an attempt to transit the firewall is made

```
# telnet gateway rules:
tn-gw:                  denial-msg      /usr/local/etc/tn-deny.txt
tn-gw:                  welcome-msg     /usr/local/etc/tn-welcome.txt
tn-gw:                  help-msg        /usr/local/etc/tn-help.txt
tn-gw:                  timeout 90
tn-gw:                  permit-hosts 196.1.2.* -passok -xok
tn-gw:                  permit-hosts * -auth
# Only the Administrator can telnet directly to the Firewall via Port 24
netacl-in.telnetd: permit-hosts 196.1.2.202 -exec /usr/sbin/in.telnetd
# ftp gateway rules:
ftp-gw:                 denial-msg      /usr/local/etc/ftp-deny.txt
ftp-gw:                 welcome-msg     /usr/local/etc/ftp-welcome.txt
ftp-gw:                 help-msg        /usr/local/etc/ftp-help.txt
ftp-gw:                 timeout 300
ftp-gw:                 permit-hosts 196.1.2.* -log { retr stor }
ftp-gw:                 permit-hosts * -authall -log { retr stor }
```

s/key

- a one-time password system capable of providing authentication over networks that are subject to eavesdropping/reply attacks
  - no secret information is stored anywhere, including the host being protected
    - *secret information is used as the seed in a formula that can generate a unique sequence of numbers*
    - *it is this sequence that is used as the one-time passwords*
  - the user's secret information never crosses the network
    - *it is only used to seed the secret sequence initially and then to select which number in the sequence to present during a given login*
    - *actually, the number converted to a six word phrase is used*
  - even if a presented phrase is observed when used, it cannot be re-presented
    - *the last used number is stored on the host and used to generate the next in the sequence when the next login is attempted*

```
login: bob
s/key (65) password: FOUR HAT THEE MAIL KING LASS
ok:
```

More s/key

- **an important point is that the entire sequence never needs to be stored or written down**
  - knowing the previous number used and the secret information, it is possible to determine the next number
  - only the 'legal' user will know both these things
- **another important point is that it is possible to make using s/keys very easy**
  - perhaps as a program in a PDA or even embedded within a "smart card" style of device

SSL

- SSL (Secure Socket Layer)
  - *"SSL is an encryption method developed by Netscape to provide security over the Internet. It supports several different encryption protocols, and provides client and server authentication. SSL operates at the transport layer, creates a secure encrypted channel of data, and thus can seamlessly encrypt data of many types."*
  - intended to foster e-commerce
    - *e.g. to transmit credit card numbers to web based forms*
    - *based on a Public Key Infrastructure*
      - public certificates and private keys used to enforce security
    - *serves as the basis for secure communications with Netscape Communicator*
  - Netscape makes a reference implementation available
    - *with certain key restrictions for people outside the US*
    - *SSLeay was written by Eric Young (from Brisbane) to be an equivalent, high-quality implementation free of US export silliness*
    - *home site is ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL*

ssh

- ssh (Secure Shell) is a program for logging into a remote machine and executing commands in a remote machine
  - uses public key authentication based on the use of digital signatures
    - *each user creates a public / private key pair for authentication purposes*
    - *the server knows the public key, and only the user knows the private key*
- intended to replace telnet, rlogin and rsh, and provide secure encrypted communications between two untrusted hosts over an insecure network such as the internet
- X11 connections and arbitrary TCP/IP ports can be forwarded over the secure channel
- can also compress data for efficiency

PGP

- **Phil Zimmerman's Pretty Good Privacy**
  - an implementation of a public key cryptography system
  - uses one key for encryption, and one key for decryption
  - traditionally, cryptography involves using the same key for encryption that is used for decryption. This "private key" must be known to both parties, and somehow transferred from one another securely.
  - public key encryption alleviates the need to securely transmit the key that is used for encryption by using two separate keys, a public key and a private key
  - each person's public key is usable by anyone who wishes to encrypt data for that person's private use
  - each person keeps his or her private key to decrypt messages encrypted with the correct public key
  - very popular Linux application
    - *also well supported on Macs, PCs, etc.*
    - *typically integrated with mailers, editors etc.*
  - http://www.pgp.com/

CERT Advisories; CIAC List

- **new vulnerabilities are being discovered (and introduced) all the time**
  - CERT (Computer Emergency Response Team) regularly issues (signed) email alerts when a vulnerability is discovered and (usually) identifies what needs to be done to close the security hole
    - *thorough, but sometimes criticized for being slow*
    - *see*
      - http://www.cert.org/
      - http://www.cert.org.au/
  - CIAC (Computer Incident Advisory Capability) at Lawrence Livermore National Labs. in the U.S.A. is another good resource
    - *http://www.ciac.llnl.gov/*