Security and Network Vulnerabilities

Dave Goodell, Nasko Oskov, Chris Clausen

What is Security?

- Restricting information from parties who should not have access to it.
- Maintaining control of resources, like computers and networks, such that malicious users cannot exploit them.

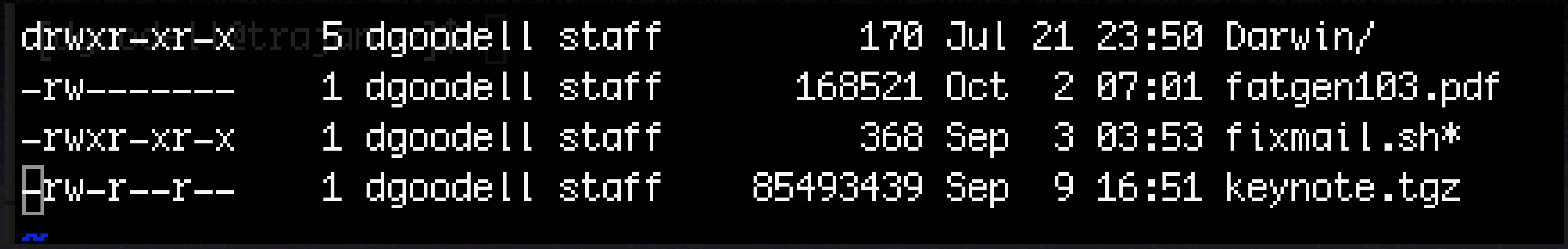
Good Passwords

- Good passwords are the starting point for lots of systems. Poor password choice leaves you open to simple guessing and potential dictionary attacks.
- Good passwords should have non-alphanumeric characters as well as a mix of uppercase and lowercase letters and numbers. Passwords should also be as long as is feasible and allowed by the system (8 characters on most UNIX systems).

File Permissions

- Essential to system security... Imagine if someone was allowed to change your password file, or alter network configurations.
- Implemented differently on different operating systems.

Permissions - UNIX



```
drwxr-xr-x   5 dgoodell staff       170 Jul 21 23:50 Darwin/
-rw-------   1 dgoodell staff    168521 Oct  2 07:01 fatgen103.pdf
-rwxr-xr-x   1 dgoodell staff       368 Sep  3 03:53 fixmail.sh*
-rw-r--r--   1 dgoodell staff  85493439 Sep  9 16:51 keynote.tgz
```

- Model has been around since UNIX was created over 30 years ago, has a few weaknesses.
- Four groups (special, user, group, and other) of three bits (read, write, and execute for the last three groups).

Permissions - ACLs

- Access Control Lists give you more flexibility than the UNIX approach.
- ACL lists users (or groups of users) and the permissions they have (read, write, execute, etc).
- Different filesystems provide varying levels of granularity. Some only allow ACLs on directories, others allows files too.

Permissions - Windows

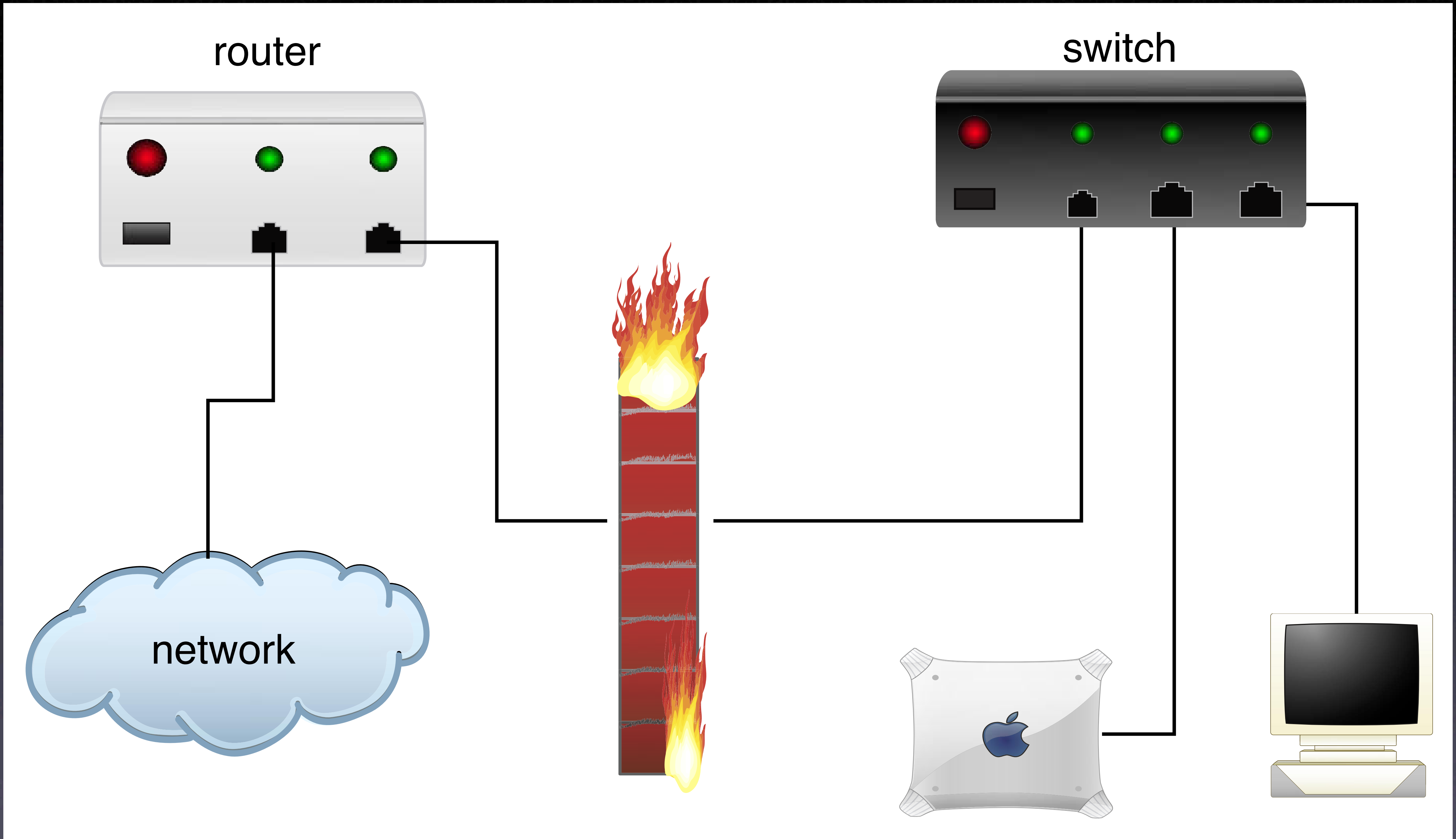
- Uses a very customizable ACL system.
- Pre-set permissions: read, write, read & execute, modify, full control
- Custom ACLs can be setup using ‘cacls’ or ‘xcacls’

Keeping Up to Date

- Windows Update
- RedHat Network / up2date
- Debian ‘apt-get update’
- Mac OS X System Updater

Networking Review

- IP addresses (Internet Protocol)
- TCP/UDP ports
- Ethernet + MAC addresses
- switched vs repeated networks



router

switch

network

Switched Networks... Truly Safe?

- At first glance, switched networks seem to solve the problems associated with repeated (hubbed) networks.
- ARP poisoning allows you to sniff packets that switching would normally prevent you from seeing.

Encryption is the Key

- Encryption is essential for security in modern systems. Using ssh instead of telnet, pgp instead of unsigned/unencrypted email, etc...
- HOWEVER, encryption is no substitute for good security practices. SSH won't matter a whole lot if your password is sitting on a post-it note on your monitor.

Tunneled Services

- Tons of services can be tunneled over encrypted channels.
- SSH tunneling can encrypt arbitrary network connections, SSL (Secure Socket Layer) allows for secure email and web access (among other things).

Firewalls

- Provide control over the network connections into and out of a network or machine.
- Firewalls are not the magic beans of security... just as with any other technology discussed, good security practices in general are needed too.

Firewalls on Various Platforms

- ipfw/ipfilter/pf on *BSD
- ipfw on Mac OS X
- iptables/ipchains/ipfwadm on linux
- checkpoint on Solaris
- Zone Alarm, builtin (XP & 2003) on Windows

Network Address Translation (NAT)

- Allows multiple devices to use one IP address.
- Available in most home routers.
- Great “poor man’s security” tool.
- Not perfect, some things need a globally routable address.

Wi-Fi Networking

- Wireless access points are becoming more and more prevalent today.
- Unlike a wired system, where you can keep someone from getting direct access to your network through physical security, someone can sit outside your room/area and listen to the radio signals being broadcast.

WEP is One Option

- Wired Equivalent Privacy attempts to increase your security in the data link layer.
- One of the major flaws is that the RC4 implementation used in most access points is weak.
- Still useful because it substantially complicates an attacker’s life.

MAC Addresses and Other Options

- Most wi-fi access points allow you to restrict access to a set of MAC addresses.
- Basically security through obscurity, because an attacker can always set his MAC address to be whatever he wants.
- VPN, Radius authentication, 802.1x are more expert options.

Questions?