Secure Networks

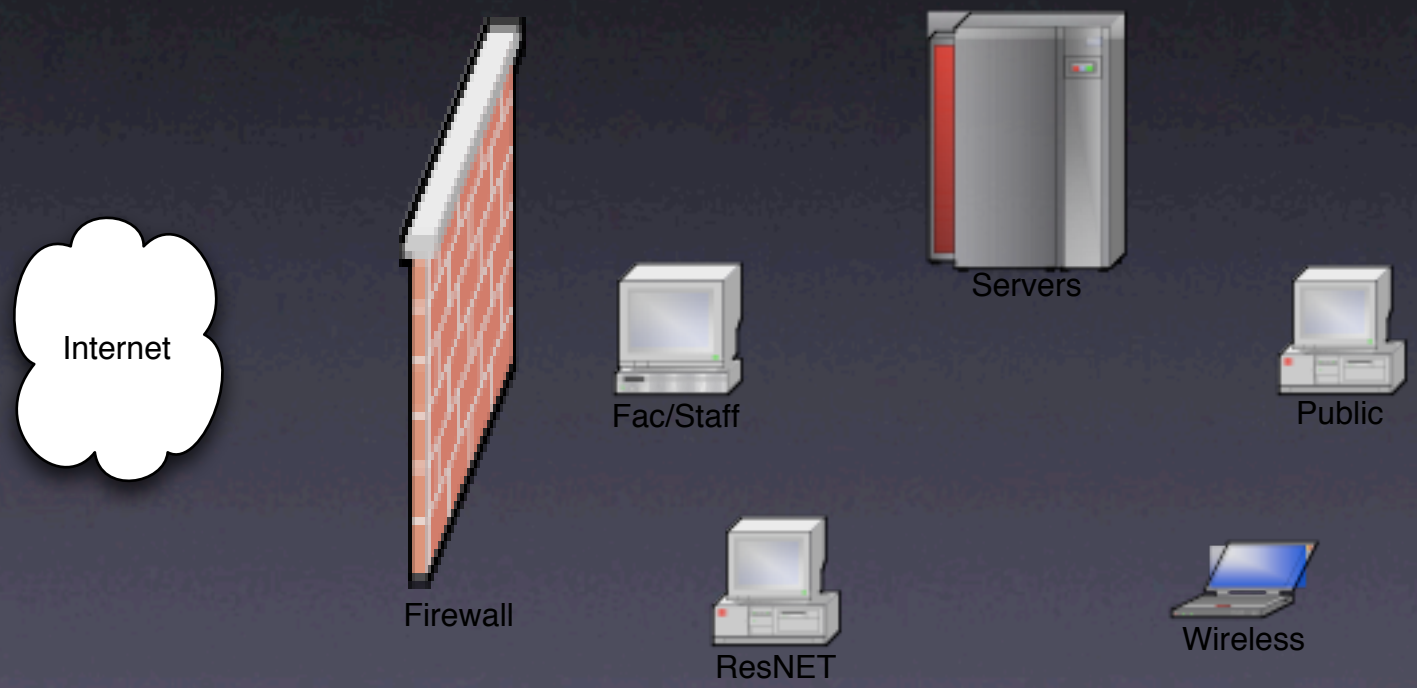
...

Presentation to
Plymouth State University
IT Systems & Networking Staff
Fall 2003

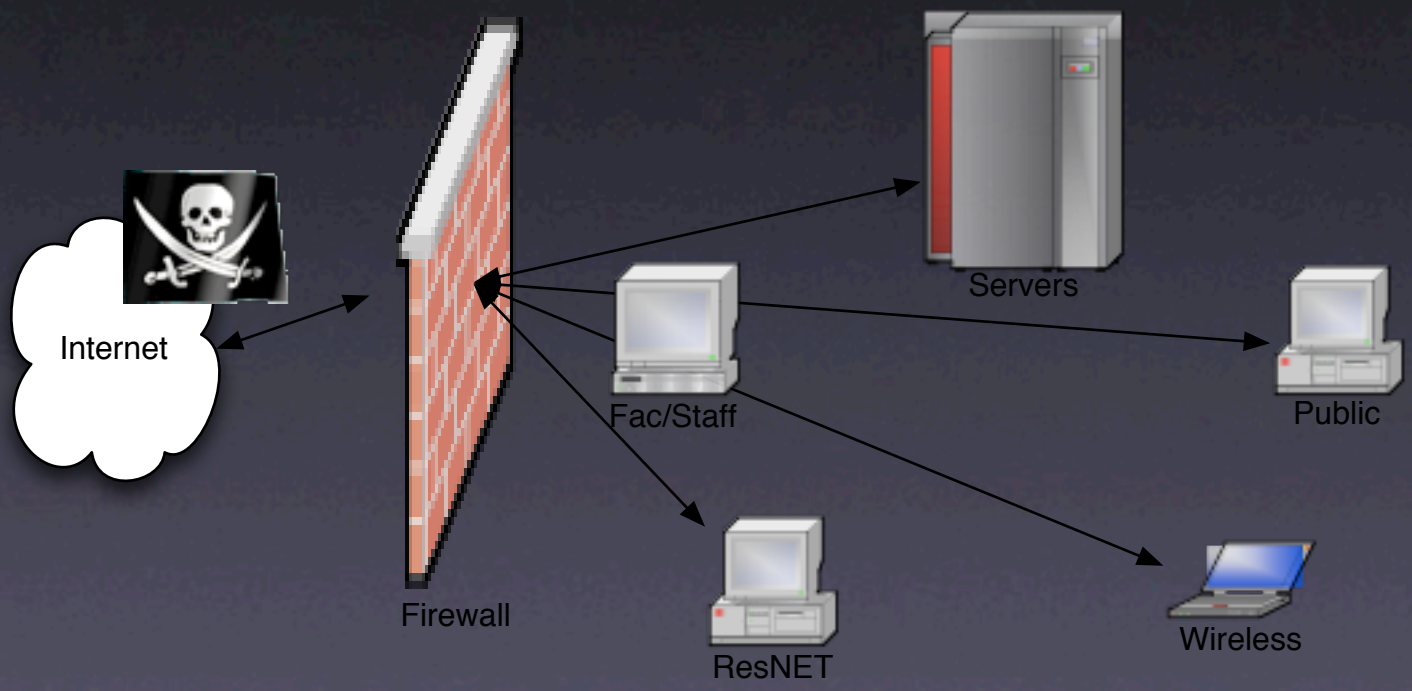
Security By Isolation

…

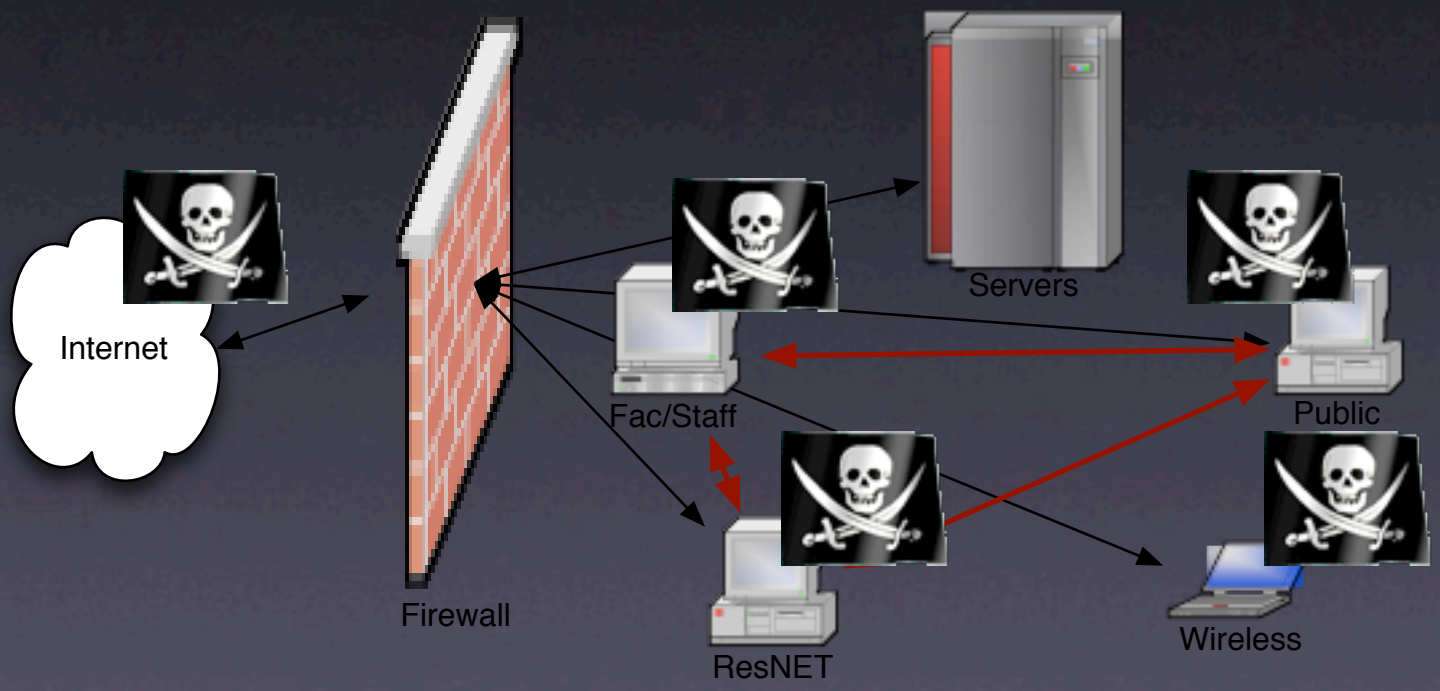
Our Network


Internet
Firewall
Fac/Staff
Servers
Public
ResNET
Wireless

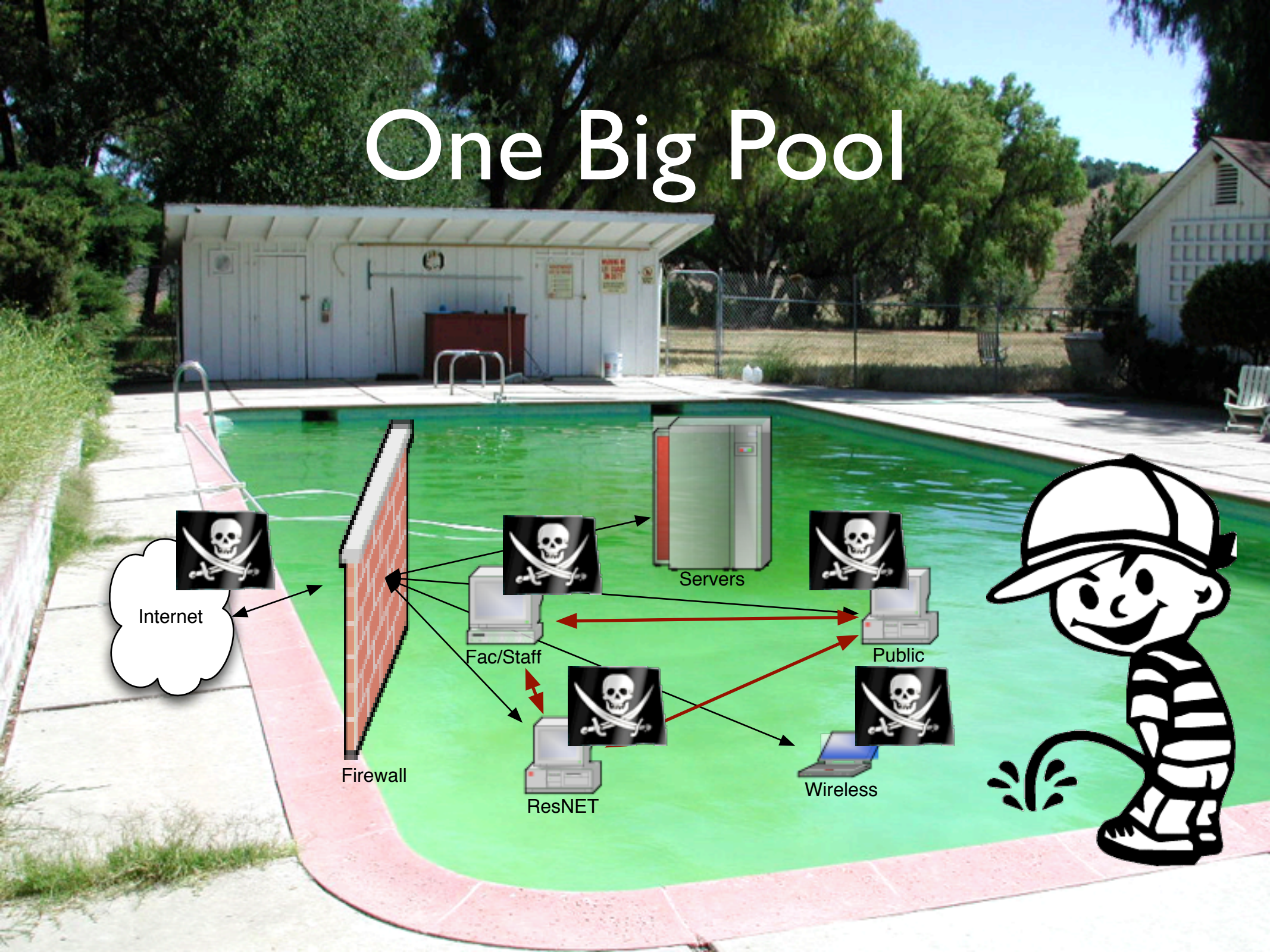
Border Security



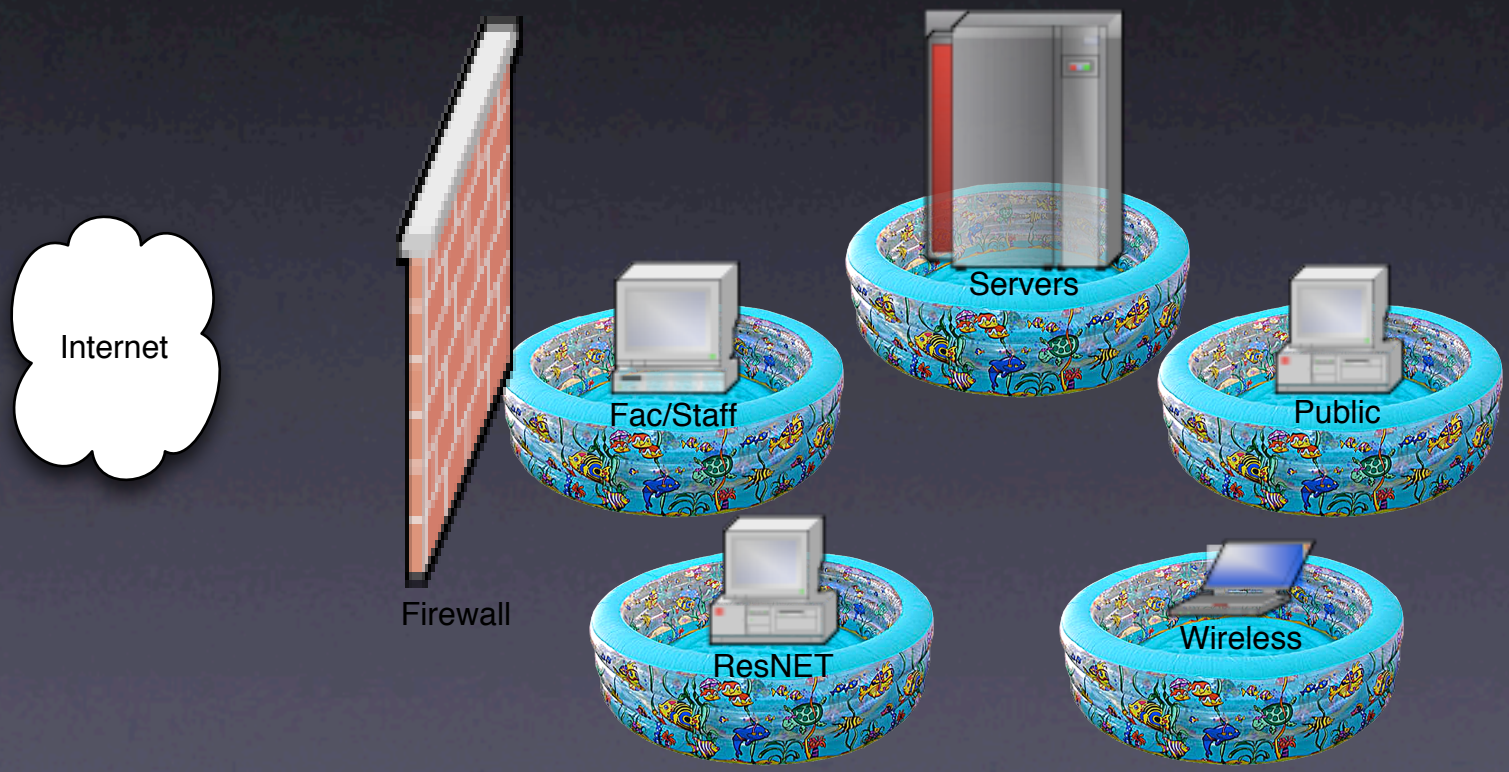
Interior Anarchy



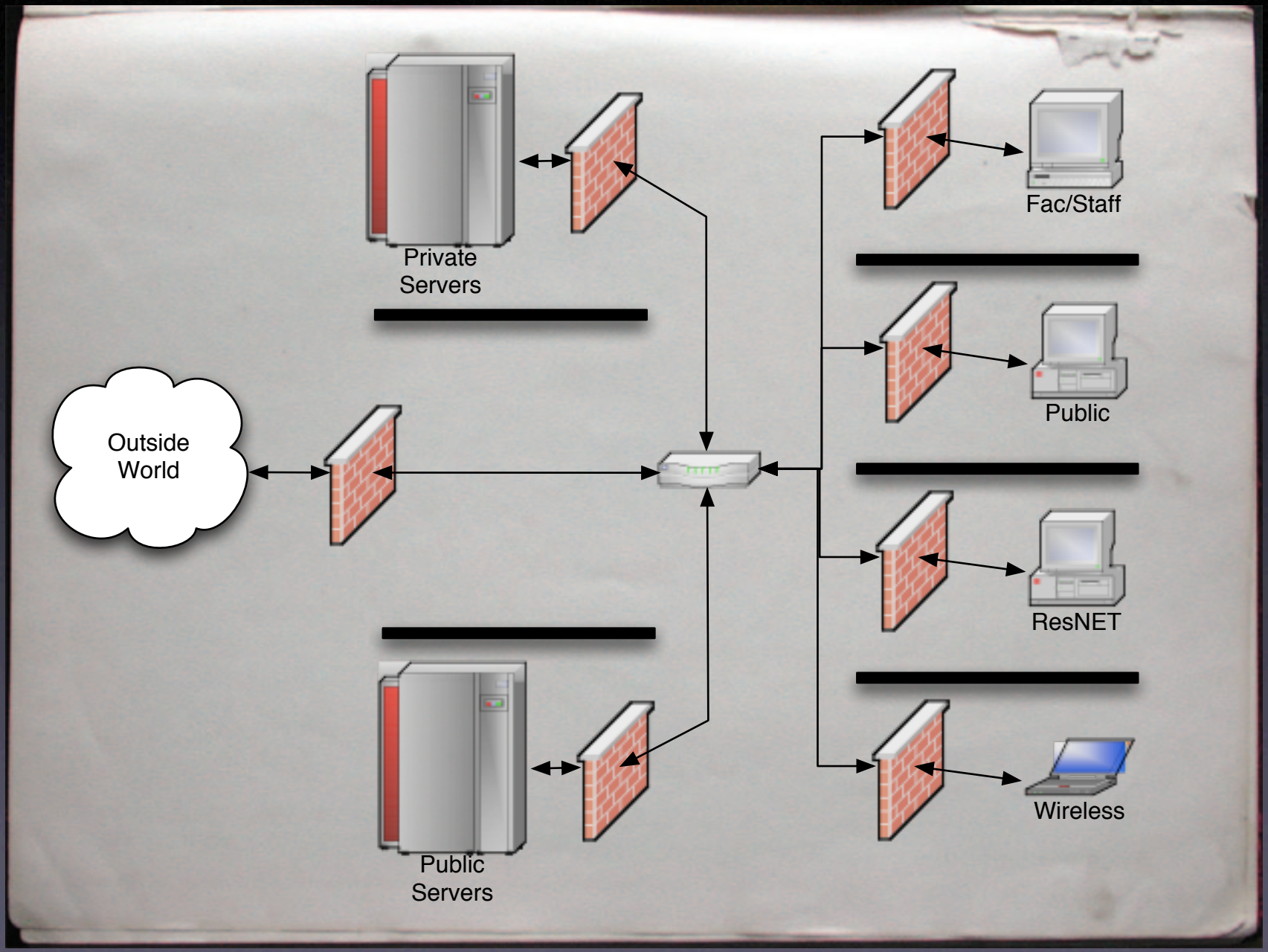
One Big Pool


Internet
Firewall
Servers
Fac/Staff
Public
ResNET
Wireless

Isolate Groups In Their Own Pools



Isolated.


Private
Servers
Outside
World
Public
Servers
Fac/Staff
Public
ResNET
Wireless

Networked, But Isolated

- Group computers according to users and their activities
- Aggressive firewalling as appropriate by group
- Limit access to networks by group association
- Also to consider: NAT and NoCatAuth

Policy Based Networking

- Update our old ideas of ‘private’ and ‘public’ networks
- Make the logical structure of our network match our access and security policy
- Develop mechanisms to support and enforce this policy

Network Vulnerabilities

...

Attack Vectors

- Attacks originating outside our network
- Attacks originating from within our network on targets here or elsewhere
- Man-in-the-middle; interception (sniffing) and manipulation of data en-route

Attack Profiles

- The Vandal
  - Denial of service, random damage, data loss
- The Brigand
  - Uses our resources in support of greater crimes
- The Thief
  - Data theft or manipulation

From Whom Are We Vulnerable?

- We fear miscreants and hackers

  ...but...

- Every user, authorized and unauthorized, is a potential threat
- Threats from ‘authorized’ users, while perhaps less likely, are more directed

Who Are We Trying to Serve?

- Thousands 
- About 7,000 Faculty, Staff and Students now have computer accounts and privileges here

  Do we trust every one of them?

So...

- Any decisions about network security must be made with the recognition that we have a huge number of un-trusted users.

WEP

...

WEP Vulnerabilities

- WEP is shared encryption...
- No matter how you distribute it or how often you change the key, all ‘authorized’ WEP users can see and sniff all other WEP ‘encrypted’ traffic

WEP Vulnerabilities

- ...And you don't even have to crack it...
- WEP encrypted traffic is sent with IP information in the clear

  Packets can be intercepted, re-addressed, and re-sent through the AP to a host on the wired network

  The AP does the decryption, allowing even unauthorized users to easily sniff traffic

Is There An 802.11 Standard That Works?

- There is lots of activity to find a real solution to WEP's failures, but...
- Interoperability is two to three years away

What Can We Do Now?

- First, we must recognize that many of the risks of wireless also exist on our wired network
- And, yes, wireless will always be less secure than wired communications
- With that in mind, let's figure out how to secure our entire network

Reading Room

- *Wireless Hacks* by Rob Flickenger
  O'Reilly Press, 2003
- *Network Magazine*
  CMP United Business Media

  Remember to be conscious of context
  Most of the work and reporting is directed to corporate users

Solutions

…

Similar Service Models

- Because of the number and types of customers we serve, we're more like a public service, a utility, an ISP
- We should look to WISPs — wireless internet service providers — for solutions

The WISP Model

- Low minimum requirements for client software and hardware — 802.11b wireless with recent browser
- Use ‘clientless’ authentication — enter credentials in secure web page
- Depend on application layer security, warn customers to do the same
- Is secure enough to prevent abuse and theft of service

What Is NoCatAuth?

- An open-source captive portal for network authentication and client management.
- Integrates DHCP, firewall, and authentication services.
- Uses web browser interface to take credentials, changes firewall behavior based on authentication. Looks for and reports ARP spoofing.
- Free for client and server; requires no additional client configuration.