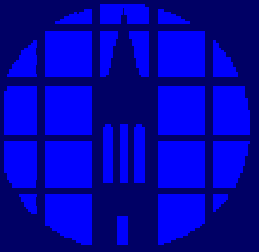
Microlab 2005 Summer Internship

Subha Gollakota

High School Junior

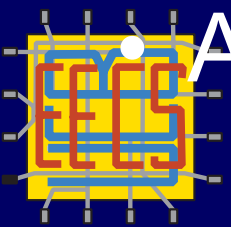
Harker High

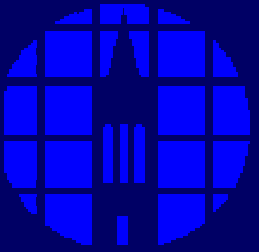
San Jose, CA



Agenda

- System administration
  - Unix vs. Windows
  - Terms
  - Active Directory
  - Proactive Security Measures
- Viruses and security
  - What is a virus?
  - Terms
  - Recent Virus Episode
  - Recovery Process
- Database Management
  - SQL
- Acknowledgements





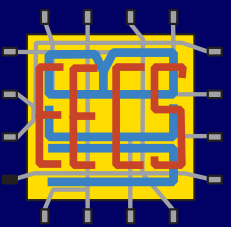
Unix vs. Windows

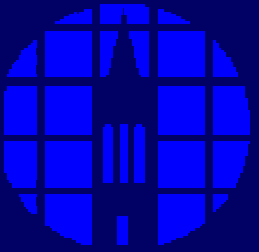
Windows

- GUI based, menu-based
- internal code not visible
- easier when things are working
- PC ideals

Unix

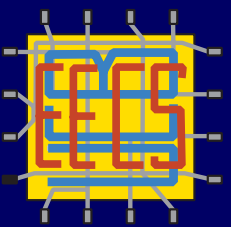
- command line layout, GUIs optional
- open source
- better for problems
- easier networking and remote access





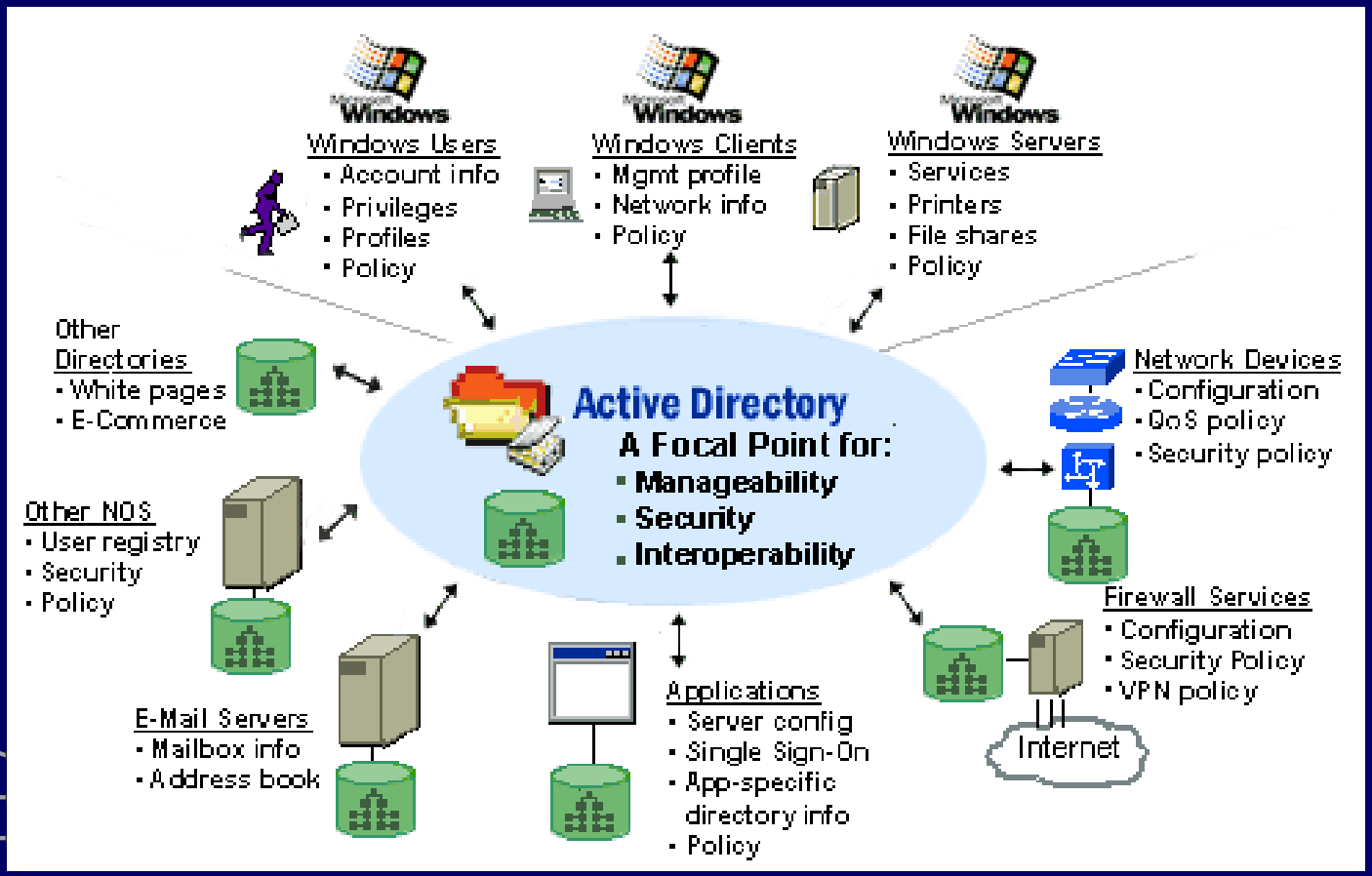
Terms

- **Server**
  - computer software application that carries out some task (i.e. provides a *service* such as web, database, email, printing, remote login) on behalf of a client software
- **Domain**
  - Windows Server domain or Windows NT Domain is a group of computers running versions of the windows OS system that can be centrally managed by one or more Windows Servers



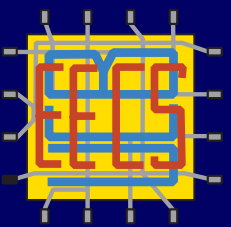
Active Directory

- Windows active directory: Active Directory provides a single point of management for Windows-based user accounts, clients, servers, and applications



Proactive Security Measures

- System administrators regulate permissions given to users for file integrity and security
  - Limit program access for users in order to minimize risk of harmful programs taking advantage of un-patched vulnerabilities in other programs.
  - Prevent users from monopolizing resources (i.e. network bandwidth, disk space, cpu)

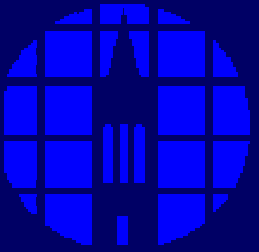


What is a Virus ?

- Virus is a program that can replicate itself by making possibly modified copies of itself.
- It spreads itself by means of 'hosts'; can only spread from one computer to another when host is taken to the uninfected computer
  - by a user sending it over a network
  - by a user carrying it on a removable disk.
- Computers with the same vulnerabilities are susceptible to the same viruses
  - More risk when computers are connected (i.e. through a domain)

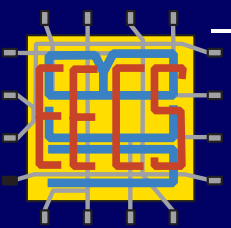
Terms

- **VNC: virtual network computing**
  - Remote control software which allows you to view and interact with one computer (the "server") using a simple program (the "viewer") on another computer anywhere on the Internet
    - the system admin can view or takeover your desktop from their desktop.
- **Buffer overflow**
  - Program does not properly check available space in buffer (destination area) before depositing data. If data exceeds available space, buffer overflow occurs and computer overwrites previous contents of that memory, possibly damaging the computer.



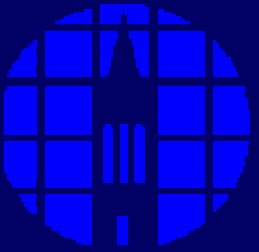
Recent Virus Episode

- **Exploited Vulnerability Note VU#598581**
  - Note from US-Cert Advisory, United States Computer Emergency Team
  - AT&T WinVNC server contains buffer overflow in Log.cpp
  - A buffer overflow in the WinVNC server on Windows systems can allow an intruder to gain control of the VNC server and execute arbitrary code with the privileges of the user running the server.
- **Virus**
  - By providing a specially crafted request to the VNC server, an attacker can overflow a buffer in the server, This gives full control to the attacker. This vulnerability used to gain control of computers and put fakegina.trojan, which steals passwords and changes them
  - GINA: graphical identification and authentication library



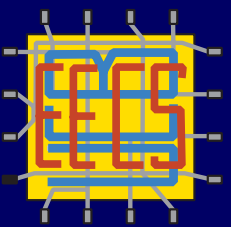
Recovery process

- Pull computer off the network
- Inventory files on computer
- Reformat hard drive of pc and reinstall windows
- Reinstall all the programs
- Replace files
- Run windows update to make sure vulnerabilities are patched
- Rejoin domain



Database Management

- Database Management Systems
  - DBMS
    - Commercial software (and occasionally, hardware and firmware) system used to define, create, maintain, and provide controlled access to the database and also to the repository.
  - RDBMS
    - A database management system that manages data as a collection of tables in which all data relationships are represented by common values in related tables

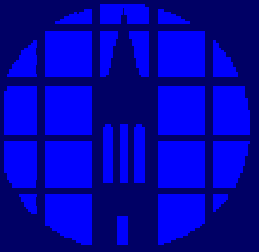


Database Management

- INGRES
  - INteractive Graphics and REtrieval System
  - Research project at UCB from early 1970s to early 1980s
  - Spawned a number of commercial database applications, including Sybase, Microsoft SQL, Server, Informix …
  - Uses tables to store data.
  - There are also system tables that keep track of user tables and roles and data types. This is called the Relationship Model.
  - Relational database model
    - two tables are related when they share a common field
  - Still used as database for new system (Mercury)

Database Management

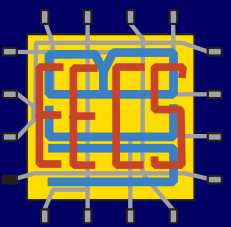
- Mercury:
  - Very user friendly
  - Java-based GUI (Graphical User Interface) as opposed to ascii based and runs on Unix, Linux or MS Windows.
  - Replacement for BCIMS service (wand)
- Data Migration
  - Data moved from old database to new database
  - Qualification Migration Script (based on Equipcap Reader)
  - Modified C# script
- Microsoft SQL Server
  - Works well with other Microsoft Applications and MS Windows applications.



SQL

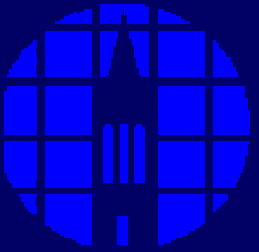
- Structured Query Language (SQL)
  - Most popular computer language used to create, modify and retrieve data from RDMS.
- Sample Queries:
  - SELECT * FROM MEMBERS WHERE firstname='Subha';

    |2243|subha|Gollakota|Subha |406 Cory|642-2716|408-257-1574| |a |06/19/2005 10:33:36|06/14/2005 13:26:28|01/01/1970 00:00:00| 1229| 3032
  - SELECT * FROM VENDORS WHERE NOT state='CA';
    - Many more results not displayed here



What I Did

- Read “An Introduction to SQL: Second Edition” and created sample database
- Connected, disconnected and transported computers (replacing monitors, scanners, etc.)
- Solved minor problems in the microlab office (printing problems, login problems, installation, etc.)
- Reformatted hard drives and other steps for virus recovery
- Data migration; created a computer database using microsoft sql server and displayed it on the web using a modified c# script



Acknowledgments

- Todd Merport for being an excellent mentor
- Eniko Seen for simplifying database theory
- Katalin Voros for providing this opportunity
- Rosemary Spivey for logistical support