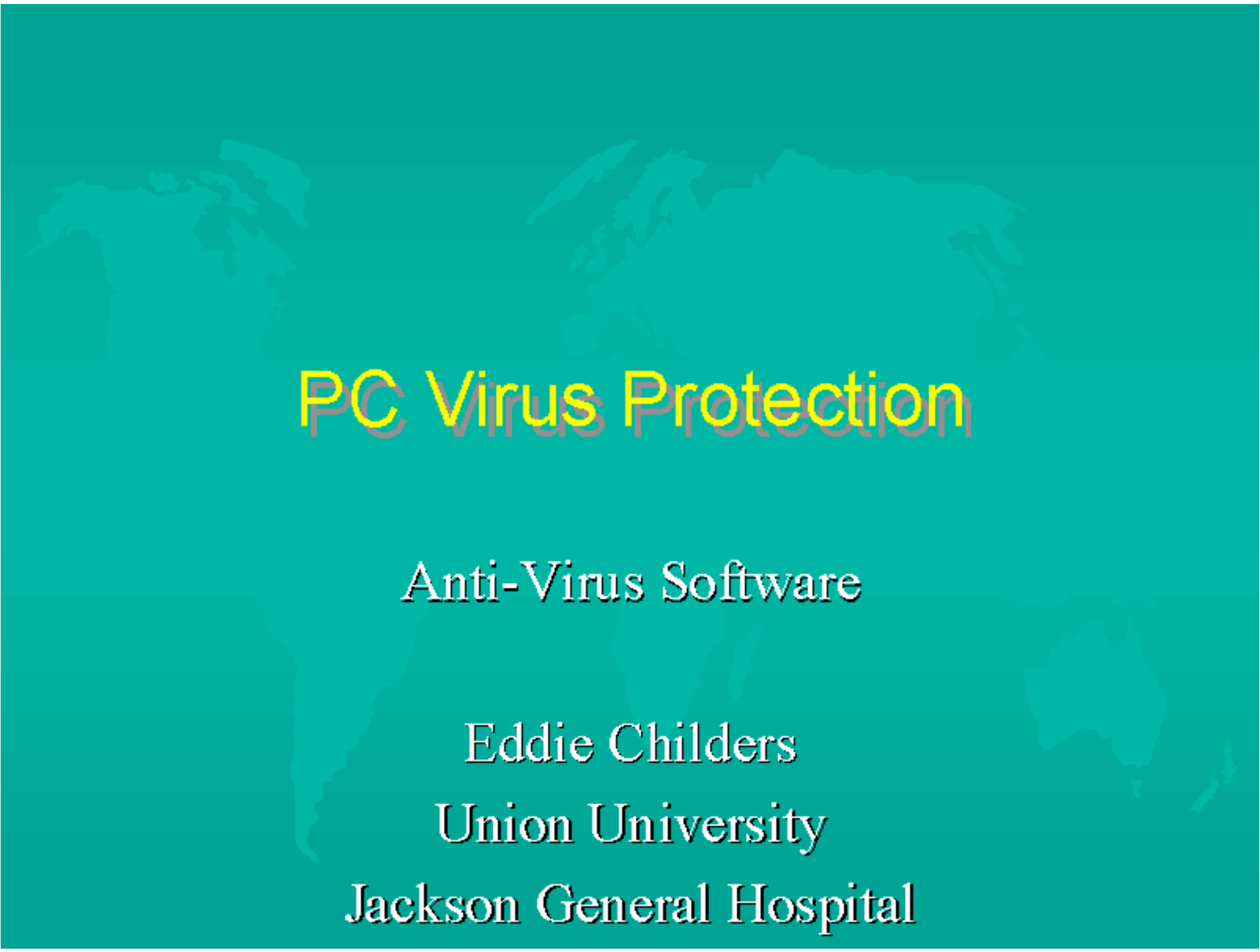




PC Virus Protection

Anti-Virus Software

Eddie Childers

Union University

Jackson General Hospital

Introduction

- ◆ Collection of Viruses
 - Types of Viruses
- ◆ Collection of Anti-Virus software
- ◆ Implementation
- ◆ Results
 - Who is the best?
- ◆ Regrets

Collection of Viruses

◆ Types of viruses

– Boot Sector Viruses

– Michaelangelo or C-brain

– File Infectors

– NuKE

◆ Macro Viruses

– DMVexcel

◆ Stealth Viruses

– Stealth C

◆ Polymorphic Viruses

Collection of Viruses

- ◆ Executable
- ◆ Assembly code
- ◆ Hexadecimal code

Collection of A-V Software

◆ Collection of Anti-Virus Software

– DOS version

- ◆ Dr. Solomons Evaluation FindVirus for DOS
- ◆ Data Fellows F-PROT Free Version for DOS
- ◆ McAfee Version 3.0.0 for DOS
- ◆ CPAV from Central Point Software
- ◆ VSAFE from Microsoft

Implementation

◆ DOS Versions

- Dr. Solomon Eval FindVirus
 - ◆ Finds all file infectors
 - ◆ Does not find inactive boot sector viruses
- Data Fellows F-PROT Free DOS Version
 - ◆ Does not work
- McAfee Version 3.0.0
 - ◆ Finds all viruses including inactive boot sector viruses

Implementation

- ◆ Versions for DOS continued
 - CPAV by Central Point
 - ◆ Did find “a” virus but did not recognize
 - VSAFE by Microsoft
 - ◆ Did find Darth Vader 2 virus

Results

- ◆ F-PROT worst
- ◆ VSAFE and CPAV
 - Lack of virus scan
 - Relied on integrity checking
- ◆ Dr. Solomon
 - Excellent on File Infectors and Macros

Results

◆ Second Place

– McAfee Virus Scan 3.0.0

- ◆ Excellent on File Infectors
- ◆ Excellent on Macros
- ◆ Excellent on Stealths
- ◆ Excellent on Boot Sectors
 - Only failed to disable inactive Boot Sectors

Results

- ◆ The “Best”

- A reliable backup

- ◆ Can't run a virus on
 - ◆ Can't erase or format
 - ◆ Can't touch

Regrets

- ◆ Lack of a Windows 95 computer
 - Unable to run 95 anti-virus software
 - Unable to see hueristics

Sources

- ◆ Cheyenne
 - www.cai.com/cheyenne/security
- ◆ McAfee
 - www.mcafee.com
- ◆ Dr. Solomon
 - www.drsolomon.com/response/pcweek.html
- ◆ Norton
 - www.symantec.com