

HCCL

HUMAN CENTERED COMPUTING LAB



Prime III



One Machine, One Vote for Everyone

Juan E. Gilbert, Ph.D.

TSYS Distinguished Associate Professor

Fellow, AU Center for Governmental Services

Auburn University

Computer Science & Software Engineering

Human Centered Computing Lab

gilbert@auburn.edu

http://www.juangilbert.com/

HCCL
HUMAN CENTERED COMPUTING LAB

Prime III

User Interface



Voter - Multimodal

- ✓ Multimodal Interactions
  - ➢ Voters can speak and touch interchangeably





Voter

- ✓ Be accessible to a wide range of voters
  - ➢ Use multiple means of interaction (Touch, Voice, or Both)
  - ➢ Large screen layout
- ✓ Voter can change vote
  - ➢ Voter can change their vote at anytime before casting the actual ballot
- ✓ Voter verification is **required**
  - ➢ Voters **must** confirm ballot (touch or voice)



Voter - Visual



- ✓ Large touch screens
  - ➢ Large fonts
  - ➢ Images or No Images
  - ➢ Touchable Names
- ✓ Voter touches the screen to make selection
  - ➢ Confirmation is visual
- ✓ Ballot layout
  - ➢ One race per screen
  - ➢ Voter confirms ballot twice before it is recorded

Voter - Verbal

- ✓ Headset
  - ➢ The system speaks to the voter through the headset
  - ➢ Conversation is confidential – no one can hear the machine's speech, but the voter
  - ➢ System's speech is can be pre-recorded or computer generated



- ✓ Embedded microphone in the headset
  - ➢ Candidates are randomly assigned to numbers
  - ➢ Voter speaks the number for a candidate
  - ➢ Confirmation is verbal

Voter - Accessibility



- ✓ Sighted
- ✓ Blind
- ✓ Deaf
- ✓ Illiteracy
  - ➢ Sighted and Blind
- ✓ Physical Disabilities
  - ➢ Limited or no use of hands
  - ➢ For example, military wounded in Iraq, elderly, etc.

- ✓ All of these voters can independently vote!

HCCL
HUMAN CENTERED COMPUTING LAB

Prime III

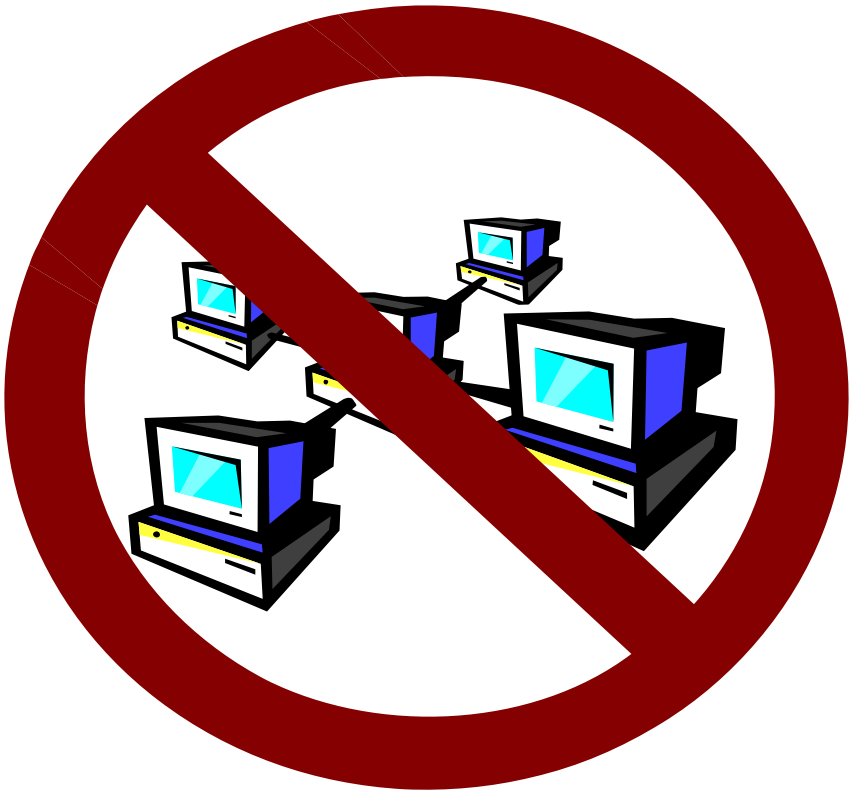
Usable Security



Security



- ✓ No Network Access



Security



- ✓ Prime III DVD
  - ➢ Created, approved and sealed by an Election Center
  - ➢ Technical team that verifies the DVD's contents are authentic
- ✓ Bootable DVD Contains
  - ➢ Executable Prime III Code
  - ➢ Encrypted Ballot files
  - ➢ Encrypted Key



Security



- ✓ All transactions are recorded (audio/video)
  - ➢ Separate video recorder, e.g. VHS, DVD
  - ➢ Each Prime III machine is attached to 1 or 2 separate video recorders



- ✓ Video and audio captured
  - ➢ Video of screen captured with
  - ➢ Audio produced by Prime III (not the voter's voice)
  - ➢ Video recorder is active when activity occurs. Sleeps otherwise
  - ➢ **Voter remains anonymous**

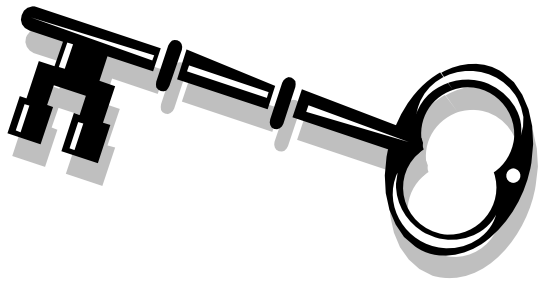
Security



- ✓ Video surveillance of the machine, not the voter
  - ➢ The voters' intent is accurately captured
  - ➢ Precise audit trail of voting events
  - ➢ Voter Verifiable Video Audit Trail (VVVAT)



- ✓ Voter files are encrypted
  - ➢ Advanced Encryption Standard (AES)
  - ➢ 3Des
  - ➢ And others …



Security - VVVAT



Prime III machines running software from DVDs

Video recorders

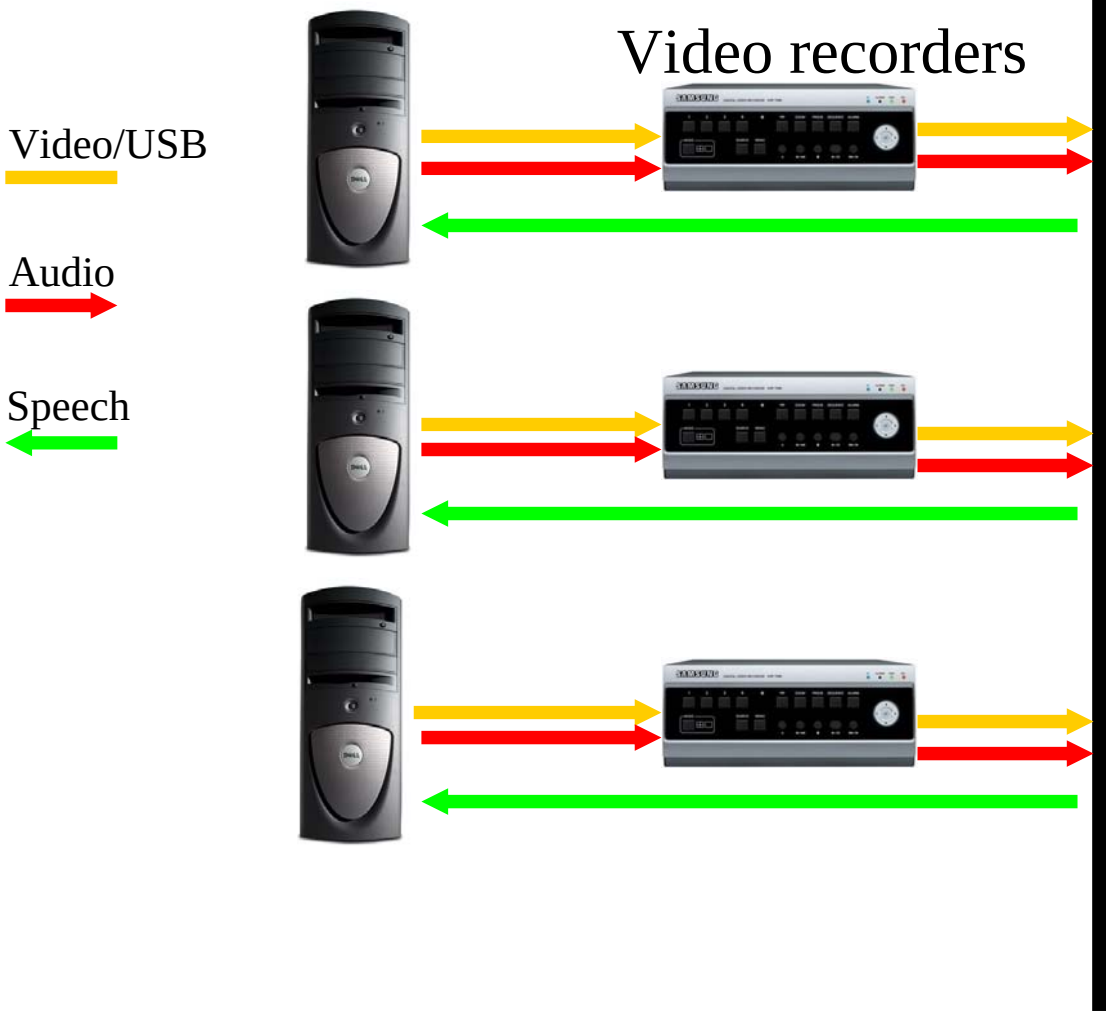
Connector Switch

Voting Booths

Video/USB

Audio

Speech



Voter Speech

Security



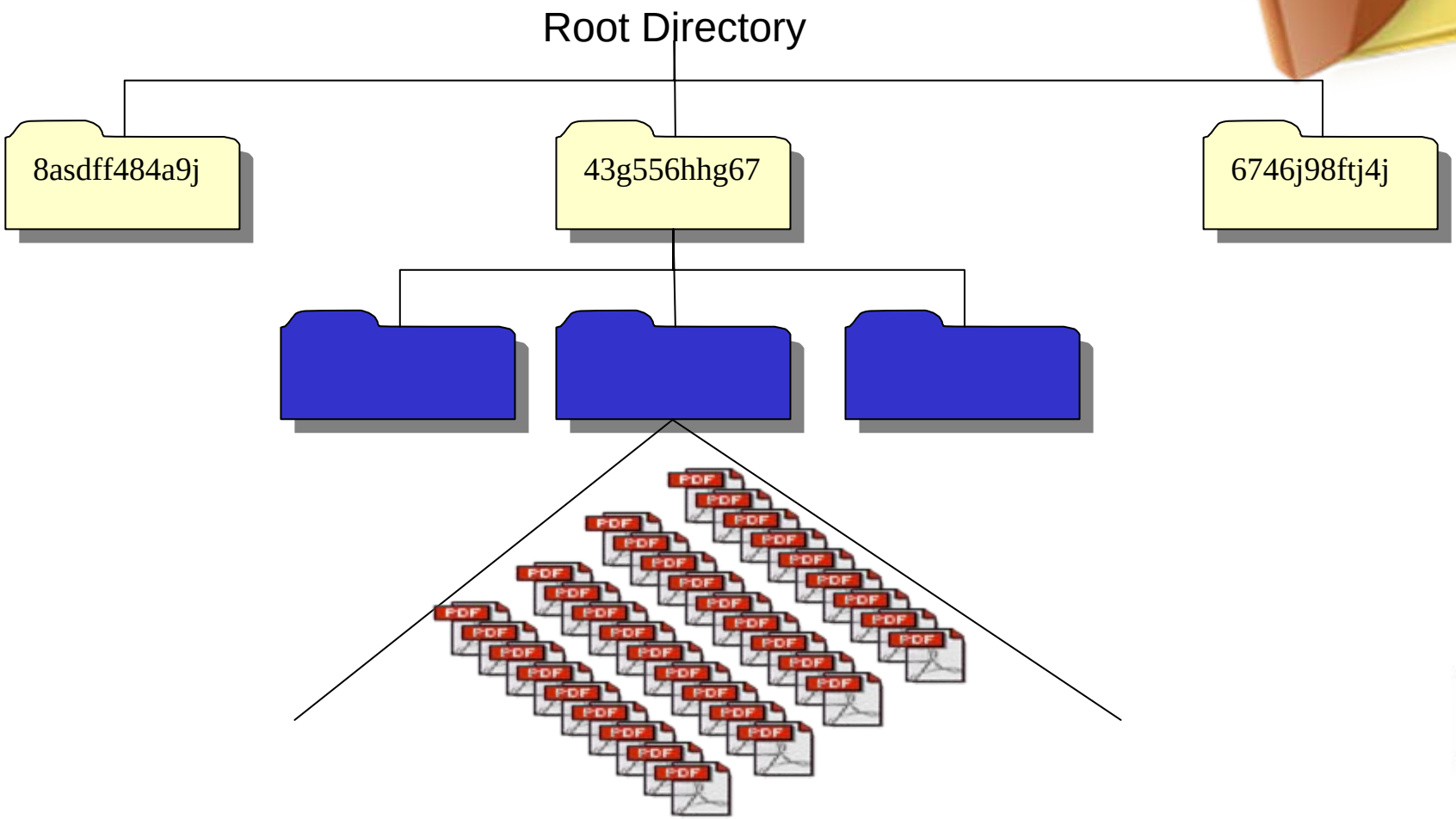
- ✓ Imposter Files
  - ➢ Each machine has encrypted imposter vote files
    - ➢ Imposter vote files are constantly updated
    - ➢ Several encryption schemes are used
    - ➢ Vote files organization/layout will vary
    - ➢ Encryption Key contains
      - ➢ Key to encryption algorithm
      - ➢ Vote file organization/layout





Security





Security



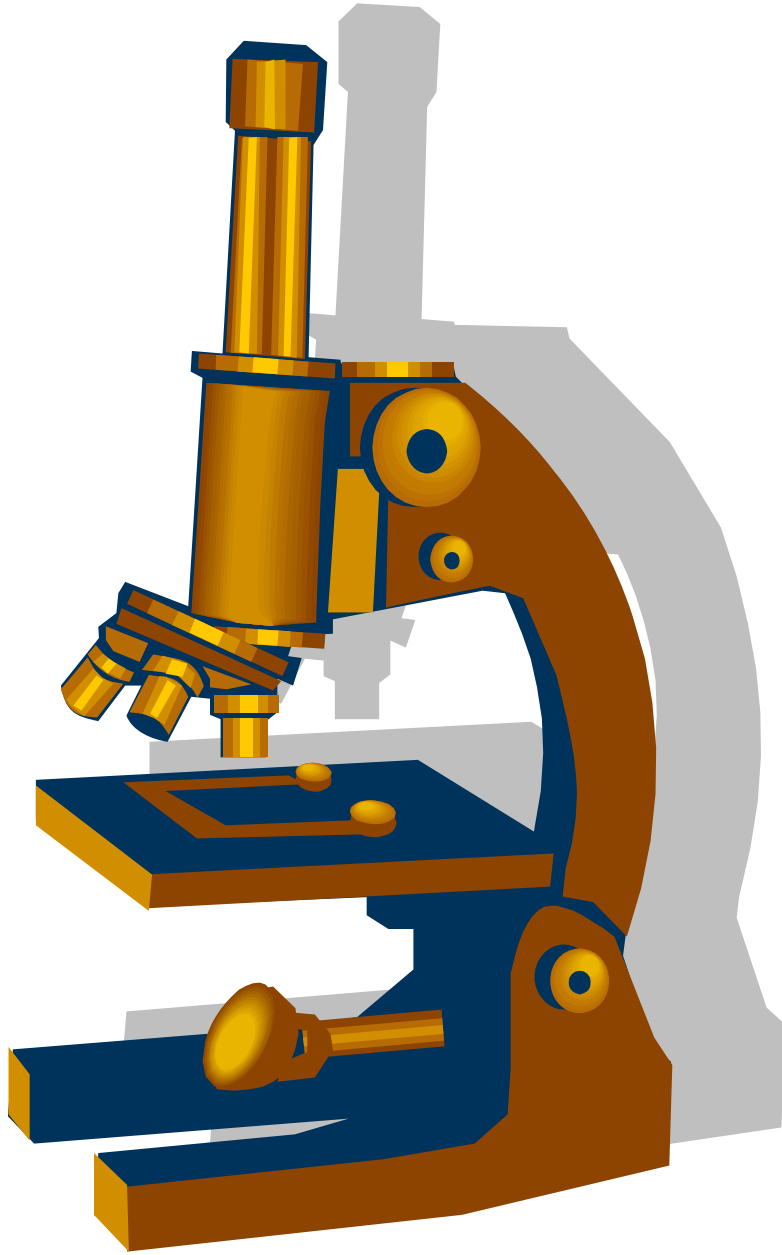
- ✓ We can print ballots as well
  - ➢ Printed ballots will contain only the selections for each race
  - ➢ Printed ballots will mirror the final ballot



HCCL
HUMAN CENTERED COMPUTING LAB

Prime III

Preliminary Findings



Studies

- ✓ Alabama Institute for Deaf and Blind Study
- ✓ Osher Lifelong Learning Institute
  - ➢ 500+ senior citizens
  - ➢ Counting study
  - ➢ Setup and break down study
  - ➢ **VR study**
- ✓ Campus election
- ✓ AU Elderhostel (March 13, 2008)



Studies

- ✓ NSBE Election (March 21 & 22, 2008)
- ✓ Indiana University
  - ➢ Security studies with IBM Code Processor
- ✓ Future Studies
  - ➢ People First of Alabama
  - ➢ Georgia Disability Vote Project Community



What makes Prime III novel?

- ✓ Multimodal Interface with Automatic Speech Recognition
  - ➢ We are the only system with speech recognition in the world
- ✓ Component Design
  - ➢ Easily integrated into existing systems
- ✓ Video Surveillance
  - ➢ Software independence – "*If an undetected change or error in its software cannot cause an undetectable change or error in an election outcome*" (Rivest and Wack, 2006)
- ✓ Encrypted Imposter Files



HCCL

HUMAN CENTERED COMPUTING LAB





Prime III



One Machine, One Vote for Everyone

Juan E. Gilbert, Ph.D.
TSYS Distinguished Associate Professor
Fellow, AU Center for Governmental Services
Auburn University
Computer Science & Software Engineering
Human Centered Computing Lab
gilbert@auburn.edu
http://www.juangilbert.com/

