Outline

1. ENose Sensor
   - Brief Project Description
   - How it works
   - REU Do’s and Don’ts

2. Prime III
   - Background
   - Project Description
   - Prime III Security
   - Security Algorithms
   - Summary
   - Future Work
Brief Description of ENose Sensor

(I) Developed by NASA’s Jet Propulsion Laboratory (JPL) and with help from Caltech to monitor the air quality on the Space Shuttle and the International Space Station


(III) Sensor worked in Space
How does the ENose Work?

(I) Has 8 different sensors
(II) Each consist of carbon black based polymer films deposited on gold contacts
(III) Carbon black changes conductivity when exposed to different chemicals
ENose Sensor In Action

Figure: Figure 1: Sensors at Baseline

Figure: Figure 2: Sensor Reaction
REU Do’s and Don’ts

(I) Use your resources
(II) Be on time
(III) Network
(IV) Have a good attitude
Outline

1. ENose Sensor
   - Brief Project Description
   - How it works
   - REU Do’s and Don’ts

2. Prime III
   - Background
   - Project Description
   - Prime III Security
   - Security Algorithms
   - Summary
   - Future Work
Background and Problem Statement

(I) 2000 Presidential Election
   (a) Al Gore vs. George Bush
(II) Unassisted voting
(III) Secure voting
(IV) Universal Design
Voting Machines

Figure: Figure 3: Older Voting Machines

Figure: Figure 4: Modern Voting Machine
Prime III Project

(I) First version created in 2005 by HCCL

(II) Prime III is an electronic voting system
   (a) Audio/Voice
   (b) Audio/Touch
   (c) Audio/Touch/Voice
   (d) Touch

(III) Universal Design

(IV) Third Generation of Voting Systems
Prime III Operating Example

Figure: Figure 5: Sample Prime III screen with voice prompts and possible user responses
Security

(I) Separation between User and Prime III system
   (a) Limits user interaction

(II) Hidden aspects
   (a) Touch Screens
   (b) Headset Audio

(III) Uses authentication methods
   (a) Windows
   (b) SELinux

(IV) Uses imposter files and encryption

(V) Screen video recording
   (a) Voter-Verifiable Video Audit Trail (VVVAT)
Figure: Figure 6: Imposter Files Illustration
Figure: Figure 7: VVVAT Illustration
Security Algorithms

(I) Data Encryption Standard (DES)
   (a) Developed by IBM in the 1970’s
   (b) Uses a 64 bit key block size
   (c) Uses 56 bits during execution
   (d) Unsecure since development of DES Cracker

(II) Triple Data Encryption (TDES, Triple-DES)

(III) Advanced Encryption Standard (AES)
   (a) Designed by Vincent Rijmen and Joan Daemen (Rijndael)
   (b) Contest Winner for National Institute of Standards and Technology (NIST)
   (c) Uses a 128 bit key block size
   (d) Operates on a 4x4 array of bytes
(I) Employs a multimodal user interface

(II) Universal method of Voter Verification

(III) Implements intuitive security
   (a) video recorders
   (b) advanced encryption schemes with imposter files
   (c) physical security model.

(IV) Uses usable security model
Future Work

(I) Grasp security algorithm concepts
(II) Learn more about security code processor
(III) Think of ways to implement security code processor
(IV) Implement security code processor
Acknowledgements

(1) Ravi Patel
(2) Lehigh University
(3) Dr. Gilbert
(4) Human Centered Computing Laboratory