Secure Virtual Election Booth with Two Central Facilities

CSE505A Data Security

Janga Sireesha
So-In Chakchai

Washington University in St. Louis

Outline

- Introduction
  - Motivation
  - Secure Voting Requirements
  - Voting Protocols
- System Design
- Conclusion
- References
- Demonstration
- Questions

Washington University in St. Louis

Introduction

- Motivation
  - Convenience of online voting
  - Make use of today's amazing technology
  - Enhanced existing voting protocol with two central facilities
- Secure Voting Requirements
- Voting Protocols

Washington University in St. Louis

Introduction (cont.)

- Secure Voting Requirements
  - Only authorized voters can vote
  - No one can vote more than once
  - No one can determine for whom anyone else voted
  - No one can duplicate anyone else's votes
  - No one can change anyone else's vote
  - Every voter can make sure that his vote has been taken into account in the final tabulation
  - *(Everyone knows who voted and who didn't)*

Washington University in St. Louis

Introduction (cont.)

- General Voting Protocols
  - Voting with Blind Signatures
    - Voter generates 10 message sets containing identification numbers and the possible votes with a blinding factor and sends them to a CTF
    - The CTF verifies that nine of the ten sets are valid votes, signs each message in the tenth set and sends it back to the voter
    - The voter then unblinds the returned message set and selects his vote and submits his vote again to CTF

Introduction (cont.)

- General Voting Protocols (cont.)
  - Voting with Blind Signatures
    - If submitting a vote isn't completely anonymous, the CTF can determine how each voter voted
    - Nothing stops the CTF from generating its own signed/valid votes by itself (e.g. the CTF submits false votes)
    - Voter cannot prove that the serial number in question was actually his

Introduction (cont.)

- General Voting Protocols (cont.)
  - Voting without a Central Tabulating Facility
    - The voters themselves manage the election with out a central facility.
    - Each voter has a public/private key pair, and everyone knows each other's public keys.
    - Quite Complicated and extremely impractical amount of computation required
  - Voting with a single Central Facility
    - A corrupt CTF can allocate the votes of those who intended to vote but did not
    - Voter cannot verify or prove his vote

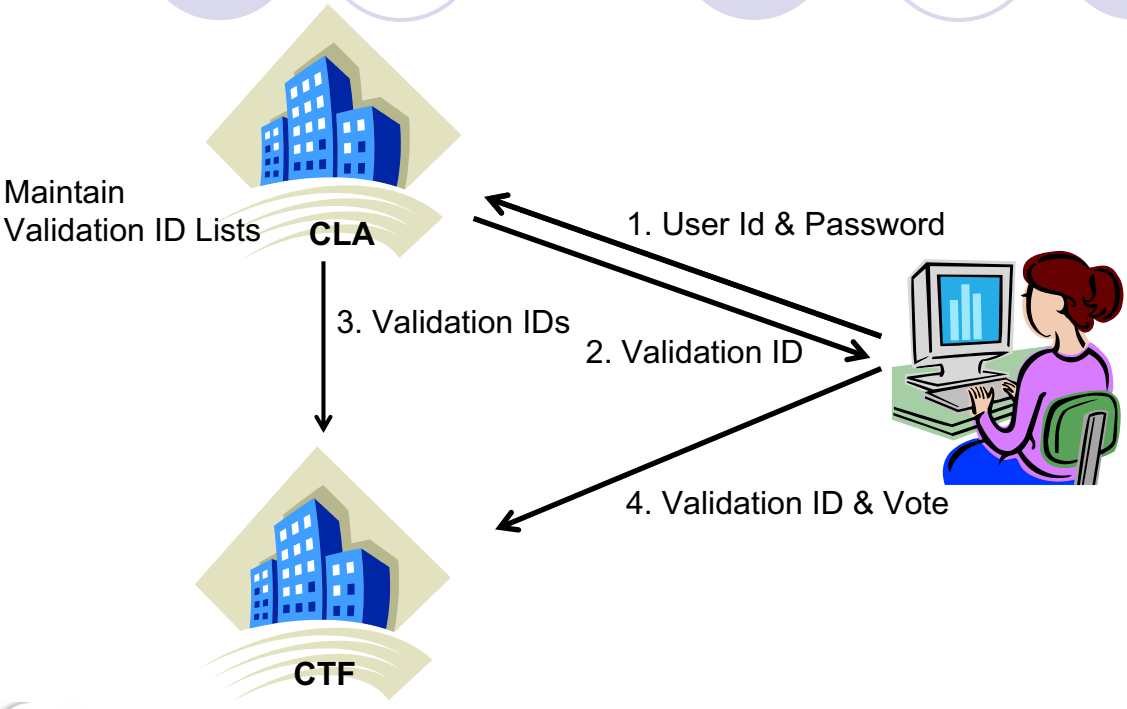
Washington University in St. Louis

Introduction (cont.)

- General Voting Protocols (cont.)
  - Voting with Two Central Facilities (VTCF)
    - CTF - Central Tabulating Facility - Used to compile results, process the election, and publish pertinent information
    - CLA - Central Legitimization Agency - Used to authenticate users
    - Voter – Client/GUI for interaction with voters.
  - VTCF Voting Communication
  - VTCF Pros & Cons

Washington University in St. Louis

VTCF Voting Communication



Washington University in St. Louis

VTCF (Pros & Cons)

- Pros:
  - CTF and CLA watch each other
  - The voter can make sure his vote was counted
- Cons:
  - The CLA could certify ineligible voters or certify eligible voters multiple times
    - CLA publish a whole list of certified voters
  - CLA and CTF work together
    - Make the different database with separate organization control
  - Voter cannot verify his vote *(Security Trade off)*
  - Once the user logs in, he has to vote

Washington University in St. Louis

Modified VCTF

- System Design
  - Secure Encryption Method
  - Modified VTCF Voting Protocol
  - Modified VTCF Voting Communication

Washington University in St. Louis

System Design

- Secure Encryption Method (flexible)
  - Platform : Java 1.4 (Platform independent & inbuilt security features)
  - GUI : Java Swing
  - RSA (1024 bits) : Public Key encryption
  - BlowFish (56 bits) : Symmetric Key encryption
  - SHA-1 (160 bits): Signature/Hashing
  - Nonce and Nonce+1 for returning message
  - CA : Secure Public Key Transmission

Washington University in St. Louis

Modified VTCF Voting Protocol

- Central Authority
  - PrCA[PuCLA] and PrCA[PuCTF]
  - PuCA (Voters)
- Voter & CLA (encrypted by Ks)

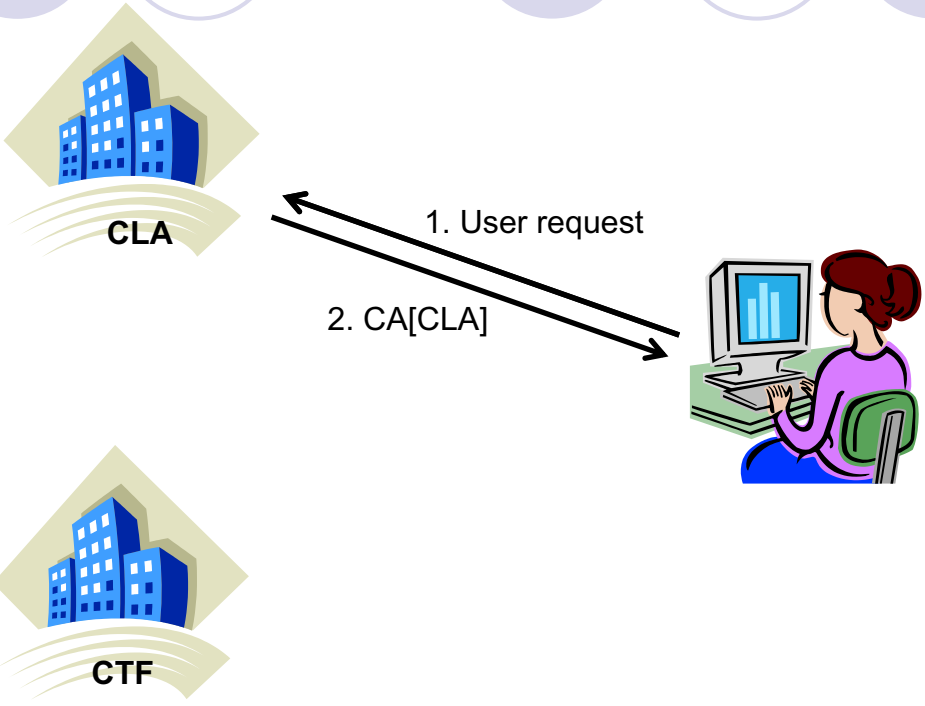
control	user	passwd	validation	nonce	signature

- Voter & CTF
- CTF & CLA

control	validation	id	nonce	signature

Washington University in St. Louis

Modified VTCF Communication



Washington University in St. Louis

Modified VTCF Communication

Maintain
Validation ID Lists

CLA

3. User Password

4. Validation ID

CTF

Washington University in St. Louis

Modified VTCF Communication

CLA

5. User request

6. CA[CTF]

CTF

Washington University in St. Louis

Modified VTCF Communication

CLA

8. CTF request

9. CA[CLA]

7. Control: Validation ID

CTF

Control:
Request Candidate
Request to Vote
Request to Verify Vote

Washington University in St. Louis

Modified VTCF Communication

CLA

10. Validation ID

11. Valid Validation ID

12. Control: confirm action

CTF

Control:
Candidate Lists
Confirm Vote
Verify Vote

Washington University in St. Louis

VTCF Requirements

- Only authorized voters can vote
  - There is a unique random validation ID for each user
  - It's computationally infeasible for an attacker to guess at a valid pair and also validation ID (the length is long enough)
  - Only CTF can cast a vote with valid validation ID
- No one can determine for whom anyone else voted
  - All transaction is secure and singed to prevent someone else to intercept the message

Washington University in St. Louis

VTCF Requirements (cont.)

- No one can vote more than once
  - CTF returns "Duplicate Vote" if Voter is already voted
- No one can duplicate anyone else's votes
  - Given the assumption that there is another secure channel to deliver user and password directly to each voter, nobody would know those from anybody else
- No one can change anyone else's vote without being discovered
  - Given random unique validation id and secure and signed transmission, nobody can change anyone else's vote even CTF

Washington University in St. Louis

VTCF Requirements (cont.)

- Every voter can make sure that his vote has been taken into account in the final tabulation
  - When Voter casts vote, CTF do count for the selected candidate and return the current and updated count back to Voter to insure if his vote has been taken to final round
- Everyone knows who voted and who didn't (Optional)
  - Given the recorded validation ID from CLA, CTF can provide the list of who voted by hashing validation ID

Conclusion

- Secure Online Voting
- Secure Voting Requirements
- Voting and Modified Voting with Two Central Facilities Protocol
- Buy and Sell votes

Reference

[1] Stallings William, "*Cryptography and Network Security*," Third Edition, Prentice Hall, 2004

[2] Schneier Bruce, "*Applied Cryptography*," Second Edition, Jon Wiley & Sons, 1996

[3] Salomaa, Arto, *"Public-key cryptography,"* Second Edition, Berlin New York, Springer, 1996

[4] Ronald L. Rivest, "*Electronic Voting,"* Laboratory for Computer Science , MIT

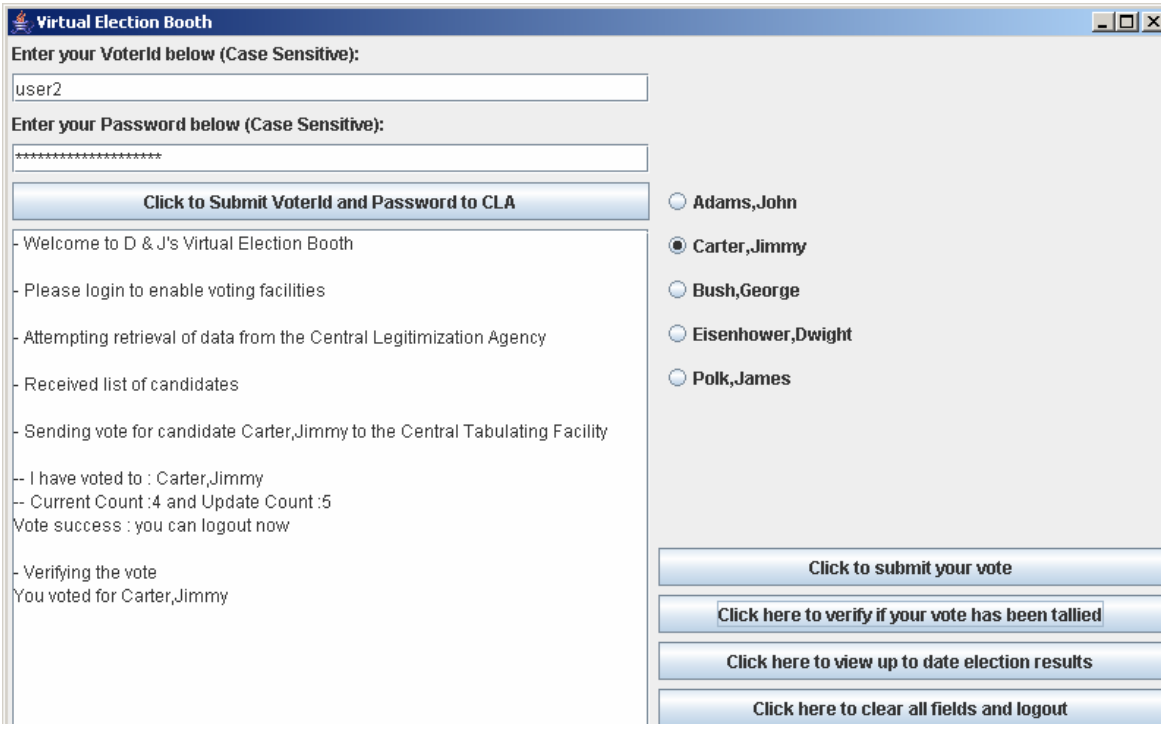
[5] Matt Zaske, "Seth and Matt's Digital Voting Presentation"

[6] JavaTM Cryptography Extension (JCE) Reference Guide: available online at *http://java.sun.com/j2se/1.4.2/docs/guide/security/jce/JCERefGuide.html*

[7] JavaTM Cryptography Architecture API Specification & Reference: available online at *http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html*

Washington University in St. Louis

Demonstration



Questions
?