12.03.2019

**CMPE-455 Term Project “Voting System”**

**Task**

Develop an **on-line** application on at **least two host computer systems** providing concurrent (parallel) work of four actors (participants) of the Voting System (VS) [1]: **A, central government, creator; B, local government, proxy creator; R, voter, registrant; voting committee, V.** VS [1] is reviewed briefly in Appendix 1 together with sample numerical data. It is a team work.

**Reports on the Term Project shall be handed 27.05.2019, before 12.00 to the Lab Coordinator Mr. Hossein G. Zefrehi or to Lab Assistant Mr. Tansel Sarihan, CMPE117.**

Report shall have

* 1. Cover page (University, Department, Course, Semester, Year, City, Country, Term Project subject, Team members, Lecturer, Lab assistants)
  2. Outline
  3. Problem definition (see **Task** above)
  4. VS [1] description
  5. Description of the tools used for the VS [1] implementation (programming tools, distributed system organization tools, communication tools, synchronization tools, database management system tools, web-server tools, etc.)
  6. Description of VS [1] implementation in your programming language/operating system
  7. Description of the system architecture including at least two host computers
  8. Description of the software system organization specifying parallel processes used for implementation of the creator, A, proxy creator, B, voter, R, and voting committee, V, their communication and synchronization
  9. Description of the data structures used for implementation of the creator, A, proxy creator, B, voter, R, and voting committee, V
  10. Description of the algorithms used for implementation of the creator, A, proxy creator, B, voter, R, and voting committee, V
  11. Description of the tests conducted and their results, **screenshots** of them
  12. Conclusion
  13. References
  14. Appendices with the code developed (shall be referred when giving explanations required in item 6 above. Appendices shall be structured, e.g., Appendix 1. Source code of the Creator process)

**Reports shall be printed and have attached CD’s with all related to the project information (report, design materials, sources, executables, etc.)**

**References**

1. S.-Y. Chiou, T.-J. Wang,, and J.-M. Chen, “Design and Implementation of a Mobile Voting System Using a Novel Oblivious and Proxy Signature”, *Security and Communication Networks*, 2017, vol. 2017, article ID 3075210, 16 pages, <https://doi.org/10.1155/2017/3075210>, https://staff.emu.edu.tr/alexanderchefranov/en/teaching/cmpe312/homework

**Appendix 1. Brief review of VS [1]**

The VS has six phases 1) set-up, 2) proxy, 3) registration, 4) circling, 5) voting, and 6) vote counting. In the phases, some data are generated by the participants, and some by a system process which may be attributed to the creator, A. Some data intended for common use are published in the bulletin board (BB). For secret data passing and digital signature, RSA encryption/decryption [4] and non-RSA modular exponentiations are used; these operations are the most computationally intensive in the VS. Also, for data hiding, some symmetric cryptography algorithm is used. We introduce the VS having the six phases below. To illustrate settings, in line with the VS description, we, for better understanding, provide some numerical examples using small values contrary to the large ones required by the protocol.

*VS [1] description*

1. *Set-up phase*
   1. *Two large primes, such that q|( are selected, e.g., . They are published.*
   2. *Two numbers such that are selected, e.g., . They are published.*
   3. *The creator, A, selects randomly its secret key, , and calculates its public key, , e.g., , and is published.*
   4. *The proxy creator, B, selects randomly its secret key, , and calculates its public key, , e.g., , and is published.*
   5. *B chooses two secret large primes, for RSA [4], e.g., .*
   6. *B computes , e.g., .*
   7. *B computes Euler’s totient function, , e.g., .*
   8. *B selects, such that , e.g., . RSA public key of B, , is published.*
   9. *B calculates , e.g., , which may be calculated using Extended Euclidean Algorithm [5]. B’s RSA secret private key is .*
2. *Proxy phase*
   1. *Creator, A, randomly chooses and computes , and , e.g., .*
   2. *Creator, A, RSA encrypts the pair, , using B’s public key, , forwards the encrypted pair to B, and publishes .*
   3. *Proxy creator, B, decrypts using its private key, , and checks whether holds, e.g., . If it does, B accepts proxy, and computes as his proxy signature, e.g., .*
   4. *B generates RSA signature, , and forwards it to A.*
   5. *A checks whether holds, if so, A approves the further work.*
3. *Register phase*
   1. *A voter, R, picks a pseudoname, pn, and password, pw, computes , encrypts using , and sends it to B, proxy creator.*
   2. *B decrypts using , and checks whether R is a legal user. If so, B stores in the system database, sets , calculates , and , returns to R, and publishes to the bulletin board, BB, where .*
   3. *R verifies RSA signature, whether is correct. If so, R has the right to vote.*
4. *Circling phase*
   1. *B sends a challenge, random number, , to R after receiving a login request from R.*
   2. *R computes , picks a random number, v, calculates , where is a list of candidates available for R from the bulletin board, BB, and is the number of the candidate of R’s choice, which is hidden in using random , and forwards to B.*
   3. *B examines whether is correct. If so, B checks whether holds. If it holds, B chooses randomly, calculates , and , returns , to R (these are blindly signed by proxy all candidates including the one selected by R) and sets .*
   4. *R computes , and, for every , R calculates and checks whether is correct. Thus, R checks correctness of the candidates list including R’s choice blindly signed by B. If it is correct, R computes , and sets . The final oblivious signature of R is .*
5. *Voting phase*
   1. *R calculates and uses it as a symmetric key to encrypt , produces a ciphertext, , and sends to the voting center, V.*
   2. *V first examines whether holds. If so, V publishes R’s ballot, , to the bulletin board, BB.*
   3. *Every voter, R, can check whether his/her ballot is received by V via the bulletin board, BB. If it is not published, then R resends the ballot to V.*
6. *Counting phase*
   1. *B forwards to the voting center, V,*
   2. *V decrypts using the symmetric key, , publishes to the bulletin board, BB, calculates , and verifies whether is correct. If so the signature is valid, and the ballot is counted.*
   3. *V publishes the voting result. Everyone can verify and count the ballots via the bulletin board, BB.*

*End of the VS [1] description.*