I. List of some of e-voting terms cited from different resources

Safety : ”limited effects of the possible failure of the system under normal circumstances” [1]. The property of system resistance against accidental attacks or failures during it’s normal operation, this kinds of atteck could happen due to software bugs or unexpected hardware failure. This property verifies the design correctness.

Security: ”system resistance against attack by attacker trying to make the system fail” [1]. The property of system resistance against intentional internal or external attacks trying to affect election result integrity. This property assessed by verifying the tamper-resistance of the design.

Note: e-voting as compared with paper voting is more safe (as it reduces the possibilities of errors both in votes casting and counting) but it is less secure (as more attacks exists in e-voting systems).

Resistance to disruption: ”means that it is difficult for an unintentional or malicious adversary to cause a delay, rescheduling, or stoppage of the election process” [2]. From this term, we can conclude that the term disruption refers to both of accidental and intentional attacks.

Actual security: ”security assessment by technical experts” [1].

Perceived security: ”security assessment by non-technical community” [1].

Reliable system: ”is the system that people can use confidently without having to worry about the details” [1].

System reliability: ”System development (design, implementation, maintenance, etc.) should attempt to minimize the likelihood of accidental system bugs and malicious code” [3].

Trustworthy system: ”is the system that people can assess the risk of and that they still want to use” [1].

Trust: ”people trust in system in term safety and security” [1].

Correctness in e-voting: ”Every participant should be convinced that the election tally accurately represents the sum of the votes cast” [4].

Secrecy in e-voting: ”requires that only the voter knows his voting decision and nobody else is able to gain information about it” [5]. Secrecy includes that votes are remaining secret while the voting is not completed.

Privacy: the insurance that there is no leak to sensitive information.

Voter privacy: The value of the vote casted by that voter is not known to anyone and only voter can learn how the he/she voted. [6],[2], [7],[4]. The rquirements of voter privacy are :

- voter must be able to privately and independently cast vote. [8],
- voter identitiy can’t be recorded or identified in casted votes after election [5], [8]. This requirement termed as **Anonymity:** ”the impossibility to link the vote to the voter who cast it” [5].

Accuricy: ensuring that voter’s intent is recorded and counted.[9]

Resistance to tampering: built-in checks and security that protect accuricy.[9]

Election integrity: ”means that each voter casts his ballot as intended; the system records the ballot as casted; the system tallies the votes as recorded; and the Election Boards certify the results as tallied” [2].

Receipt-freeness: ”the infeasibility for the voter to prove his vote (even if he wants to do so)” [5].

Coercion resistance: ”the infeasibility for an adversary to coerce a voter into casting his vote in a particular way” [5].

Another definition, **Coercion resistance:** ”No voter should be able to convince any other participant of the value of its vote” [4].

verifiability: ”means that voters have a way of checking that their votes where actually counted and that the published result of the election is correct” [7].

Another definition,**veriability:** ”allows voters and observers to verify that the election outcome corresponds to the votes legitimately cast” [10].

Individual verifiability: ”is commonly referred to as the possibility for any voter to verify that his vote was included in the tally” as cited by [5].

Another definition, **Individual verifiability:** ”a voter can check that her own ballot appears on the bulletin board” [7],[10].

Universal verifiability: ”can be summarized as the possibility for any observer to check that the tally has been correctly computed. Some authors include the property that the tallied votes were cast by legitimate voters in the notion of universal verifiability [11],[12]” [5].

Another definition, **Universal verifiability:** ”requires that anyone can check that the election outcome corresponds to the ballots published on the bulletin board” [7],[10].

end-to-end verifiability: ”to emphasise voter’s ability to verify the results of the entire election process” [10].

Eligibility veriability: ”anyone can check that each vote in the election outcome was cast by a registered voter and there is at most one vote per voter; and, a voter can check that her own vote is considered legitimate” [10].

Note : ”The concept of election veriability signicantly reduces the necessity to trust electronic systems, by allowing voters and election observers to verify independently that votes have been recorded, tallied and counted correctly” [10].

A bulletin board: ”is a public channel where data can be published by authorized participants only and, once published, cannot be erased or overwritten by anyone” [5].

Another definition, **bulletin board:** ”refer to the output produced at the end of an election process” [10].

References

[1] b. . K. t. . A. p. . S. p. . . y. . . W. Pieters, series = Lecture Notes in Computer Science, vol. 3986.

[2] A. T. Sherman, A. Gangopadhyay, S. H. Holden, G. Karabatis, A. G. Koru, C. M. Law, D. F. Norris, J. Pinkston, A. Sears, and D. Zhang, "An Examination of Vote Verification Technologies: Findings and Experiences from the Maryland Study," in *EVT*, 2006.

[3] P. G. Neumann, "Security criteria for electronic voting," in *Proc. 16th National Computer Security Conference*. Baltimore, Maryland: NIST/NCSC, Sep 1993.

[4] J. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections (extended abstract)," in *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*. ACM, 1994, pp. 544–553.

[5] L. Langer, A. Schmidt, M. Volkamer, and J. Buchmann, "Classifying privacy and verifiability requirements for electronic voting." in *GI Jahrestagung*, vol. 154. GI, 2009, pp. 1837–1846.

[6] C. N. Donald F. Norris, Andrew S., "A Study of Vote Verification Technologies Part I: Technical Study," National Center for the Study of Elections of the Maryland Institute for Policy Analysis & Research, Tech. Rep., 2006.

[7] R. Küsters, T. Truderung, and A. Vogt, "Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study," in *IEEE Symposium on Security and Privacy (S&P 2011)*. IEEE Computer Society, 2011, pp. 538–553.

[8] N. Ansari, P. Sakarindr, E. Haghani, C. Zhang, A. K. Jain, and Y. Q. Shi, "Evaluating electronic voting systems equipped with voter-verified paper records," *IEEE Security and Privacy*, vol. 6, pp. 30–39, May 2008.

[9] "Voting systems advisory council: Initial report to monroe county commissioners," Voting Systems Advisory Council, Tech. Rep., 2009. [Online]. Available: http://www.co.monroe.in.us/tsd/Government/Commissioners/VotingSystemsAdvisoryCouncil.aspx

[10] S. Kremer, M. Ryan, and B. Smyth, "Election verifiability in electronic voting protocols," in *Proceedings of the 15th European conference on Research in computer security*, ser. ESORICS'10. Springer-Verlag, 2010, pp. 389–404.

[11] M. Hirt, "Multi-Party Computation: Efficient Protocols, General Adversaries, and Voting," Ph.D. dissertation, ETH Zurich, 2001.

[12] W. D. Smith, "New cryptographic election protocol with best-known theoretical properties." Frontiers of Electronic Elections, 2005.