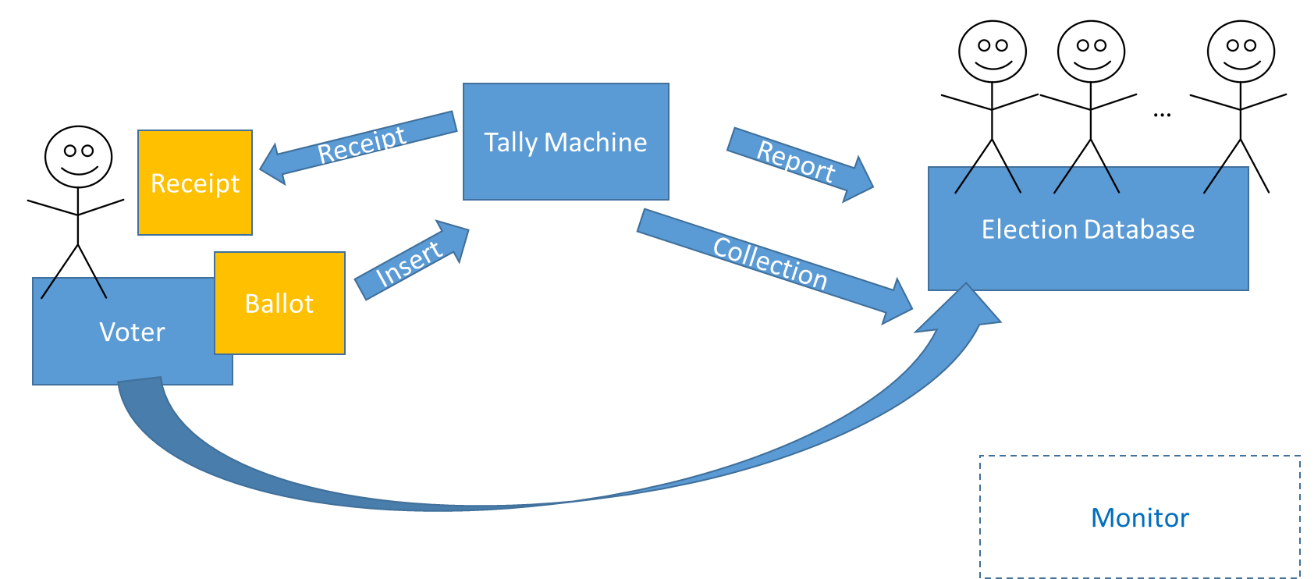
CS 6600 Take Home Final – Due 12/14, 10:30 AM CST in rm 325 CS.

This exam is to be solely your own work and fall under the jurisdiction of 200.010, Conduct of Students <https://registrar.mst.edu/academicregs/>. Any Academic Dishonesty will be dealt with by assigning a 0% grade for the exam and the incident reported to the primary administrative officer that investigates student misconduct.

Exam:

This exam considers the problem of an electronic voting (e-voting) system. Voting systems have conflicting requirements[[1]](#footnote-1), auditability vs. ballot secrecy. For this exam, consider an e-voting system constructed as follows:



Subjects: Voter (V), Tally Machine (TM), Election Database (E), Monitor (M)

Objects: paper Ballot (B), Receipt/Code (C), Vote (v)

The Voting Process works as follows. A Voter takes a ballot *B*, marks their selections, and inserts *B* into the Tally Machine *TM* which records the vote, *v*, and produces a receipt with a unique code *C* on it. *v* and *C* are submitted to the election database *E* where humans verify *v* (but do not see *C*). *E* also collects *B*. The Monitor is there and can be attached to anything, but does not currently function.

*V* may query *E*, using *C* to ask if their vote exists in *E* and what *v* was stored, both messages are transmitted over a secure channel.

Questions:

1. Consider a BLP model of
   * 1. High Security: *E*
     2. Medium Security: *TM*
     3. Low security: *V,v,B,C*
2. Does the system function according to the Voting Process? Show formally within the BLP command structure. (10 pts) If not, show how to adjust the BLP model to satisfy the Voting Process (10 pts).
3. Is either system secure from an attack where another voter V’ can determine the vote that V made? (10 pts)
4. Consider a NI/NF/ND/MSDND model where each domain is labeled as above, but are not hierarchical.
   1. Show, formally, that TM’s behavior is MSDND (or ND) to E. (10 pts)
   2. Show, formally, that V’s behavior is MSDND (or ND) to E. (10 pts)
   3. Show, formally, that TM’s behavior is
      1. MSDND (or ND) to V (10 pts)
      2. not NI from TM to V (10 pts)
   4. What can you conclude about this e-voting system from the above analyses (15 pts)?
5. Show how a Clark-Wilson style IVP implemented in the monitor can mitigate the MSDND portion of 2a, above. Does your solution violate the MSDND portion of 2b, above? (15 pts)

1. S. Peisert, M. Bishop, Security and Elections, IEEE Security and Privacy, Sept.-Oct. 2012, pp. 64-67, vol. 10, [10.1109/MSP.2012.127](https://doi.ieeecomputersociety.org/10.1109/MSP.2012.127) [↑](#footnote-ref-1)