CS 6600 Take Home Final Fall 2021

Matthew Whitesides

1) Considering the Voting System BLP model.
   a) The BLP model of the system does not currently function according to the Voting Process? The fact that "TM records v and produces c" violates the *-Property of the BLP model by allowing the subject *TM* with a security level of **Medium** to write to the object c with a security level of **Low**.

      To show this we can define our formal model as follows:
      $S = \{V, TM, E, M\}, O = \{b, c, v\}, P = \{r, w\}, C = \{High, Medium, Low\}, K = \{ALL\}$
      $f_c(S) \in \{(Low\{ALL\}), (Medium\{ALL\}), (High\{ALL\})\}$
      $f_o(O) \in \{(Low\{ALL\}), (Medium\{ALL\}), (High\{ALL\})\}$

      Now we can suppose:
      $b_1 = \{(TM, c, w)\}$
      $f_c, 1(TM) = \{(Medium\{ALL\})$
      $f_o, 1(c) = \{(Low\{ALL\})$
      $V_0 = (b_1, m_1, f_1) \in V$
   b) Is either system secure from an attack where another voter V' can determine the vote that V made?
2) Consider a NI/NF/ND/MSDND model where each domain is labeled as above, but are not hierarchical.
   a) Show, formally, that TMHs behavior is MSDND (or ND) to E.
   b) Show, formally, that V's behavior is MSDND (or ND) to E.
   c) Show, formally, that TM's behavior is:
      i) MSDND (or ND) to V.
      ii) Not NI from TM to V.
3) 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?

ACKNOWLEDGMENT

The author would like to thank Professor Bruce McMillin with the Department of Computer Science, Missouri University of Science and Technology.

Matthew Whitesides Master's Student at Missouri University of Science and Technology.