DRAFT

5-30-12

Trust-el Phase Two Analysis Criteria

1. Questions to ask:
   1. How does the method improve trust?
   2. How does the method address the following threats (from x1254 and OneID lists)

|  |  |
| --- | --- |
| T.OnlineGuessing | The degree to which the technique minimizes the threat of online guessing as defined in X.1254 |
| T.Eavesdropping | The degree to which the technique minimizes the threat of offline guessing as described in X.1254 |
| T.ReplayAttack | The degree to which the technique minimizes the threat of eavesdropping as described in X.1254 |
| T.ManInTheMiddle | The attacker positions himself or herself between the entity and relying party so that he or she can intercept and alter the content of the authentication protocol messages. The attacker typically impersonates the relying party to the entity and simultaneously impersonates the entity to the verifier. Conducting an active exchange with both parties simultaneously may allow the attacker to use authentication messages sent by one legitimate party to successfully authenticate to the other. |
| T.SpoofingAndMasquerading | The degree to which the technique minimizes the threat of spoofing and masquerading as described in X.1254 |
|  |  |

* 1. Are there implementation requirements for  
     improving trust? If so, what are they and why are they necessary?
  2. Are there privacy and/or confidentiality issues  
     engaged when using the method? Are there reasonable solutions for potential  
     privacy impacts?
  3. What are the usability issues when using the method? Are there reasonable solutions for potential usability impacts?

1. Ontological query (post analysis):
   1. Is there a generic “family” of methods (perhaps  
      in mechanism for raising or enabling trust); a cluster of “families” or is each  
      identified method its own “family?”
   2. Are there any implications, which we should be aware of, to the answer to “a”  
      above?