|  |  |
| --- | --- |
| *Trust Elevation Method:* | Context consists of any additional attributes relevant to the user or situation. Some of these are specific to other trust elevation methods and some are generic. Context-based trust elevation can adjust dynamically to the circumstances surrounding the transaction based on the risk mitigation needs of the relying party application, and, it only needs to be invoked when needed. Context includes, but is not limited to:   * Location; * Time of access; * Frequency of access; * Party; * Prior relationship ; * Social relationship; * Source and endpoint identity attributes such as   + Date of last virus scan   + IP address   + Subscriber identity module (SIM)   + Device basic input/output system (BIOS)   + Virus scan software version   + CallerID   + Cookie (presence and/or contents); * Multi-channel combination; * Credential lifecycle attributes; * Certificate binding and or other chain of trust attributes; * Secure device with user specific disk allocation. |
| Questions: |  |
| Which party is performing the method? | Relying Party |
| How does the method improve trust? | This method looks past the inputs of the human user to the attributes associated with the transaction. Attributes considered for trust elevation from one level to another is based on the assurance required for each level. Each assurance level determines the types and combination of attributes that will be needed to verify before elevating trust of the user. A human user is trusted more when the transaction initiates and occurs within a familiar location and during a familiar time frame of user activity. If the same user were to initiate a transaction from an unfamiliar location and during unexpected time frame, then trust upon the individual would be significantly reduced and the customer may need to present supplemental credentials to elevate trust. |
| How does the method address the threat of eavesdropping? | Attributes collected and used outside of a transaction session could be used to address eavesdropping. Attributes collected during a session can be altered if they are not collected using a secure connection. |
| How does the method address the threat of online guessing? | This method does contain information that can be guessed, however, a requirement for a combination of multiple attributes for a particular assurance level would help to address the threat of online guessing. The combination requirement is determined by a predetermined “trust score” for a particular assurance level. |
| How does the method address the threat of replay attack? | This method by itself will not address the threat of replay attack |
| How does the method address the threat of man in the middle? | A combination of multiple attributes - both session and non-session based (knowledge based) would address the threat of man in the middle to a certain extent, but not completely. |
| How does the method address the threat of spoofing and masquerading? | A combination of multiple attributes - both session and non-session based (knowledge based) would address the threat of man in the middle to a certain extent, but not completely. |
| Are there implementation requirements for improving trust? If so, what are they and why are they necessary? | 1. The relying party needs to establish baseline attribute data before enforcing this method. 2. A human who is just introduced to the relying party system may not be trusted as much as a human who has been interacting with the system for years. 3. The system need some time to learn about the user before enforcing this method. 4. User may need to go through a registration process with the system to provide baseline attribute data as well as information that would help the system to collect supplemental non session attribute data. |
| Are there privacy and/or confidentiality issues engaged when using the method, such as user consent for attribute release/exchange? Are there reasonable solutions for potential privacy impacts? | Yes. The relying party may collect sensitive information on the human user and the relying party needs to get consent from the user before collecting and using such data. Use of access controls and cryptography may reduce threat of loss of personal identifiable information, however, that does not mitigate the risk of collecting unauthorized data on an individual. Consent is required. Greater protection is required for PII than for general data. |
| What are the usability issues when using the method? Are there reasonable solutions for potential usability impacts? | This method is particularly well-suited to customer usability as it requires little or no user interaction for the typical session. However, user need to go through a one time registration process to establish baseline attributes and the user needs to provide some kind of identity authentication to the system for each session before the method can be enforced. |