|  |  |
| --- | --- |
| *Trust Elevation Method:* | [description] What you typically do consists of attributes related to an individual’s repeated behaviors or behavioral habits. We differentiate this category from biometric behaviors that have a physical component such as key signature and voice. It includes attributes related to correlation or statistical analysis of browsing patterns (order in which pages are accessed, duration of access, links accessed, etc.); |
| Questions: |  |
| Which party is performing the method? Include details of multiple parties and attestation where appropriate. | The Relying Party. Generally there is no other party involved. This method depends on information that the RP has gained via previous accesses to its own site. |
| How does the method improve trust? | This method provides an additional opportunity to detect impersonations. |
| How does the method address the threat of eavesdropping? | If a person succeeds in fraudulently gaining access via eavesdropping, this method may indicate that the person is unlikely to be who they say they are so that additional actions can be taken. |
| How does the method address the threat of online guessing? | If a person succeeds in fraudulently gaining access via online guessing, this method may indicate that the person is unlikely to be who they say they are so that additional actions can be taken. |
| How does the method address the threat of replay attack? | If a person succeeds in fraudulently gaining access via a replay attacking, this method may indicate that the person is unlikely to be who they say they are so that additional actions can be taken. However a sophisticated attacker may also be able to replay enough of the user’s behavior to elude the browsing patterns analytics engine |
| How does the method address the threat of man in the middle? | If a person succeeds in fraudulently gaining access via a man in the middle attack, this method may indicate that the person is unlikely to be who they say they are so that additional actions can be taken. |
| How does the method address the threat of spoofing and masquerading? | If a person succeeds in fraudulently gaining access via spoofing and masquerading this method may indicate that the person is unlikely to be who they say they are so that additional actions can be taken. |
| Are there implementation requirements for improving trust? If so, what are they and why are they necessary? | This method does not work on the first visit to a site. It works better after many visits. |
| How does the method address the threat of theft | This method works even if all credentials are stolen because it does not rely on any credential. |
| How does the method address the threat of phishing? | If a person succeeds in fraudulently gaining access via phishing, this method may indicate that the person is unlikely to be who they say they are so that additional verifications can be performed. |
| How does the method address the threat of credential duplication? | This method works even if all credentials are duplicated because it does not rely on any credential. |
| How does the method address the threat of session hijacking? | This method could potentially detect session hijacking if the hijacker engages in different behaviors than the actual user, as long as the session hijacking doesn’t include replay of browsing patterns. . |
| 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? | Since analysis of browsing patterns is only valid for the site on which the browsing patterns were gathered, typically information is not shared with any other party so there are no confidentiality issues. If the RP’s site was hacked, the browsing pattern information could be captured. This information would typically not include any PII. |
| What are the usability issues when using the method? Are there reasonable solutions for potential usability impacts? | This method does not require any action on the part of the user so its usability is high. If an anomaly is detected, then the user may be challenged to further identify themselves. If the algorithm is tuned to be too sensitive there could be too many unnecessary challenges. Ideally the analysis algorithms should be designed so that if the RP makes standard changes to their site, browsing behavior that was previously collected can still be used. Otherwise this method would stop working for a period, each time the website was changed, and create an unacceptably high level of false negatives. |