

[0080] In the example shown in FIG. 2, the static confidence window is established a priori and the required confidence threshold falls within this bounded range of confidence. If the authentication threshold had fallen outside this window, authentication will be inhibited and no further analysis is needed. It is anticipated that this embodiment will simplify the function of the Rule Base as it constrains the number of confidence parameters for a given context.

[0081] Returning to the generalized form of the invention, its dynamic nature is exemplified by the system dynamically informing the user of whether or not the confidence level meets the confidence threshold. The user can then alter the confidence level, either autonomously or in response to a request from the system. This is done by varying and/or adding one or more confidence parameters such as the user repeating a login process, changing their location or performing a similar action which, although under the control of the user, nevertheless verifies that the user is authorized to access the resource.

[0082] Autonomous changes in confidence parameters may occur when the system itself detects a change in an extrinsic factor such as network routing or firewall/proxy behaviour which can affect the confidence level without the users input.

[0083] FIG. 3 illustrates the situation where the upper bound of the confidence window changes. As discussed above, the confidence window reflects confidence parameters which are considered fundamental and substantially static for a specified transaction context. Such parameters include the characteristics of the user device. In FIG. 3, the effect of changing the device characteristics is shown by the step in the upper confidence bound. The device security has increased and therefore the potential future confidence level range has been expanded. FIG. 4 illustrates a dataflow graph for an exemplary transaction where an authentication request fails and the transaction context is therefore re-authenticated. A GetResource request is sent from a requester to the system, i.e.: from a users device to the system shielding the resource. In this embodiment, this is done by transmitting the request 40 to the Guard & Monitor 16 which shields the resource from the outside world. The Guard & Monitor 16 gets the CurrentConfidence 41 from the Confidence Engine 15 which dynamically monitors the confidence level of the transaction context. The Confidence Engine 15 then requests 42 the Device Capability from the device. In the present example, this act is such as to decrease the confidence level 43. This may be due to the device not being sufficiently sophisticated in terms of security. In response, the Confidence Engine sends a request 44 to an Authentication Mechanism which requires the user to re-authenticate. The result of this 45 is sent back to the Confidence Engine 15 where the changed Confidence Level is transmitted 46 to the Guard whereupon, the Guard & Monitor 16 authenticates the transaction and gets the resource 47. The resource is transmitted 48 to the Guard & Monitor and then passed to the Requestor 49.

[0084] FIG. 5 illustrates the confidence update process. Here, the Rule Base 19 operates by applying a one-to-one mapping between the known event type and the known event confidence. The Rule Base can be updated by a number of mechanisms. New rules may be included by acts such as the user device loading new functionality, for

example virus monitoring functionality, from the web. Other possibilities include devices exchanging new rules in a peer-to-peer manner. Also, the owner of the resource can classify the meaning of a specific authentication event.

[0085] In a preferred embodiment, the system will operate according to the central maxim that the highest level of trust cannot authenticate transactions which require a higher confidence level than the confidence level of the users input device. To this end, a further simple example of an application of the invention can be used to illustrate an implementation of the dynamic authentication process.

[0086] According to this scenario, a user working for an insurance company possesses 30 several handheld devices and a standard laptop. The user travels frequently and needs to access sensitive personal and company information when required. Transactions performed with the laptop operating as a standalone device are trusted (i.e.; meet the required confidence threshold). However, the user is aware that certain data should not be displayed in certain environments such as at the airport. Use such as this is considered to be insecure as someone standing close by could view the potentially sensitive data. Also, while the data might be legally able to be viewed in The United States, such viewing in the European Union could violate the European Data Protection Rights.

[0087] The user trusts his laptop for the initial authentication mechanism. However, the subsequent context such as location and sensing the proximity other users, indicates that the level of trust should be lower. This sensing may done be using specific hardware to detect the other people, or be predicated upon a set of assumptions about the location and behaviour of the user which defines a statistical likelihood that the security assumptions relating to the situation is in fact correct. The user may therefore be prompted to re-authenticate under new conditions or will simply be denied access to the data. This will depend on the threshold set by the local policy in relation to this class of sensitive data.

[0088] If the user is denied access via his laptop, he or she may switch to a different output device such as a mobile phone and obtain the information via audio streaming of the data. This context assumes that "listening" to the data is acceptable and therefore the confidence level exceeds the confidence threshold for the given transaction context. In order to re-authenticate in this physical context, the user would perhaps need to authenticate with a smart card and possibly use some type of biometric sensor which ensures that the correct person is in fact listening to the data.

[0089] Other more complicated transaction contexts can be constructed involving combinations of factors such as location, user device and user behaviour. Indeed, it is envisaged that in extended embodiments of the invention, confidence data could be accumulated based on assumptions about the behaviour of the user

[0090] For example, the determination of the confidence level might involve a set of assumptions about periodic behaviour of the user such as the statistical likelihood that a user will be in a particular location at a particular time or looking at the users spending patterns. Such assumptions may be used to abbreviate the authentication process by requiring a lesser confidence level. However, it is also possible that non-periodic or chaotic behaviour of the user