

[0040] when the confidence level is above the confidence threshold, authenticating the transaction;

[0041] a plurality of authentication means adapted to dynamically provide, to the confidence engine, confidence parameters relating to the security of the transaction context.

[0042] Preferably the system further includes a rule database adapted to correlate the plurality of confidence parameters with the confidence level.

[0043] Preferably the system further includes a guard means adapted to act as a proxy for the resources which are the subject of the transaction.

[0044] Preferably the system further includes device means adapted so that the user can interact with the authentication system, wherein the device has an authentication level which is taken into account when authenticating the transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

[0045] The present invention will now be described by way of example only and with reference to the drawings in which:

[0046] **FIG. 1:** illustrates a simplified schematic of an embodiment of a dynamic authentication system;

[0047] **FIG. 2:** illustrates a time-varying authentication process;

[0048] **FIG. 3:** illustrates a time-varying authentication process where the device characteristics change;

[0049] **FIG. 4:** illustrates a dataflow diagram for an example of a transaction authentication; and

[0050] **FIG. 5:** illustrates the process of updating the Rule Base.

BEST MODE FOR CARRYING OUT THE INVENTION

[0051] The present invention will be described in the context of a generalized abstract model of a transaction and the security issues surrounding it as well as a number of specific exemplary embodiments.

[0052] The description of these embodiments follows a transaction request/authentication model. This approach is considered to be a useful framework describing the exemplary embodiments below. However, it is to be understood that the method of the invention is inherently dynamic and could equally be described by considering a process which focuses on sequentially or concurrently accessing resources on a network having specific access control levels.

[0053] Referring to **FIG. 1**, a high-level functional diagram of an embodiment of the invention is shown. The various components in **FIG. 1** are intended to be representational only and their functionality may be implemented using a range of technologies and suitable hardware. Examples will be given where they help illustrate the operation of the functional block.

[0054] The authentication system shown in **FIG. 1** includes a confidence engine **15** which is adapted to dynami-

cally maintain at least one confidence level by monitoring (**21, 22, 23**) a plurality of confidence parameters. The confidence engine **15** may be an application running on a server.

[0055] Confidence parameters are numerical or logical metrics which correspond to specific measures of the confidence inherent in various aspects of the transaction.

[0056] It can be helpful to classify these parameters in two ways, intrinsic and extrinsic.

[0057] Intrinsic context parameters are those which can be considered to be under the control of, or within the scope of, the user. These include things such as the physical characteristics and security features of the user input device, the users location, the users identity, co-location of multiple users or individuals and the elapsed time after the users initial authentication request or most recent authentication act.

[0058] Extrinsic context parameters include thing such as changes in communications network characteristics, the security of the authentication system itself and dynamic changes in the sensitivity of the transaction.

[0059] An extrinsic confidence parameter may perhaps even reflect a transitory circumstance decoupled from the transaction context itself. For example, the authentication system might be able to take into account the security history of the environment. Such history might include a suspicion that the system may be susceptible to a hacking attack or has been the subject of a recent hacking attack. In this case, additional authentication may be required to allow the transaction to proceed. Other historical factors might also include susceptibility to particular viruses etc. Taking these factors into account will complicate the function of the Rule Base. However, it is considered that the invention may be extended to this degree of complexity.

[0060] Extrinsic confidence parameters can also include the required transaction security level or the resource security level that must be achieved in order to access that resource. It is noted that when static, these parameters can be used to define the confidence level which must be attained by the user. That is, the confidence threshold which must be exceeded for authentication to be achieved and the transaction to proceed. An alternative preferred embodiment of the invention uses the concept of a confidence window to simply the confidence level comparison. This will be discussed in detail below.

[0061] The confidence level reflects the security of the transaction context and can be thought of as a dynamically determined measure of the security of the transaction at a point in time. The confidence level can change, for example as the user changes location, re-authenticates or uses two different devices in close proximity. Other confidence parameter changes are possible.

[0062] As noted above, the confidence engine compares the confidence level derived from the confidence parameters with a predetermined confidence threshold. When the confidence level is below the confidence threshold, the confidence engine requests new confidence parameters or alternatively or in combination, varies existing confidence parameters. When the confidence level is above the confidence threshold, the confidence engine authenticates the