

DYNAMIC USER AUTHENTICATION

TECHNICAL FIELD

[0001] The present invention relates to user authentication. More particularly, although not exclusively, the invention relates to processes and apparatus for verifying the identity of a user or process initiated by a user for the purpose of accessing resources, performing operations, retrieving data and the like. More specifically, although without limitation, the present invention relates to the evaluation or determination of an authentication process based on static and dynamic context parameters.

BACKGROUND ART

[0002] As a preliminary point, the following discussion will refer to user and process authentication. User authentication will be familiar to the reader in terms of a dynamic or interactive verification process occurring in real time between a user and a resource. However, it is anticipated that the invention may be implemented in situations where a process needs to be authenticated. In this case, a user might initiate a process which itself requires authentication when it is initialized or operates. An example of a process might be performing a sequence of financial transactions whereby a user submits a descriptor file which accesses and manipulates financial records. This indirectly authenticates the user and the validity of the transaction. It is anticipated that scenarios may exist where process authentication can be considered distinct from an interactive form of user authentication. Such variations are considered to be within the scope of the present invention. Although the discussion has referred generally to the concept of a 'transaction', this operation includes within its scope the specific class of action of accessing a resource. A resource may be a database, document or similar. In this case, the sensitivity of the resource would be predefined according to external criteria.

[0003] A binary login process exemplifies the simplest type of user authentication. This type of process usually requires two input parameters: a login identifier, or userid, which identifies the user to the recipient system, and a password which verifies that the user is in fact the authorized, or trusted, user of that identifier. This type of authentication is suited to situations where the security context of the user is well known for a particular transaction context and does not change over time. Once a user is authenticated in such a system, the security of the transaction is assumed to be one hundred per cent or within the anticipated confidence level of the login and password mechanism.

[0004] Binary approaches such as this are satisfactory in contexts where the confidence in the security level is static and assured. An example is where a user logs into a desktop personal computer in an office environment. Here, extrinsic security effects such as restricted access to the input machines themselves increases the anticipated security and confidence level of the interaction as does the existence of a secure static physical data link between the users computer and the remote data or resource which the user wishes to access.

[0005] It is known to implement stepped or incremental forms of authentication in situations where the transaction or desired resources have varying levels of trust-sensitivity.

[0006] An example of this situation might be where a user logging into a corporate intranet is automatically allowed access to internal company documents. However, to access sensitive resources a secondary and perhaps tertiary, login process would be required. According to this example, an employee might have access to company resources such as memos, procedures, news and internal library catalogues. However, a member of the companies legal department might need access to confidential and highly sensitive documents such as legal pleadings and material which is restricted to specific people or organizations within the corporate, but is nevertheless stored on the same intranet. In this situation, when attempting to access the trust-sensitive materials, the user is presented with a secondary login process which requires that the user is authenticated before he or she is allowed access to these specialized resources.

[0007] Such incremental login processes are common in intranets using HTML-based resources whereby attempts to access a restricted url produces a login and password dialogue. In this example, this secondary login would require that a user identifier be input, which identifies the user as being a member of a group of allowed users, along with a password which verifies that the user is actually a trusted member of that group.

[0008] These forms of incremental authentication systems are adequate when used in contexts where the transaction context is static and predetermined. In such cases, the confidence in the security of the transaction context is predicated on an a priori assumption about the behaviour of the user

[0009] Other more complex authentication systems include those which rely on the input of a token or a biometric parameter uniquely identifying the user.

[0010] One example of a token-based authentication system is predicated on the user having a userid and password as well as having access to a token generator. To achieve authentication, the user performs a two-step authentication comprising a standard binary login followed by a token authentication. The token is obtained from a device in the users possession. The token generator can itself require the input of a secure key or personal identification number (PIN) whereupon the token is generated. The confidence level in this case is increased by the token generator using a secure encryption technique. The authenticating process shielding the desired resource evaluates the token that is input and authentication is achieved if the token is decrypted or otherwise evaluated correctly.

[0011] In this case, the confidence level of the transaction is higher as not only does the user need to know the initial binary userid/login information, he or she also must have access to, and be able to properly operate, a correct physical token-generating device. Since the aim of authentication is to prevent unauthorized access to resources, the confidence level of such an interaction will be higher than if a user merely carried out a userid/login binary authentication process.

[0012] Biometric authentication is currently still the subject of research and there are relatively few practical systems in use at this time. Those that are presently feasible use iris scanning, fingerprint matching and the identification of similar forms of unique biometric input unique to the user.