TOKEN SHARING SYSTEM AND METHOD

Cross-Reference to Related Application

[0001] This application claims the benefit of provisional application Serial No. 60/678,214 filed May 6, 2005, the disclosure of which is hereby incorporated in its entirety by reference herein.

Field of the Invention

[0002] The field of the invention is computer security, in particular authentication.

Background of the Invention

[0003] Enterprises are known to employ strong authentication techniques to protect the confidentiality, integrity and assured service of their data and information technology. This has been accomplished using a variety of methods, including issuing a digital certificate to each employee, providing a token to each employee, etc. Strong authentication for an enterprise can be relatively straightforward to implement because there is generally a single entity to which a controlled group of users must authenticate themselves, i.e., the enterprise itself.

[0004] It can be difficult to apply strong authentication techniques for consumer applications. Digital certificates and tokens can be perceived as an encumbrance to the consumer's interaction with other entities, such as merchants, and can be an expense that neither the consumer nor the other entity is willing to bear. However, the consumer's willingness to adopt certain strong authentication techniques can be expected to grow in view of the increasingly sophisticated and damaging threat posed by hackers, such as identity theft, phishing, man-in-the-middle attacks and credit card theft. This is further accentuated by the increasing amount of commerce and other activities that take place online each year.

[0005] Indeed, the unanswered threat of compromise and the resultant accumulation of negative events can itself be considered a modern impediment to the continued migration of consumer activities to an online environment. Although stronger authentication is needed for the consumer, certain known solutions can be difficult to implement. For example, unlike most enterprise clients, a consumer must authenticate itself to a broad range of diverse entities. A consumer typically may not want to keep track of a different authentication credentials that are associated with

different entities. For example, many consumers have multiple bank, credit card, service provider, healthcare and government accounts. Each of these could benefit from strong authentication by the consumer. In this case, if the consumer is issued one authentication device per account, he or she may potentially have a pocket or key ring full of devices. This may be undesirable to the consumer.

[0006] What is needed is an authentication system and method that can operate using a shared token that can be used by the consumer to authenticate himself to a wide variety of enterprises. If a single token can be shared across many sites, then it is much more likely that the consumer will begin to carry it around as a necessary personal tool much like a cell phone, car keys or credit cards.

Brief Description of the Drawings

[0007] Figure 1 shows a centralized validation service in accordance with an embodiment of the present invention.

[0008] Figure 2 shows a distributed validation service in accordance with an embodiment of the present invention

[0009] Figure 3 shows a credential wallet architecture in accordance with an embodiment of the present invention.

[0010] Figure 4 shows a cell phone implementation of a single device that can generate multiple tokens in accordance with an embodiment of the present invention.

Detailed Description

[0011] As used herein, "identity sharing" means sharing the ability to authenticate the personal identity of the holder of a token. "Second factor sharing" means sharing the ability to authenticate an alias associated with a token. For example, a two-factor authentication system can include a Personal Identification Number ("PIN," the "first factor") and a One-Time Password ("OTP," the "second factor.") The PIN is a secret shared between the individual holder of the token and the authentication system. A particular OTP can be one in a sequence of numbers that can be uniquely generated only by a given token and be checked by the authentication system. When an authentication system receives and verifies a PIN from a user, the system can authenticate the user as being that user who is correlated with that particular PIN. Likewise, when an authentication system receives and verifies an OTP from a token, it can authenticate the token as being that token that is correlated with that

particular OTP. In an identity sharing system, any of several entities can authenticate the identity of the user based upon, for example, the PIN or the PIN and the OTP. In a second factor sharing system, the any of several entities can authenticate the token itself using the OTP. Although identity and second factor sharing has been discussed using a two-factor authentication device as an example, any authentication scheme can be used in accordance with the present invention. For example, digital certificates and/or challenge-response schemes can be used for second factor sharing.

Centralized Token Service Model

[0012] In accordance with an embodiment of the present invention, a centralized token service infrastructure is employed to provision and validate the second factor credential, such as a certificate or an OTP, e.g., stored on and/or implemented by a hardware token. The token implementing the second factor can be activated at any of a variety of applications and/or web-sites. An application can manage the first factor, such as a username and password, in the application's own user database. As part of token activation, the application can store a mapping between the local username and a shared second factor token identifier, such as a token serial number.

[0013] For validation, the user can enter a first factor, such as a username and password, and a second factor, such as a OTP from the token or a certificate stored on the token. The application can validate the first factor locally. Upon successful validation, it can retrieve the token serial number that can be associated with the first factor and then validate the second factor by sending a validation request to a centralized validation service, e.g., over a network such as the Internet, a Virtual Private Network, etc. To accomplish this, an enterprise hosting the application can deploy a validation proxy (the "Authentication Agent,") to the centralized validation service.

[0014] Figure 1 shows a centralized validation service in accordance with an embodiment of the present invention. Internet Service Provider ("ISP") 101 and bank 102 are coupled to Centralized Validation Service 103 through network 104. ISP 101 includes ISP application 105, ISP authentication agent 106 and ISP user store 107. ISP user store can be a database that correlates a first factor with the identity of a user (such as the identity of an ISP customer, administrator, employee, etc.) for one or more first factors and user identities. Bank 102 can include banking application 108, bank

authentication agent 109 and bank user store 110. Bank user store 110 can be a database that correlates a first factor with the identity of a user (such as a bank account holder, a bank officer, a bank IT administrator, a bank employee, etc.) End user 111 can activate a shared token, where the token is shared in this example between ISP 101 and bank 102. To authenticate himself to the ISP 101, end user 111 can enter his ISP username, which in this case is his e-mail address, e.g., joe@isp.com. End user 111 can also enter his associated password (e.g., "rolf362") and an OTP from his token. ISP validates the username and password provided by end user 111 by consulting ISP user store 107. An example of a record in user store 107 includes a username, a user password and a device identifier. For example, (joe@isp.com, "rolf362", 27582343). ISP 101 can send to Central Validation Service 103 a request that includes the OTP received from end user 111 and the token identifier retrieved from the user store. Centralized Validation Service 103 can include token validation application 112 and token store 113. Token store 113 can be a database that correlates token identifiers with precalculated OTPs and/or one or more secrets stored in the token associated with the token identifier and/or other information needed to verify a OTP from a token. Validation application 112 can compare the received OTP with one or more OTPs obtained from token store 113 and/or can calculate a OTP for comparison with the received OTP based upon data obtained from token store 113. Centralized Validation Service 103 can send a response message to ISP 101 indicating that the OTP has or has not been successfully validated. ISP 101 can provide Internet services to end user 111 if both the username/password and the OTP from end user 111 are successfully validated.

[0015] Similarly, end user 111 can provide a username (e.g., jsmith@bank.com) and a password to bank 102, which can validate these using bank user store 110. Bank 102 can send an OTP and token identifier received from end user 111 to Centralized Validation Service 103, which can validate these and send a response message to bank 102. If both the username and password and OTP are successfully validated, bank 102 can provide to end user 111 access to end user 111 account information and banking services.

[0016] In this example, end user 111 can initially obtain the token either from ISP 101, bank 102 or Centralized Validation Service 103. Each application can pay a centralized validation service and a token issuer for providing authentication services and products to the parties to a transaction.

Distributed Validation System

[0017] In accordance with another embodiment of the present invention, a distributed architecture is employed to validate the second factor. Figure 2 shows an embodiment of the distributed validation architecture. ISP 204 and bank 102 are coupled to Token Lookup Service 201 through a network 104, such as the Internet. ISP 204 can include token store 203, which can be a database that correlates token identifiers with precalculated OTPs and/or one or more secrets stored in the token associated with the token identifier and/or other information needed to verify a OTP from a token. This can be implemented at a one time password validation server 205 at ISP 204.

[0018] Token Lookup Service 201 can include Token Mapping Store 202. Token Mapping Store 202 can be a database that includes records that correlate token serial numbers with the network address (e.g., the IP address) of a validation server 205 that can validate the second factor credential from that token. Such a validation server is the Authoritative Validation Node (AVN) for that token serial number. Several AVNs can comprise a network of distributed validation servers. An example of a record stored at Token Mapping Store can be (IP-Address,Token_Identifier), e.g., (123.21.3.156, 1453422207). In this example, 123.21.3.156 can be the network address of the one time password validation server 205 and 1453422207 can be the identifier of the token whose one time password is to be validated by server 205.

[0019] In the example shown in Figure 1, ISP 101 can act as a token issuer by registering a list or range of token serial numbers with Token Lookup Service 201. The list or range of token serial numbers can be stored in token mapping store 202, which correlates the serial numbers to the IP address of ISP 101. Bank 102 acts as a relying party. When end user 111 requests access to information and services provided by bank 102 (the bank can be a "resource" sought to be accessed by a user of the token), end user 111 provides to bank 102 first and second authentication factors and the serial number for end user 111 token. Bank 102 can validate a first factor (such as username and password) using bank user store 110. This can be implemented using a resource validation server at Bank 102, e.g., a server on which the authentication agent 109 is implemented. It can store the mapping between Joe's username and token serial number in the local user store. It can also cache AVN information for the token locally. Caching may be implemented as it is implemented for DNS caching.

[0020] Bank 102 can also send a request to Token Lookup Service 201 that includes the token serial number provided by end user 111. Token mapping store 202 correlates the token serial number to the AVN IP address, which in this example is the IP address of ISP 101. Token lookup service 201 can return the IP address of the AVN (ISP 101) to bank 102. ISP 101 can include token store 203 and token validation application 205. Bank 102 can then send a validation request to ISP 101, which can validate the second factor using token validation application 205 and token store 203. ISP 101 can send the results of the validation to bank 102 in a response message.

[0021] In the example shown in Figure 2, end user 111 can authenticate to his ISP using his username (joe@isp.com), his associated password ("rolf362") and the OTP from his token. Since both the ISP and the bank have implement the distributed validation service, end user 111 can log into his online banking application at bank 102 utilizing his username (jsmith@bank.com), the associated password ("Rolf362") and the OTP from his ISP-issued token.

[0022] Token issuers, relying parties and Token Lookup Service 201 can authenticate themselves to each other as necessary. This can permit parties to introduce authorization and billing functionality for second factor validation, enabling a rich set of business models.

Credential Wallet

[0023] In accordance with another embodiment of the present invention, a credential wallet model leverages next generation mobile devices such as Java cell phones and PDAs that have storage and application capabilities and some form of graphic interface to manage credentials. In this embodiment, a mobile device can be a 'wallet' that can contain multiple instances of a second factor credential. For each site needing strong authentication, the appropriate credential or credentials can be accessed.

[0024] Each site or application can provision, manage and validate its own instance of the second factor credential, such as OTP tokens on the same physical device, thereby obviating the need for users to carry multiple tokens. For example, ISP 301 can include token validation application 303 and token store 203. Likewise, bank 302 can include token store 305 and validation application 304.

[0025] In the example shown in Figure 3, end user 111 mobile phone (not shown) can have different OTP credentials provisioned for different applications and/or sites. End user 111 can log into ISP 301 by using his ISP username (e.g.,

joe@isp.com), the associated password ("rolf362") and the appropriate OTP value for ISP 301. The second factor for ISP 301 can be validated using ISP validation application 303 and token store 203. End user 111 can obtain the appropriate OTP value for ISP 301 as shown in Figure 4. End user 111 can scroll a cursor 401 to the appropriate icon shown on the display screen 402 of cell phone 403. End user 111 can be asked to enter a PIN 404, which can be validated by cell phone 403. Upon successful validation of the PIN, the OTP value can be displayed 405 on screen 402.

[0026] End user 111 can logon to his online bank account using his username (jsmith@bank.com), associated password ("rolf32") and the OTP value from his bank's OTP token, as generated by his cell phone. The second factor for bank 302 can be validated using bank validation application 304 and token store 305.

[0027] In this credential wallet embodiment, each entity can deploy its own first and second factor authentication infrastructure. There is no dependency on an external authentication/validation party because the token itself is not shared. Rather, various tokens "share" a common token-generating device, such as a cell phone with the appropriate software.

[0028] Each of the embodiments discussed above can coexist and can be integrated to participate in the same authentication network. Each embodiment can be deployed independently as part of an evolutionary process towards a common end state, which can be a trusted, flexible, economical and easy to use authentication system for consumer applications.

[0029] Embodiments of the present invention can associate and authenticate users of various devices and/or credentials across multiple systems using a credential identifier. The credential identifier can be an identifier for the user (such as a name or an email address), or it may be an anonymous identifier (such as a number). The anonymous identifier can be an opaque identifier such as the result of a one-way transform of a set of user identifiers (such as hashing a username and/or a token identifier, credential reference, etc.)

[0030] Embodiments of the present invention can support an anonymizer service to generate an opaque identifier from a real identifier. Further, Different credential identifiers can be used for the same user by different relying parties for the same device. A credential can be transmitted in a way that preserves privacy, e.g. by using randomization (pure randomization, random encryption, etc.) or any suitable process to avoid tracking of a user.

[0031] The method in accordance with embodiments of the present invention can describe a service for discovering the correct validation node based on the token ID, i.e., a token lookup service. The token lookup service can maintain a list that maps token identifiers to token validation nodes. There may be more than one token identifier for each token. Authorized parties can query the token lookup service to determine the correct validation node for each service. The invention can operate works with multiple devices and multiple authentication algorithms. It can be implemented in software on desktop PCs, software on mobile devices, dedicated hardware or any other suitable platform.

[0032] The present invention can use one time password, challenge/response, and PKI (digital certificate) based credentials and authentication algorithms. Anonymous devices and credentials, and devices and credentials containing personal identifiers can be employed.

[0033] Embodiments of the invention include a centralized service that enables multiple relying parties to send validation requests for the same authentication device or credential.

[0034] Embodiments of the invention can be used for "token wallets." These wallets can contain multiple credentials for different services. Each credential in the wallet could be used by multiple services. A wallet may contain more than one shared credential, unshared credentials and multiple types of credentials, such as OTP credentials, digital certificates, challenge and response credentials, etc. It may contain more than one of each type of credential, or none of any type of credential.

[0035] Embodiments of the present invention can include centralized maintenance functions. If a credential is lost, broken, or stolen, then the token can be disabled across all applications in a single operation. If a credential is revoked or misused, an administrator can disable the credential across all or a designated subset of applications. This can be done in a single operation.

[0036] The foregoing is meant to illustrate and not limit the scope of the present invention. Other embodiments not explicitly described above are encompassed by the claims, as will be appreciated by those of skill in the art.

What is claimed is:

1. An authentication system, comprising:

a token constructed and arranged to have an identifier and to generate a one time password;

a one time password validation server constructed and arranged to validate the one time password generated by the token, the validation server having a network address;

a token lookup service constructed and arranged to correlate a token identifier with a network location of the validation server;

a resource validation server constructed and arranged to validate at least a first authentication factor provided by a user of the token, and to send a request for the location of the one time password validation server to the token lookup server if the first factor is successfully validated and to send a one time password validation request to the one time password validation server.

2. The system of claim 1, wherein the first authentication factor provided by the user of the token includes a username.

3. The system of claim 1, wherein the first authentication factor provided by the user of the token includes secret shared between the user of the token and the resource validation service.

4. A token lookup server, including:

a processor;

a memory coupled to the processor, the processor and memory constructed and arranged to store a network address of a one time password validation server and a token identifier, wherein the one time password validation server is constructed and arranged to validate a one time password generated by a token that corresponds to the token identifier.

5. The token lookup server of claim 4, wherein the processor and memory are further constructed and adapted to receive a request for a network address for a one time password validation server for a token, the request including a token identifier corresponding to the token, determine a network address that corresponds to the received token identifier and to send the determined network address in response to the request.

6. A method for authentication, including:

receiving at a token lookup service a request for a network address of a one time password validation server, the request including a token identifier;

determining a network address corresponding to a once time password validation server and the received token identifier; and

sending the network address in response to the request.