

SYSTEM AND METHOD TO AUTHORIZE THE ACCESS OF THE SERVICE TO AN END USER

Technical Field

[0001] The present disclosure relates to application layer security mechanism, and particularly, to a system and a method for authorizing the access of service based on the end user and the environmental context where the service is accessed.

Background

[0002] There exists several device management techniques. The techniques involve a complete solution is built in to the software stack of the underlying operating system of the device and the device is controlled through a central server. These techniques have a limitation that they are platform or operating system specific. Individual applications which act as agent is built for individual platform and the agent receive instructions from centralized server to control the device. This approach can handle multiple platforms. Both the above approaches works fine until enterprise own the device and employee only uses the device to access the enterprise information. But the recent trends are that employee brings in their own device and use the device to access the information. In this situation employee don't prefer the enterprise controlling or monitoring the device. Hence both the models proposed above in not suitable for addressing employee's privacy concern.

[0003] Accordingly, there is a need for a technique that enables, the enterprise focus on securing the application and provide the access to the service requested by the employees.

Summary of the invention

[0004] Aspects of the disclosure relates to describing method and system that authorize the access of the service to an end user based on the environment of access.

[0005] According to the one aspect of the present disclosure, a method for authorizing access to service for an end user comprises receiving an encrypted user request for access of the service through an encrypted communication channel by an enterprise application gateway server. The encryption of the user request can be performed by invoking a one-time password generator using a personal identification number of the end user. The metadata is accessed by the one-time password generator and a value is retrieved from the metadata to generate a dynamic key. The dynamic key generated can be converted to a symmetric encryption key or a symmetric decryption key, which can be used to encrypt the user request. The user credentials are gathered by the enterprise application management server and the user credentials can be exchanged between the enterprise application management server and the enterprise application gateway server. After receiving the encrypted user request, the enterprise application gateway server checks with the enterprise application management server to check if the end user has the credentials to access the requested service. If the end user is authorized, the end user is enabled to navigate the application enterprise server, wherein the application enterprise server comprises the requested service.

[0006] In the embodiment of the present disclosure, the end user can register from an electronic device.

Drawings

[0007] These and other features, aspects, and advantages of the present disclosure will be better understood when the following detailed description is read with reference to the accompanying drawings in which like characters represent like parts throughout the drawings, wherein:

[0008] Fig. 1 is a flow chart illustrating a method 100 for authorizing access to service for an end user, in accordance with an embodiment of the present disclosure;

[0009] Fig. 2 is a block diagram illustrating a system 200 for authorizing access to service for an end user, in accordance with an embodiment of the present disclosure; and

[0010] Fig. 3 is a system illustrating a generalized computer network arrangement, in accordance with an embodiment of the present disclosure.

Detailed Description

[0011] Fig. 1 is a flow chart illustrating a method 100 for authorizing access to service for an end user, in accordance with an embodiment of the present disclosure. Method 100 comprises a step 110 wherein receiving an encrypted user request for access of the service through an encrypted communication channel by an enterprise application gateway server. The end user may request the enterprise application gateway server to authorize access to a particular service. The end user request can be encrypted using the symmetric encryption key generated by the one-time password generator. The end user may provide a personal identification number (PIN) as an input while registering through an electronic device. The PIN may be an alpha numeric value, which may also include special characters. A one-time password generator is invoked using the PIN. It should be noted that only the correct PIN invokes the one time password generator. The one-time password generator may be any one-time password generator known in the art. On entering of the correct PIN by the user, the metadata is accessed and the value present in the

metadata is unlocked. The metadata may be a seed file that contains a value. a dynamic key is generated by referring to the value or the value along with the personal identification number stored in the metadata file. In accordance with an embodiment, a new dynamic key is generated for every session during a transaction. A new dynamic key can be generated for every request. Further, every dynamic key generated may be stored and referred to at a later point in time. The dynamic key is converted to a symmetric encryption key. Further, the symmetric encryption key may be in any of a 32-bit, a 64-bit, a 128-bit and a 256-bit or any other format. It should be noted that the symmetric encryption key by itself is not sent to the server; instead, the symmetric key is used to encrypt the user request and the encrypted user request is sent to the enterprise application gateway server. Furthermore, the encrypted messaging channel can be but not restricted to a https session.

[0012] Continuing with reference to Fig.1, the method 100 also comprises a step 120 which includes associating the encrypted user request with a corresponding end user by the enterprise application gateway server. The encrypted user request may be associated with the client id, service id, message Id, optional information which can be used to identify the key size and encryption algorithm used as part of the message header for the message created or which part of the message if the message is truncated. Prior to associating the encrypted message user credentials, the user identification credentials and the details related to the environment from which the service is being accessed is gathered by the enterprise application management gateway when the end user registers using the electronic device. The user identification credentials may comprises one or more of, but not restricted to, a user information, a device identifier, client identification, access details, application information, a user service access

detail, device information; and device configuration information. The device configuration information can be but not restricted to device or user or application. The configuration on the device can be but not restricted to Bluetooth on/off, location on/off, Wi-Fi on/off, application configuration like periodic scheduling, notifications etc. Application information may comprise of a client identification number which may be used to identify a client.

[0013] Furthermore, the access details may comprise one or more of, but not restricted to, a user service access details which can be based on the role of the user what the enterprise decides user can access. In another embodiment of the present disclosure, rules mapping client can be allowed to access or not access using client identification. Also, rules mapping user access based on the current context type of device, device hardware or device software information. The access details can also be based on the channel used for access such as, GPRS, 3G data, time, location, peripheral devices connected to the device or the network used in terms of 2G or 3G.

[0014] In another embodiment of the present disclosure, the eligibility to grant the access to the end user may be decided based on the environment and the user details. The final access level to the service can be one or more of null, partial or full.

[0015] The user information may comprise, but not restricted to unique identity to identify the user within the enterprise. The device information may be but not restricted to device identification and a unique identity to identify a device. For example, the unique can be an IMEI number of the mobile phone. The device information can be but not restricted to both hardware and software details. For example, CPU, RAM, OS installed, OS Version, applications installed,

and applications version. Furthermore, once the user identification credentials are received by the enterprise application management server, the user identification credentials may also store in the enterprise application management server.

[0016] Furthermore, the method 100 further comprises the step 130 wherein, the eligibility of the end user to access the requested service is determined. The enterprise application management server is enabled to communicate with the enterprise application gateway server. After receiving the encrypted user request message from the end user, the enterprise application gateway server communicates with the enterprise application management server to retrieve the user identification credentials, wherein the identification credentials can be but not restricted to key and the access permission. The access permission can be full, or partial or none. The enterprise application gateway server provides the message header to the enterprise application management server. The enterprise application management server based on the information available specifies whether access to the service can be granted or not.

[0017] At step 140 of the method 100, access to the requested service is granted to the end user after the enterprise application management server authorizes the end user based on the user identification credentials. The enterprise application gateway server decrypts the message and forwards the request to the enterprise application server based on the service Id for further processing. The enterprise application server processes the request and responds back with the reply message to enterprise application gateway server.

[0018] Fig. 2 is a block diagram illustrating a system 200 for authorizing access to service for an end user, in accordance with an embodiment of the present disclosure. The system comprises an

end user 210, an enterprise application gateway server 220, an enterprise application management server 230, and an enterprise application server 240.

[0019] The end user 210 may register using an electronic device and send an encrypted user request to the enterprise application gateway server 220. The encrypted user request can be encrypted using the key generated by the one-time password generator based on the PIN entered. The encrypted user request from the end user 210 can be associated with the client id, service id, message Id, optional information which can be used to identify the Key size and encryption algorithm used as part of the message header. For example, the service Id identifies which category the service falls under. For example, a sales person can access sales related information, field agent can access problem ticket related information. In another embodiment of the present disclosure the Service Id can be at the request level. For example, request for a video content.

[0020] The encrypted user request can be sent along with the header inside an https message to the enterprise application gateway server (EAGS) 220. The EAGS 220 retrieves the message along with the header from the https. The EAGS 220 provides the message header to the enterprise application management server 230 (EAMS). The EAMS 230 based on the information available specifies whether access to the service can be granted or not. If granted provides the symmetric decryption key to decrypt the encrypted user request.

[0021] In another embodiment of the present disclosure, a check can be made about the environmental conditions where the end user 210 has accessed the service. For example, an antivirus software could have been removed which make the access more vulnerable to the enterprise server. If the current process running indicates spyware etc, the access is vulnerable. Hence the access can be blocked in the above cases. Based on the environment access can be null

or partial or full. Another example of the embodiment would be, access can be allowed to view the content not download the data. Based on the location information access can be enabled or disabled.

[0022] The EAGS 220 decrypts the message and forwards the request to the enterprise application server (EAS) 240 based on the service Id for further processing. EAS 240 process the request and responds back with the reply message to EAGS 220. The EAGS 220 encrypts the message with the symmetric encryption key and appends the header with the header information received in the encrypted user request message and forwards the reply to the end user 210.

[0023] In another embodiment of the present disclosure, the EAGS 220 can modify the header before appending, to reflect the change in parameters such as but not restricted to encryption algorithm or key size.

[0024] One or more of the above-described techniques may be implemented in or involve one or more computer systems. Fig. 3 illustrates a generalized example of a computing environment 300. The computing environment 300 is not intended to suggest any limitation as to scope of use or functionality of described embodiments.

[0025] With reference to Fig. 3, the computing environment 300 includes at least one processing unit 310 and memory 320. In Figure 3, this most basic configuration 330 is included within a dashed line. The processing unit 310 executes computer-executable instructions and may be a real or a virtual processor. In a multi-processing system, multiple processing units execute computer-executable instructions to increase processing power. The memory 320 may be volatile memory (e.g., registers, cache, RAM), non-volatile memory (e.g., ROM, EEPROM,

flash memory, etc.), or some combination of the two. In some embodiments, the memory 320 stores software 380 implementing described techniques.

[0026] A computing environment may have additional features. For example, the computing environment 300 includes storage 340, one or more input devices 350, one or more output devices 360, and one or more communication connections 370. An interconnection mechanism (not shown) such as a bus, controller, or network interconnects the components of the computing environment 300. Typically, operating system software (not shown) provides an operating environment for other software executing in the computing environment 300, and coordinates activities of the components of the computing environment 300.

[0027] The storage 340 may be removable or non-removable, and includes magnetic disks, magnetic tapes or cassettes, CD-ROMs, CD-RWs, DVDs, or any other medium which may be used to store information and which may be accessed within the computing environment 300. In some embodiments, the storage 340 stores instructions for the software 380.

[0028] The input device(s) 350 may be a touch input device such as a keyboard, mouse, pen, trackball, touch screen, or game controller, a voice input device, a scanning device, a digital camera, or another device that provides input to the computing environment 300. The output device(s) 360 may be a display, a television, a hand held device, a head mounted display or a Kiosk that provides output from the computing environment 300.

[0029] The communication connection(s) 370 enable communication over a communication medium to another computing entity. The communication medium conveys information such as

computer-executable instructions, audio or video information, or other data in a modulated data signal. A modulated data signal is a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media include wired or wireless techniques implemented with an electrical, optical, RF, infrared, acoustic, or other carrier.

[0030] Implementations may be described in the general context of computer-readable media. Computer-readable media are any available media that may be accessed within a computing environment. By way of example, and not limitation, within the computing environment 300, computer-readable media include memory 320, storage 340, communication media, and combinations of any of the above.

[0031] The sequence of instructions as explained in the method steps may include a program code adapted for receiving an encrypted user request for access of the service through an encrypted communication channel by an enterprise application gateway server. The sequence of instructions may also include a program code adapted for associating the encrypted user request with a user identification credentials. Furthermore, the sequence of instructions may also include a program code adapted for associating the encrypted user request with a user identification credentials. The sequence of instructions may also comprise, program code adapted for determining eligibility of the user to access the service and program code adapted for authorizing the user use the service based on the eligibility.

[0032] The sequence of instruction may also comprise program code adapted for enabling the user to register on an electronic device. Furthermore, the sequence of instructions may comprise of program code adapted for gathering the user identification credentials, wherein the user

identification credentials comprises, a device identifier, a device information and a device configuration information.

[0033] The sequence of instructions may also include program code adapted for storing the user identification credentials on an enterprise application management server.

[0034] The sequence of instruction may also include, program code adapted for decrypting the encrypted user request by the enterprise application gateway server using the symmetric decryption key.

[0035] The sequence of instruction may comprise of program code adapted for enabling the user to navigate an enterprise application server, wherein the enterprise application service comprises the service.

[0036] Having described and illustrated the principles of our invention with reference to described embodiments, it will be recognized that the described embodiments may be modified in arrangement and detail without departing from such principles. It should be understood that the programs, processes, or methods described herein are not related or limited to any particular type of computing environment, unless indicated otherwise. Various types of general purpose or specialized computing environments may be used with or perform operations in accordance with the teachings described herein. Elements of the described embodiments shown in software may be implemented in hardware and vice versa.

[0037] In view of the many possible embodiments to which the principles of our invention may be applied, we claim as our invention all such embodiments as may come within the scope and spirit of the following claims and equivalents thereto.

What is claimed is

1. A method for authorizing access to a service for an end user, the method comprising:
 - receiving, by an enterprise application gateway server, an encrypted user request for access to the service through an encrypted communication channel;
 - transmitting, by the enterprise application gateway server, request information relating to the encrypted user request to an enterprise application management server;
 - associating, by the enterprise application management server, the encrypted user request with at least one user identification credential corresponding to the end user;
 - determining, by the enterprise application management server, whether the end user is permitted to access the requested service based at least in part on the at least one user identification credential and the environment of access;
 - transmitting, by the enterprise application management server, access information to the enterprise application gateway server indicating whether the end user is permitted to access the requested service;
 - decrypting, by the enterprise application gateway server, the access information transmitted by the enterprise application management server;
 - transmitting, by the enterprise application gateway server, the decrypted access information to an enterprise application server;
 - transmitting, by the enterprise application server, a reply message to the enterprise application gateway server;
 - encrypting, by the enterprise application gateway server, the reply message; and
 - transmitting, by the enterprise application gateway server, the encrypted reply message to the end user.
2. The method of claim 1, wherein encryption of the user request is performed by:
 - invoking a one-time password generator using a personal identification number of the end user;
 - accessing a metadata by the one-time password generator, wherein a value is retrieved from the metadata to generate a dynamic key; and

converting the dynamic key to a symmetric encryption key.

3. The method of claim 1, further comprising:
enabling the user to register from an electronic device.
4. The method of claim 3, further comprises:
gathering the user identification credentials and an environment of access, wherein the user identification credentials and the environment of access comprises:
 - a device identifier;
 - a user authentication;
 - a client identification;
 - a type of data channel;
 - a plurality of peripheral devices;
 - a device information; and
 - a device configuration information.
5. The method of claim 4, further comprises:
storing the user identification credentials on an enterprise application management server.
6. The method of claim 5, further comprises:
enabling the enterprise application management server to communicate with the enterprise application management gateway.
7. The method of claim 2, further comprises:
converting the dynamic key to a symmetric decryption key.
8. The method of claim 7 further comprising:
decrypting the encrypted user request by the enterprise application gateway server using the symmetric decryption key.
9. The method of claim 8 further comprises:

enabling the user to navigate an enterprise application server, wherein the enterprise application server comprises the service.

10. A system for authorizing access to service for an end user, the system comprising:

an enterprise application gateway server configured to (i) receive an encrypted user request for access to the service through an encrypted communication channel from the end user, and (ii) transmit request information relating to the encrypted user request;

an enterprise application management server communicably coupled to the enterprise application gateway server, the enterprise application management server configured to (i) associate the encrypted user request with at least one user identification credential corresponding to an end user, (ii) determine whether the end user is permitted to access the requested service based at least in part on the at least one user identification credential and the environment, and (iii) transmit access information to the enterprise application gateway server indicating whether the end user is permitted to access the requested service; and

an enterprise application server communicably coupled with the enterprise application gateway server, the enterprise application server configured to transmit a reply message to the enterprise application gateway server, wherein the enterprise application server comprises the services requested by the end user,

wherein the enterprise application gateway server further (iii) decrypts the access information transmitted by the enterprise application management server, (iv) transmits the decrypted access information to the enterprise application server, (v) encrypts the reply message, and (vi) transmits the encrypted reply message to the end user.

11. The system of claim 10, wherein the encrypted communication channel is a https session.

12. The system of claim 10, wherein the enterprise application gateway service is configured to receive the encrypted user request with a message header from the end user.

13. The system of claim 10, wherein the enterprise application management server is further configured to store and authenticate based on one or more of:

a device information;

- a client identification;
- a plurality of peripheral devices connected;
- a type of data channel;
- a user service access detail;
- a device identifier; and
- a device configuration information.

14. The system of claim 12, wherein the enterprise application gateway service is configured to send the message header to the enterprise application management server.

15. The system of claim 14, wherein the enterprise application management server is further configured to authorize permission to the end user based on the information present in the message header.

16. The system of claim 10, wherein the enterprise application gateway server further comprises a processor, wherein the processor is configured to perform the task of:

- invoking a one-time password generator using a personal identification number of the end user;

- accessing a metadata by the one-time password generator, wherein a value is retrieved from the metadata to generate a dynamic key; and

- converting the dynamic key to a symmetric decryption key.

17. The system of claim 10, wherein the reply message is a service reply message, and wherein the enterprise application server is further configured to respond back with the service reply message to the enterprise application gateway server.

18. The system of claim 17, wherein the enterprise application gateway server is configured to receive the service reply message and append the message header to the service reply message.

19. The system of claim 18, wherein the enterprise application gateway server is further configured to send the service reply message with the message header to the end user.

20. The system of claim 19, wherein the enterprise application gateway server is further configured to encrypt the service reply message and send the encrypted service reply message to the end user.

21. A computer program product, comprising a machine-accessible medium having instructions encoded thereon for enabling a processor to perform the operations of:

- program code adapted to cause an enterprise application gateway server to receive an encrypted user request for access to the service through an encrypted communication channel;

- program code adapted to cause the enterprise application gateway server to transmit request information relating to the encrypted user request to an enterprise management server;

- program code adapted to cause the enterprise application management server to associate the encrypted user request with at least one user identification credential corresponding to the end user;

- program code adapted to cause the enterprise application management server to determine whether the end user is permitted to access the requested service based at least in part on the at least one user identification credential and the environment of access;

- program code adapted to cause the enterprise application management server to transmit access information to the enterprise application gateway server indicating whether the end user is permitted to access the requested service;

- program code adapted to cause the enterprise application gateway server to decrypt the access information transmitted by the enterprise application management server;

- program code adapted to cause the enterprise application gateway server to transmit the decrypted access information to an enterprise application server;

- program code adapted to cause the enterprise application server to transmit a reply message to the enterprise application gateway server;

- program code adapted to cause the enterprise application gateway server to encrypt the reply message; and

program code adapted to cause the enterprise application gateway server to transmit the encrypted reply message to the end user.

22. The computer program product of claim 21, further comprising:
program code adapted for enabling the user to register on an electronic device.
23. The computer program product of claim 21, further comprising:
program code adapted for gathering the user identification credentials and an environment of access, wherein the user identification credentials and the environment access comprises:
 - a device identifier;
 - a user authentication;
 - a plurality of peripheral devices;
 - a client identification;
 - a type of data channel;
 - a device information; and
 - a device configuration information.
24. The computer program product of claim 23, further comprising:
program code adapted for storing the user identification credentials on an enterprise application management server.
25. The computer program product of claim 23, further comprising:
program code adapted for decrypting the encrypted user request by the enterprise application gateway server using the symmetric decryption key.
26. The computer program product of claim 23, further comprising:
program code adapted for enabling the user to navigate an enterprise application server, wherein the enterprise application service comprises the service.
27. The method of claim 1, wherein only partial access to the service can be authorized.

28. The system of claim 10, wherein only partial access to the service can be authorized.
29. The computer program product of claim 21, wherein only partial access to the service can be authorized.
30. The method of claim 1, wherein the encrypted user request is received with a header inside a HyperText Transmission Protocol, Secure (HTTPS) message.
31. The method of claim 30, wherein the header is transmitted to the enterprise application management server by the enterprise application gateway server.
32. The method of claim 31, wherein the enterprise application gateway server appends the header with header information received from the encrypted user request message when transmitting the encrypted reply message to the end user.