DELEGATED ADMINISTRATION OF PERMISSIONS USING A CONTACTLESS CARD

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/360,149, entitled "DELEGATED ADMINISTRATION OF PERMISSIONS USING A CONTACTLESS CARD" filed on March 21, 2019. The contents of the aforementioned application are incorporated herein by reference in their entirety.

TECHNICAL FIELD

[0002] Embodiments herein generally relate to computing platforms, and more specifically, to delegated administration of permissions using a contactless card.

BACKGROUND

[0003] Users often must have permissions to access computing resources and/or perform actions using computing resources. The complexity and difficulty in managing permissions in an organization increases as the number of users in the organization increase. Conventional solutions to managing permissions require substantial user effort and often lack robust security measures.

SUMMARY

[0004] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for delegated administration of permissions using a contactless card. In one example, a permissions module may receive a request from a first account to grant a second account access to a computing resource, the computing resource comprising one or more of: (i) an application, (ii) a data, and (iii) an operation performed using the application. The permissions module may receive, from a communications interface of a contactless card associated with the first account, permissions data associated with the first account and encrypted data generated by the contactless card, an applet of the contactless card to generate the encrypted data based at least in part on a private key for the contactless card stored in a memory of the contactless card. The permissions module may transmit the permissions data and the encrypted data to an authentication server. The authentication server may verify the encrypted data by decrypting the encrypted data based at least in part on a private key for the contactless card associated with the first account stored in a memory of the authentication server, and determine, based on the permissions data associated with the first account, that the first account has permissions to grant access to the computing resource to the second account. The permissions module may receive, from the authentication server, an indication of the verification of the encrypted data and a permissions vector associated with the second account, the permissions vector reflecting the grant of access to the computing resource to the second account.

[0004a] In accordance with an aspect of the present application, there is provided a method. The method comprises: receiving, by an application executing on a processor, a first request comprising a first account and a resource; receiving, by the application, a cryptogram from a contactless card; transmitting, by the application, the cryptogram to an authentication server; receiving, by the application from the authentication server, a result indicating that the authentication server decrypted the cryptogram; receiving, by the application, a permissions vector of the first account, the permissions vector comprising a plurality of entries; determining, by the application based on the permissions vector of the first account, that the first account is permitted access to the resource; and granting, by the application, the first account access to the resource based on the result indicating that the authentication server decrypted the cryptogram and the permissions vector of the first account.

[0004b] In accordance with another aspect of the present application, there is provided a computer-readable storage medium including instructions that when executed by a processor, cause the processor to: receive, by an application, a first request comprising a first account and a resource; receive, by the application, a cryptogram from a contactless card; transmit, by the application, the cryptogram to an authentication server; receive, by the application from the authentication server, a result indicating that the authentication server decrypted the cryptogram; receive, by the application, a permissions vector of the first account, the permissions vector comprising a plurality of entries; determine, by the application based on the permissions vector of the first account, that the first account is permitted access to the resource; and grant, by the application, the first account access to the resource based on the result indicating that the authentication server decrypted the cryptogram and the permissions vector of the first account.

[0004c] In accordance with yet another aspect of the present application, there is provided a computing apparatus comprising: a processor; and a memory storing instructions that, when executed by the processor, cause the processor to: receive, by an application, a first request comprising a first account and a resource; receive, by the application, a cryptogram from a contactless card; transmit, by the application, the cryptogram to an authentication server; receive, by the application from the authentication server, a result indicating that the authentication server decrypted the cryptogram; receive, by the application, a permissions vector of the first account, the permissions vector comprising a plurality of entries; determine, by the application based on the permissions vector of the first account, that the first account is permitted access to the resource; and grant, by the application, the first account access to

the resource based on the result indicating that the authentication server decrypted the cryptogram and the permissions vector of the first account.

Claims

1. A method, comprising:

receiving, by an application executing on a processor, a first request comprising a first account and a resource;

receiving, by the application, a cryptogram from a contactless card;

transmitting, by the application, the cryptogram to an authentication server;

receiving, by the application from the authentication server, a result indicating that the authentication server decrypted the cryptogram;

receiving, by the application, a permissions vector of the first account, the permissions vector comprising a plurality of entries;

determining, by the application based on the permissions vector of the first account, that the first account is permitted access to the resource; and

granting, by the application, the first account access to the resource based on the result indicating that the authentication server decrypted the cryptogram and the permissions vector of the first account.

2. The method of claim 1, wherein the resource comprises a second application, the method further comprising:

disabling, by the application, a first feature of the second application based on a first entry of the plurality of entries of the permissions vector for the first account.

3. The method of claim 2, further comprising:

enabling, by the application, a second feature of the second application based on a second entry of the plurality of entries of the permissions vector for the first account.

4. The method of claim 1, further comprising prior to receiving the first request:

receiving, by the application, a second request comprising the first account, a second account, and the resource;

receiving, by the application, a second cryptogram from a second contactless card associated with the second account;

receiving, by the application, a permissions vector for the second account from the second contactless card;

transmitting, by the application, the permissions vector and the second cryptogram to the authentication server; and

receiving, by the application from the authentication server, a result indicating that the authentication server decrypted the second cryptogram;

receiving, by the application from the authentication server, the permissions vector of the first account; and

determining, by the application based on the permissions vector of the first account, that the first account was granted access to the resource responsive to the second request.

5. The method of claim 1, further comprising:

receiving, by the application, a second request comprising the first account and a second resource;

determining, by the application based on the permissions vector for the first account, that the first account does not have access to the second resource; and

rejecting, by the application, the second request based on the determination that the first account does not have access to the second resource.

6. The method of claim 1, further comprising:

receiving, by the application, a second request comprising the first account and a second resource;

receiving, by the application from the contactless card, a second cryptogram;

transmitting, by the application, the second cryptogram to the authentication server;

receiving, by the application from the authentication server, a second result indicating that the authentication server did not decrypt the second cryptogram; and

rejecting, by the application, the second request based on the second result.

7. The method of claim 1, wherein the application is the resource, wherein the application comprises a plurality of features, wherein the permissions vector comprises a respective entry for each feature of the plurality of features of the application, wherein the permissions vector is received from one of the contactless card or the authentication server.

8. A computer-readable storage medium including instructions that when executed by a processor, cause the processor to:

receive, by an application, a first request comprising a first account and a resource;

receive, by the application, a cryptogram from a contactless card;

transmit, by the application, the cryptogram to an authentication server;

receive, by the application from the authentication server, a result indicating that the authentication server decrypted the cryptogram;

receive, by the application, a permissions vector of the first account, the permissions vector comprising a plurality of entries;

determine, by the application based on the permissions vector of the first account, that the first account is permitted access to the resource; and

grant, by the application, the first account access to the resource based on the result indicating that the authentication server decrypted the cryptogram and the permissions vector of the first account.

9. The computer-readable storage medium of claim 8, wherein the resource comprises a second application, wherein the instructions further cause the processor to:

disable, by the application, a first feature of the second application based on a first entry of the plurality of entries of the permissions vector for the first account.

10. The computer-readable storage medium of claim 9, wherein the instructions further cause the processor to:

enable, by the application, a second feature of the second application based on a second entry of the plurality of entries of the permissions vector for the first account.

11. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to, prior to receiving the first request:

receive, by the application, a second request comprising the first account, a second account, and the resource;

receive, by the application, a second cryptogram from a second contactless card associated with the second account;

receive, by the application, a permissions vector for the second account from the second contactless card;

transmit, by the application, the permissions vector and the second cryptogram to the authentication server; and

receive, by the application from the authentication server, a result indicating that the authentication server decrypted the second cryptogram;

receive, by the application from the authentication server, the permissions vector of the first account; and

determine, by the application based on the permissions vector of the first account, that the first account was granted access to the resource responsive to the second request.

12. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

receive, by the application, a second request comprising the first account and a second resource;

determine, by the application based on the permissions vector for the first account, that the first account does not have access to the second resource; and

reject, by the application, the second request based on the determination that the first account does not have access to the second resource.

13. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

receive, by the application, a second request comprising the first account and a second resource;

receive, by the application from the contactless card, a second cryptogram;

transmit, by the application, the second cryptogram to the authentication server;

receive, by the application from the authentication server, a second result indicating that the authentication server did not decrypt the second cryptogram; and

reject, by the application, the second request based on the second result.

14. The computer-readable storage medium of claim 8, wherein the application is the resource, wherein the application comprises a plurality of features, wherein the permissions vector comprises a respective entry for each feature of the plurality of features of the application, wherein the permissions vector is received from one of the contactless card or the authentication server.

15. A computing apparatus comprising:

a processor; and

a memory storing instructions that, when executed by the processor, cause the processor to:

receive, by an application, a first request comprising a first account and a resource;

receive, by the application, a cryptogram from a contactless card;

transmit, by the application, the cryptogram to an authentication server;

receive, by the application from the authentication server, a result indicating that the authentication server decrypted the cryptogram;

receive, by the application, a permissions vector of the first account, the permissions vector comprising a plurality of entries;

determine, by the application based on the permissions vector of the first account, that the first account is permitted access to the resource; and

grant, by the application, the first account access to the resource based on the result indicating that the authentication server decrypted the cryptogram and the permissions vector of the first account.

16. The computing apparatus of claim 15, wherein the resource comprises a second application, wherein the instructions further cause the processor to:

disable, by the application, a first feature of the second application based on a first entry of the plurality of entries of the permissions vector for the first account.

17. The computing apparatus of claim 16, wherein the instructions further cause the processor to:

enable, by the application, a second feature of the second application based on a second entry of the plurality of entries of the permissions vector for the first account.

18. The computing apparatus of claim 15, wherein the instructions further cause the processor to, prior to receiving the first request:

receive, by the application, a second request comprising the first account, a second account, and the resource;

receive, by the application, a second cryptogram from a second contactless card associated with the second account;

receive, by the application, a permissions vector for the second account from the second contactless card;

transmit, by the application, the permissions vector and the second cryptogram to the authentication server; and

receive, by the application from the authentication server, a result indicating that the authentication server decrypted the second cryptogram;

receive, by the application from the authentication server, the permissions vector of the first account; and

determine, by the application based on the permissions vector of the first account, that the first account was granted access to the resource responsive to the second request.

19. The computing apparatus of claim 15, wherein the instructions further cause the processor to:

receive, by the application, a second request comprising the first account and a second resource;

determine, by the application based on the permissions vector for the first account, that the first account does not have access to the second resource; and

reject, by the application, the second request based on the determination that the first account does not have access to the second resource.

20. The computing apparatus of claim 15, wherein the instructions further configure the apparatus to:

receive, by the application, a second request comprising the first account and a second resource;

receive, by the application from the contactless card, a second cryptogram;

transmit, by the application, the second cryptogram to the authentication server;

receive, by the application from the authentication server, a second result indicating that the authentication server did not decrypt the second cryptogram; and

reject, by the application, the second request based on the second result.