Title: METHODS, SYSTEMS, AND MEDIA FOR AUTHENTICATION OF USER DEVICES TO A DISPLAY DEVICE

Abstract: Methods, systems, and media for authentication of user devices to a display device are provided. In some implementations, the method comprises: authenticating a first user device to a display device, wherein an authentication token is associated with the authentication of the first user device to the display device, wherein the authentication token is stored on a server in association with an identifier of the first user device, and wherein the first user device is provided with media playback control on the display device in response to the authentication; identifying, using the first user device, a second user device in proximity to the first user device; transmitting, from the first user device to the second user device, an invitation message to authenticate the second user device to the display device; and, in response to receiving a response to the invitation message from the second user device, transmitting, from the first user device to the second user device, the authentication token that causes the second user device to request authentication to the display device from the server, wherein the second user device is provided with media playback control on the display device in response to authenticating with the display device.
METHODS, SYSTEMS, AND MEDIA FOR AUTHENTICATION OF USER DEVICES TO A DISPLAY DEVICE

Technical Field

[0001] The disclosed subject matter relates to methods, systems, and media for authentication of second screen user devices to a display device.

Background

[0002] Many people enjoy using a second screen device, such as a mobile phone or tablet computer, to select media content items to be presented on a primary device, such as a television, audio speakers, or a projector. Additionally, people may want to have multiple second screen devices be allowed to communicate with the primary device, for example, the multiple devices within a household. However, it can be time-consuming to authenticate each of the multiple devices to the primary device. For example, each second screen device may be individually authenticated with the primary device, such as a display device, with user account information, password information, device information, display device code information (e.g., a code of a display device that may itself be difficult to locate), etc. and only once such information is inputted can a user of a second screen device communicate with the primary device.

[0003] Accordingly, it is desirable to provide new methods, systems, and media for authentication of user devices to a display device.

Summary

[0004] Methods, systems, and media for authentication of user devices to a display device are provided.

[0005] In accordance with some implementations of the disclosed subject matter, a method for authentication of user devices is provided, the method comprising: authenticating a first user device to a display device, wherein an authentication token is associated with the authentication of the first user device to the display device, wherein the authentication token is stored on a server in association with an identifier of the first user device, and wherein the first user device is provided with media playback control on the display device in response to the authentication; identifying, using the first user device, a second user device in proximity to the first user device; transmitting, from the first user device to the second user device, an invitation
message to authenticate the second user device to the display device; and in response to
receiving a response to the invitation message from the second user device, transmitting, from
the first user device to the second user device, the authentication token that causes the second
user device to request authentication to the display device from the server, wherein the second
user device is provided with media playback control on the display device in response to
authenticating with the display device.
[0006] In some implementations, the method further comprises: generating, using the
first user device, the authentication token; and transmitting the authentication token to the server.
[0007] In some implementations, the method further comprises receiving, from a contact
list associated with a first user of the first user device, an indication of a second user of the
second user device, wherein the second user device is identified based on the received indication.
[0008] In some implementations, identifying the second user device further comprises
detecting the second user device based on a connection to a network.
[0009] In some implementations, identifying the second user device further comprises:
detecting a movement of the first user device; transmitting, to the server, an indication of the
movement and a first location associated with the first user device; and receiving, from the
server, an identifier associated with the second user device, wherein the second user device
detected a movement of the second user device at a second location and wherein the first location
and the second location are within a predetermined distance.
[0010] In some implementations, the method further comprises: receiving, from a user of
the first user device, an indication that the second user device is not to be authenticated to the
display device; and transmitting, to the server, a request to remove authentication permission for
the second user device to the display device.
[0011] In accordance with some implementations of the disclosed subject matter, a
system for authentication of user devices is provided, the system comprising a hardware
processor on a first user device that is configured to: authenticate the first user device to a
display device, wherein an authentication token is associated with the authentication of the first
user device to the display device, wherein the authentication token is stored on a server in
association with an identifier of the first user device, and wherein the first user device is
provided with media playback control on the display device in response to the authentication;
identify, using the first user device, a second user device in proximity to the first user device;
transmit, from the first user device to the second user device, an invitation message to authenticate the second user device to the display device; and in response to receiving a response to the invitation message from the second user device, transmit, from the first user device to the second user device, the authentication token that causes the second user device to request authentication to the display device from the server, wherein the second user device is provided with media playback control on the display device in response to authenticating with the display device.

[0012] In accordance with some implementations of the disclosed subject matter, a non-transitory computer-readable medium containing computer-executable instructions that, when executed by a processor, cause the processor to perform a method for authentication of user devices is provided, the method comprising: authenticating a first user device to a display device, wherein an authentication token is associated with the authentication of the first user device to the display device, wherein the authentication token is stored on a server in association with an identifier of the first user device, and wherein the first user device is provided with media playback control on the display device in response to the authentication; identifying, using the first user device, a second user device in proximity to the first user device; transmitting, from the first user device to the second user device, an invitation message to authenticate the second user device to the display device; and in response to receiving a response to the invitation message from the second user device, transmitting, from the first user device to the second user device, the authentication token that causes the second user device to request authentication to the display device from the server, wherein the second user device is provided with media playback control on the display device in response to authenticating with the display device.

[0013] In accordance with some implementations of the disclosed subject matter, a system for authentication of user devices is provided, the system comprising: means for authenticating a first user device to a display device, wherein an authentication token is associated with the authentication of the first user device to the display device, wherein the authentication token is stored on a server in association with an identifier of the first user device, and wherein the first user device is provided with media playback control on the display device in response to the authentication; means for identifying, using the first user device, a second user device in proximity to the first user device; means for transmitting, from the first user device to the second user device, an invitation message to authenticate the second user device to the
display device; and means for transmitting, from the first user device to the second user device, the authentication token that causes the second user device to request authentication to the display device from the server in response to receiving a response to the invitation message from the second user device, wherein the second user device is provided with media playback control on the display device in response to authenticating with the display device.

[0014] In some implementations, the system further comprises: means for generating using the first user device, the authentication token; and means for transmitting the authentication token to the server.

[0015] In some implementations, the system further comprises: means for transmitting, to the server, a request for the authentication token; and means for receiving the authentication token from the server.

[0016] In some implementations, the system further comprises means for receiving, from a contact list associated with a first user of the first user device, an indication of a second user of the second user device, wherein the second user device is identified based on the received indication.

[0017] In some implementations, the system further comprises means for detecting the second user device based on a connection to a network.

[0018] In some implementations, the system further comprises: means for detecting a movement of the first user device; means for transmitting, to the server, an indication of the movement and a first location associated with the first user device; and means for receiving, from the server, an identifier associated with the second user device, wherein the second user device detected a movement of the second user device at a second location and wherein the first location and the second location are within a predetermined distance.

[0019] In some implementations, the system further comprises: means for receiving, from a user of the first user device, an indication that the second user device is not to be authenticated to the display device; and means for transmitting, to the server, a request to remove authentication permission for the second user device to the display device.

Brief Description of the Drawings

[0020] Various objects, features, and advantages of the disclosed subject matter can be more fully appreciated with reference to the following detailed description of the disclosed
subject matter when considered in connection with the following drawings, in which like reference numerals identify like elements.

[0021] FIG. 1 shows a schematic diagram of an example of a system for authenticating user devices to pair with a display device in accordance with some implementations of the disclosed subject matter.

[0022] FIG. 2 shows an example of hardware that can be used in a server and/or a user device in accordance with some implementations of the disclosed subject matter.

[0023] FIG. 3 shows an example of an information flow diagram for authenticating a user device to pair with a display device in accordance with some implementations of the disclosed subject matter.

[0024] FIG. 4 shows an example of a process for storing indications of user devices allowed to pair with a display device in accordance with some implementations of the disclosed subject matter.

[0025] FIG. 5 shows an example of a process for detecting nearby user devices to pair with a display device in accordance with some implementations of the disclosed subject matter.

**Detailed Description**

[0026] In accordance with various implementations, mechanisms (which can include methods, systems, and media) for authentication of user devices to a display device are provided.

[0027] In accordance with some implementations, the mechanisms presented herein can authenticate a second user device for communication with a display device using a token previously used to authenticate a first user device to the display device. In some implementations, the mechanisms can cause a server to store an access control list (ACL) that indicates all user devices authenticated to communicate with a particular display device in association with the token, which can indicate an identity of the display device. In some such implementations, the server can receive requests to present particular media content items on the display device and can determine whether the user device that transmitted the request is included in the ACL associated with the display device based on the token. The server can then cause the requested media content item to be presented on the display device if it is determined that the user device is included in the ACL. The mechanisms described herein can thereby allow a first user device to transfer an authentication token to a second user device to authenticate the second
user device to the display device, and can allow the second user device to request particular
content items to be presented on the display device through the server. Upon authenticating the
second user device to the display device with the transferred authentication token, the second
user device can then, for example, receive media playback control of the display device.

In some implementations, the first user device can be authenticated to
communicate with the display device in any suitable manner, such as by receiving, from a user of
the first user device, a password and/or code associated with the display device. In some
implementations, the pairing between the first user device and the display device can be
associated with a particular token (e.g., a randomly generated alphanumeric string generated by a
server and/or the first user device), which can be stored on a server. In some implementations,
the first user device can detect other user devices near the first user device, and can then transmit
the token representing the display device that the first user device is already paired with to a
detected nearby second user device. In some implementations, the second user device can then
transmit a request to be authenticated to the display device to the server, and can include the
token in the request. In response to receiving the request from the second user device that
includes the token corresponding to the display device, the server can add an identifier
corresponding to the second user device to the ACL corresponding to the display device, thereby
allowing the second user device to be authenticated to the display device without requiring a
password and/or code to be explicitly input by a user of the second user device.

Note that, in some implementations, the first user device can detect nearby user
devices using any suitable technique or combination of techniques. For example, in some
implementations, the first user device can detect other user devices connected to a particular
network, can use audible and/or subaudible tones (e.g., ultrasonic, and/or any other suitable type
of subaudible tones) to detect other user devices, can transmit a multicast message on a network
(e.g., a WiFi network, a BLUETOOTH network, and/or any other suitable type of network) and
can detect user devices that respond to the message, and/or detect nearby user devices in any
suitable manner. Additionally, in some implementations, a second user device can be explicitly
indicated by a user of the first user device based on a selection of an identifier associated with
the second user device (e.g., via a list of contacts, a list of other devices detected on a particular
network, and/or in any other suitable manner).
In some implementations, the first user device, the second user device, and the
display device can be any suitable type(s) of devices. For example, in some implementations,
the first user device and/or the second user device can be user devices with no screen and/or
relatively small screens, such as tablet computers, laptop computers, wearable computers, a
personal assistant device, and/or any other suitable type of device. As another example, in some
implementations, the display device can be any suitable type of device suitable for presenting
media content (e.g., video content, audio content, websites, pictures, live-streamed programs,
radio programs, television programs, audiobooks, and/or any other suitable type of content). As
a more particular example, in some implementations, the display device can include a television,
a projector, audio speakers (and/or a personal assistant device that includes audio speakers), a
tablet computer, a desktop computer, a laptop computer, and/or any other suitable type of display
device.

Turning to FIG. 1, an example 100 of hardware for authenticating a user device to
a display device that can be used in accordance with some implementations of the disclosed
subject matter is shown. As illustrated, hardware 100 can include one or more servers, such as
server 102, a communication network 104, and one or more user devices 106.

Server 102 can be any suitable server for facilitating authentication of a user
device to a display device. For example, in some implementations, server 102 can store an
indication of a first user device authenticated to communicate with a display device. In some
implementations, server 102 can then grant permission to a second user device to communicate
with the display device in response to receiving a token from the second user device that
corresponds to the display device currently authenticated to communicate with the first user
device. Additionally, in some implementations, server 102 can store an ACL indicating user
devices that are authenticated to communicate with the display device. In some such
implementations, server 102 can receive, from a user device included in the ACL, a request to
present a media content item on the display device and can cause the media content item to be
presented on the display device. For example, in some implementations, server 102 can cause
the media content item to be streamed to the display device for playback on the display device.

Communication network 104 can be any suitable combination of one or more
wired and/or wireless networks in some implementations. For example, communication
network 104 can include any one or more of the Internet, a mobile data network, a satellite
network, a local area network, a wide area network, a telephone network, a cable television
network, a WiFi network, a WiMax network, a BLUETOOTH network, and/or any other suitable
communication network.

[0034] User device(s) 106 can include any one or more user devices (e.g., user device
108 and/or user device 110) suitable for requesting media content, and/or performing any other
suitable functions. For example, in some implementations, user device(s) 106 can include
mobile devices, such as a mobile phone, a tablet computer, a laptop computer, a vehicle (e.g., a
car, a boat, an airplane, or any other suitable vehicle) entertainment system, a portable media
player, a wearable computer, or any other suitable mobile device. As another example, in some
implementations, user device(s) 106 can include non-mobile devices such as a desktop computer,
a set-top box, a television, a streaming media player, a game console, audio speakers, a projector,
or any other suitable non-mobile device. User devices 106 can be connected by one or more
communications links 112 to communication network 104 that can be linked via a
communication link 114 to server 102.

[0035] Although only one server is shown in FIG. 1 to avoid over-complicating the
figure, any suitable one or more servers can be used in some implementations. Also, any
suitable number of user devices 106, and any suitable types of these devices, can be used in some
implementations.

[0036] Server 102 and user device(s) 106 can be implemented using any suitable
hardware in some implementations. For example, in some implementations, devices 102 and
106 can be implemented using any suitable general purpose computer or special purpose
computer. For example, a server may be implemented using a special purpose computer. Any
such general purpose computer or special purpose computer can include any suitable hardware.
For example, as illustrated in example hardware 200 of FIG. 2, such hardware can include
hardware processor 202, memory and/or storage 204, an input device controller 206, an input
device 208, display/audio drivers 210, display and audio output circuitry 212, communication
interface(s) 214, an antenna 216, and a bus 218.

[0037] Hardware processor 202 can include any suitable hardware processor, such as a
microprocessor, a micro-controller, digital signal processor(s), dedicated logic, and/or any other
suitable circuitry for controlling the functioning of a general purpose computer or a special
purpose computer in some implementations.
[0038] Memory and/or storage 204 can be any suitable memory and/or storage for storing programs, data, media content, and/or any other suitable information in some implementations. For example, memory and/or storage 204 can include random access memory, read-only memory, flash memory, hard disk storage, optical media, and/or any other suitable memory.

[0039] Input device controller 206 can be any suitable circuitry for controlling and receiving input from one or more input devices 208 in some implementations. For example, input device controller 206 can be circuitry for receiving input from a touch screen, from one or more buttons, from a voice recognition circuit, from a microphone, from a camera, from an optical sensor, from an accelerometer, from a temperature sensor, from a near field sensor, and/or any other type of input device.

[0040] Display/audio drivers 210 can be any suitable circuitry for controlling and driving output to one or more display/audio output circuitries 212 in some implementations. For example, display/audio drivers 210 can be circuitry for driving an LCD display, a speaker, an LED, or any other type of output device.

[0041] Communication interface(s) 214 can be any suitable circuitry for interfacing with one or more communication networks, such as network 104 as shown in FIG. 1. For example, interface(s) 214 can include network interface card circuitry, wireless communication circuitry, and/or any other suitable type of communication network circuitry.

[0042] Antenna 216 can be any suitable one or more antennas for wirelessly communicating with a communication network in some implementations. In some implementations, antenna 216 can be omitted when not needed.

[0043] Bus 218 can be any suitable mechanism for communicating between two or more components 202, 204, 206, 210, and 214 in some implementations.

[0044] Any other suitable components can be included in hardware 200 in accordance with some implementations.

[0045] Turning to FIG. 3, an information flow diagram 300 is shown in accordance with some implementations. As illustrated, in some implementations, information flow diagram 300 can be implemented on server 102, (first) user device 108, and (second) user device 110.

[0046] At 302, user device 108 can authenticate itself to a display device. User device 108 can be authenticated to communicate with the display device using any suitable technique or combination of techniques. For example, in some implementations, the display device can be
associated with a password and/or numeric code, and user device 108 can be authenticated to
communicate with the display device by a user of user device 108 entering the password and/or
numeric code (e.g., in a particular browser window, within a particular application executing on
user device 108, and/or in any other suitable manner). Note that, in some implementations,
authentication of a user device to the display device can be based on a user account that is logged
in on the user device. In some such implementations, any user device that has logged in to the
user account can be authenticated to communicate with the display device. In some
implementations, the user account can be associated with any suitable service, such as a video
sharing service, a social networking service, a particular application executing on the user
device, and/or any other suitable service.

At 304, server 102 can store a token associated with user device 108 and the
display device. In some implementations, the token can be in any suitable format. For example,
in some implementations, the token can be a randomly generated string of alphanumeric
characters. In some implementations, the token can be generated by server 102 and/or user
device 108. In instances where the token is generated by user device 108, the token can be
transmitted to server 102, for example, in connection with block 302. Additionally or
alternatively, in instances where the token is generated by server 102, the token can be
transmitted to user device 108 to allow user device 108 to store information regarding the
authentication to the display device, for example, in connection with block 304. In some
implementations where the token is generated by server 102, user device 108 can request the
token from server 102, and server 102 can generate the token in response to the request and
transmit the token to user device 108. In some implementations, the token can indicate an
identity of the display device. For example, in some implementations, the token can be
generated to be a weak hash of an identifier of the display device, and/or any other suitable
representation of the identity of the display device.

Server 102 can store the token in any suitable manner. For example, in some
implementations, the token can be stored as a key in a key-value pair in association with an
identifier of user device 108. As a more particular example, in some implementations, the token
can be stored in association with information indicating the geographic location of user device
108 (e.g., based on Global Positioning Coordinates, and/or based on any other suitable
information), an indication of an Internet Protocol (IP) address associated with user device 108,
and/or any other suitable information. Note that, in some implementations, server 102 can use the stored token to maintain an ACL that indicates user devices allowed to communicate with the display device, where the stored token corresponds to and/or indicates the display device. For example, in some implementations, server 102 can add user devices to the ACL in response to receiving requests from user devices that include the stored token.

[0049] At 306, user device 108 can detect and invite user device 110 to be authenticated to communicate with the display device. For example, in some implementations, user device 108 can automatically detect user device 110, for example, based on a detection of user devices that are determined to be within a predetermined proximity of user device 108, as described in more detail in connection with FIG. 5. As another example, in some implementations, a user of user device 108 can select a contact (e.g., from a contacts list, and/or from any other source) corresponding to a user of user device 110. In some implementations, after detecting user device 110 and/or receiving an indication of user device 110 from a user of user device 108, user device 108 can transmit a notification and/or an invitation message to user device 110 to be paired with the display device. For example, in some implementations, the invitation message can indicate a name of and/or an identifier of the display device (e.g., "Living Room Television," and/or any other suitable name or identifier).

[0050] At 308, user device 108 can transmit the token to user device 110. In some implementations, the token can be transmitted in connection with the invitation message transmitted at block 306. Additionally or alternatively, in some implementations, the token can be transmitted in response to receiving, from user device 110, an indication that the invitation to be authenticated to the display device has been accepted by a user of user device 110. Note that, in some implementations, user device 108 can transmit information indicating an identity of user device 110 to server 102. In some such implementations, server 102 can then authenticate user device 110 to the display device. Note that, in instances where the token is generated by server 202, user device 108 can receive the token from server 202 (e.g., from a transmission from server 202 at block 304, and/or at any other suitable time), and can then transmit the token to user device 110.

[0051] At 310, user device 110 can request permission to be authenticated to communicate with the display device from server 102. For example, in some implementations, user device 110 can transmit a request to be authenticated to server 102 that includes the token.
As a more particular example, in some implementations, user device 110 can transmit a Remote Procedure Call (RPC) to server 102 and can include the token as a parameter in the RPC.

[0052] At 312, server 102 can grant permission to user device 110 to communicate with the display device. For example, in some implementations, in response to receiving the token corresponding to the display device, server 102 can add user device 110 to the ACL corresponding to the display device. In some implementations, server 102 can transmit any suitable message to user device 110 indicating that permission has been granted. In some implementations, server 102 now receive requests from user device 110 to present content on the display device in response to receiving requests from user device 110. In some such implementations, user device 110 can request particular media content items to be presented on the display device through server 102, and no connection between user device 110 and the display device is required.

[0053] In some implementations, in response to receiving the token corresponding to the display device from user device 110 (which was received from user device 108), server 102 can grant rights and/or permissions to user device 110 that match the rights and/or permissions that user device 108 has in communicating with the display device. For example, server 102 can determine that user device 108 has permission to stream and/or cast media content items to the display device and, in response, grant permission to user device 110 to also stream and/or cast media content items to the display device. In another example, server 102 can determine that user device 108 has streaming rights to stream media content items to the display device but does not have administrator rights to modify settings of the display device and, in response, grant permission to user device 110 to also stream media content items while inhibiting user device 110 from receiving administrator rights to modify settings of the display device.

[0054] Note that, in some implementations, server 102 can include user device 110 in the ACL corresponding to the display device for any suitable duration of time. For example, in some implementations, server 102 can include user device 110 in the ACL until a specific instruction to remove user device 110 is received (e.g., from user device 108, and/or from any other suitable user device). As another example, in some implementations, server 102 can include user device 110 in the ACL while a particular browser window and/or a particular application is open on user device 110. As yet another example, in some implementations, server 102 can include user device 110 in the ACL while user device 110 is within a particular proximity of user
device 108 and/or the display device. As a more particular example, in some implementations, server 102 can remove user device 110 from the ACL in response to determining that user device 110 has been moved beyond a predetermined distance from the display device (e.g., more than ten feet, more than a hundred feet, more than a mile, and/or any other suitable distance). In some implementations, proximity can be based on any suitable information, such as GPS coordinates, connection to a particular network (e.g., a WiFi network within a home, a BLUETOOTH network, and/or any other suitable type of network), ability of user device 110 to detect subaudible tones, and/or any other suitable information.

Additionally, note that, in some implementations, server 102 can maintain two ACLs. For example, in some implementations, a first ACL can indicate user devices that have been authenticated to the display device. As a more particular example, as shown in information flow diagram 300, the first ACL can include user device 108 and user device 110. As another example, in some implementations, a second ACL can indicate one or more user devices that have administrative permissions to transfer an authentication token to a detected and/or invited user device. As a more particular example, as shown in information flow diagram 300, the second ACL can include user device 108.

Turning to FIG. 4, an example 400 of a process for receiving a request from a user device and causing a corresponding media content item to be presented on the display device in response to receiving the request. In some implementations, blocks of process 400 can be implemented on a server, such as server 102.

Process 400 can begin by storing an ACL associated with the display device that indicates user devices that are authenticated to communicate with the display device and cause content to be presented on the display device at 402. For example, as described above in connection with FIG. 3, process 400 can store identifiers of user devices that are allowed to cause content to be presented on the display device in association with a token that corresponds to and/or indicates the display device. As a more particular example, as described above in connection with FIG. 3, process 400 can store an identifier of a user device in response to receiving a request to access the display device that includes the token corresponding to the display device. Note that, in some implementations, process 400 can update and/or modify the ACL at any suitable time(s) and in response to any suitable requests and/or information (e.g.,
information indicating a particular application has been closed, information indicating proximity of a particular user device to the display device, and/or any other suitable information).

At 404, process 400 can receive, from a user device, a request to present a media content item on the display device. In some implementations, the request can include any suitable information and can be received in any suitable manner. For example, in some implementations, the request can include an identifier corresponding to a media content item stored on server 102. As another example, in some implementations, the request can be received via a selection of a media content item from an application or browser window presented on the user device. In some implementations, process 400 can verify that the user device is included in the ACL stored at block 402. Note that, in some implementations, the requested content can be any suitable type of media content. For example, in some implementations, the requested media content can be a television program, a video, a piece of audio content, an image or picture, a slideshow, and/or any other suitable type of media content item. As another example, in some implementations, the requested media content can be a group of media content items, such as a playlist of media content items. As yet another example, in some implementations, the requested content can be a request to begin presenting a particular channel and/or stream of content, such as a particular broadcast channel of television content, a particular live stream of content (e.g., a radio program, a live video stream, and/or any other suitable type of content).

At 406, process 400 can transmit the requested media content item to the display device. For example, in some implementations, server 102 can transmit a stream of data corresponding to the media content item to the display device. In some implementations, process 400 can additionally transmit any suitable instructions for presenting the media content item, such as instructions for rendering a media player window on the display device within which the media content item is presented, and/or any other suitable instructions. As another example, in some implementations, process 400 can include instructions to navigate to a particular source of content, such as a particular channel and/or stream of content. As a more particular example, in some implementations, the instructions can include a Uniform Resource Locator (URL) specifying a location of the particular channel and/or stream of content.

Turning to FIG. 5, and example 500 of a process for a first user device to detect a second user device and transmit an authentication token to the second user device is shown in accordance with some implementations. In some implementations, the first user device can be
one that is already authenticated to communicate with a display device, as described above in connection with FIG. 3.

[0061] At 502, process 500 can detect, at a first user device, a second user device that is near the first user device. In some implementations, any suitable device discovery techniques can be used. For example, in some implementations, the first user device can detect other user devices that are connected to a particular network (e.g., a WiFi network in a home, a BLUETOOTH network, and/or any other suitable type of network). As another example, in some implementations, the first user device can transmit a multicast message to all devices on a particular network requesting device details from the devices on the network. As yet another example, in some implementations, the first user device can transmit an audible and/or subaudible tone and can detect nearby user devices that respond to detection of the tone.

[0062] As still another example, in some implementations, nearby user devices can be discovered based on detection of predetermined gestures and/or movements. As a more particular example, the first user device and the second user device can each be programmed to notify a server (e.g., server 102) when a particular gesture and/or movement is detected (e.g., when the user device is bumped, when the user device is moved in a particular manner, when a particular gesture is detected on a touch screen of the user device, and/or any other suitable gesture and/or movement), and the notification can indicate a geographic location of the user device (e.g., using GPS coordinates, an indication of a WiFi network and/or BLUETOOTH network the device is connected to, and/or any other suitable information). In some such implementations, the server can determine that two user devices are near each other if two user devices notify the server within a predetermined time period (e.g., within one minute, within five minutes, and/or any other suitable predetermined time period) of detection of the particular gesture and/or movement and are located with a particular geographic proximity (e.g., within a particular distance, connected to the same network, and/or any other suitable proximity metric). In some implementations, in response to determining that the two user devices are near each other, the server can transmit a message to one or both user devices indicating that the two user devices are near each other.

[0063] In some implementations, process 500 can present indications of detected user devices in any suitable manner. For example, in some implementations, indications of detected devices can be presented in a list within a particular application (e.g., an application associated
with presenting media content, an application associated with a social networking service, and/or any other suitable type of application). In some implementations, indications of detected devices can include any suitable information, such as a type of device (e.g., a tablet computer, a mobile phone, a wearable computer, and/or any other suitable type of device), a name associated with the device, a model of the device, and/or any other suitable type of information.

Note that, in some implementations, a user of the first user device can select the second user device by selecting a user of the second user device, such as from a list of contacts. In some such implementations, detection of the second user device can be omitted.

Process 500 can transmit an invitation message to be authenticated to the display device at 504. For example, in some implementations, the invitation message can indicate a name of the display device, a location of the display device, and/or any other suitable information. Note that, in some implementations, process 500 can transmit the invitation message in response to receiving a selection of a particular device from a list of detected devices. For example, in instances where process 500 presents indications of detected user devices in a list, process 500 can receive (e.g., from a user of a first user device), a selection of one or more of the detected user devices, and can transmit invitation messages to be authenticated to the display device to the selected user devices.

At 506, process 500 can transmit, to the second user device, a token corresponding with the display device. As described above in connection with FIG. 3, the token can be stored on a server that maintains an ACL indicating user devices that are allowed to communicate with the display device. Note that, in some implementations, the token can be one that was generated by the server in response to a request from the first user device and authentication of the first user device to the display device. Additionally or alternatively, in some implementations, the token can be one that was generated by the first user device during authentication of the first user device to the display device. In some implementations, the token can identify the display device and can allow the second user device to be authenticated to communicate with the display device when received by the server in a request from the second user device.

It should be understood that at least some of the above described blocks of the processes of FIGS. 3-5 can be executed or performed in any order or sequence not limited to the order and sequence shown in and described in the figures. Also, some of the above blocks of the
processes of FIGS. 3-5 can be executed or performed substantially simultaneously where appropriate or in parallel to reduce latency and processing times. Additionally or alternatively, some of the above described blocks of the processes of FIGS. 3-5 can be omitted.

In some implementations, any suitable computer readable media can be used for storing instructions for performing the functions and/or processes herein. For example, in some implementations, computer readable media can be transitory or non-transitory. For example, non-transitory computer readable media can include media such as magnetic media (such as hard disks, floppy disks, and/or any other suitable magnetic media), optical media (such as compact discs, digital video discs, Blu-ray discs, and/or any other suitable optical media), semiconductor media (such as flash memory, electrically programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), and/or any other suitable semiconductor media), any suitable media that is not fleeting or devoid of any semblance of permanence during transmission, and/or any suitable tangible media. As another example, transitory computer readable media can include signals on networks, in wires, conductors, optical fibers, circuits, any suitable media that is fleeting and devoid of any semblance of permanence during transmission, and/or any suitable intangible media.

In situations in which the systems described here collect personal information about users, or make use of personal information, the users may be provided with an opportunity to control whether programs or features collect user information (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location). In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over how information is collected about the user and used by a content server.

Accordingly, methods, systems, and media for authentication of user devices to a display device are provided.

Although the invention has been described and illustrated in the foregoing illustrative implementations, it is understood that the present disclosure has been made only by
way of example, and that numerous changes in the details of implementation of the invention can
be made without departing from the spirit and scope of the invention, which is limited only by
the claims that follow. Features of the disclosed implementations can be combined and
rearranged in various ways.
What is claimed is:

1. A method for authentication of user devices, the method comprising:
   authenticating a first user device to a display device, wherein an authentication
   token is associated with the authentication of the first user device to the display device, wherein
   the authentication token is stored on a server in association with an identifier of the first user
   device, and wherein the first user device is provided with media playback control on the display
   device in response to the authentication;
   identifying, using the first user device, a second user device in proximity to the
   first user device;
   transmitting, from the first user device to the second user device, an invitation
   message to authenticate the second user device to the display device; and
   in response to receiving a response to the invitation message from the second user
   device, transmitting the authentication token from the first user device to the second user device,
   wherein the authentication token causes the second user device to request authentication to the
   display device from the server, wherein the second user device is provided with media playback
   control on the display device in response to authenticating with the display device.

2. The method of claim 1, further comprising:
   generating, using the first user device, the authentication token; and
   transmitting the authentication token to the server.

3. The method of claim 1, further comprising:
   transmitting, to the server, a request for the authentication token; and
   receiving the authentication token from the server.

4. The method of any preceding claim, further comprising receiving, from a contact
   list associated with a first user of the first user device, an indication of a second user of the
   second user device, wherein the second user device is identified based on the received indication.

5. The method of any preceding claim, wherein identifying the second user device
   comprises detecting the second user device based on a connection to a network.
6. The method of any preceding claim, wherein identifying the second user device comprises:

detecting a movement of the first user device;
transmitting, to the server, an indication of the movement and a first location associated with the first user device; and
receiving, from the server, an identifier associated with the second user device, wherein the second user device detected a movement of the second user device at a second location and wherein the first location and the second location are within a predetermined distance.

7. The method of any preceding claim, further comprising:

receiving, from a user of the first user device, an indication that the second user device is not to be authenticated to the display device; and
transmitting, to the server, a request to remove authentication permission for the second user device to the display device.

8. A system for authentication of user devices, the system comprising:

a hardware processor on a first user device that is configured to:
authenticate the first user device to a display device, wherein an authentication token is associated with the authentication of the first user device to the display device, wherein the authentication token is stored on a server in association with an identifier of the first user device, and wherein the first user device is provided with media playback control on the display device in response to the authentication;

identify, using the first user device, a second user device in proximity to the first user device;

transmit, from the first user device to the second user device, an invitation message to authenticate the second user device to the display device; and

in response to receiving a response to the invitation message from the second user device, transmit the authentication token from the first user device to the second user device, wherein the authentication token causes the second user device to request authentication
to the display device from the server, wherein the second user device is provided with media playback control on the display device in response to authenticating with the display device.

9. The system of claim 8, wherein the hardware processor is further configured to:
   generate, using the first user device, the authentication token; and
   transmit the authentication token to the server.

10. The system of claim 8, wherein the hardware processor is further configured to:
    transmit, to the server, a request for the authentication token; and
    receive the authentication token from the server.

11. The system of any of claims 8 to 10, wherein the hardware processor is further configured to receive, from a contact list associated with a first user of the first user device, an indication of a second user of the second user device, wherein the second user device is identified based on the received indication.

12. The system of any of claims 8 to 11, wherein the hardware processor is further configured to detect the second user device based on a connection to a network.

13. The system of any of claims 8 to 12, wherein the hardware processor is further configured to:
    detect a movement of the first user device;
    transmit, to the server, an indication of the movement and a first location associated with the first user device; and
    receive, from the server, an identifier associated with the second user device, wherein the second user device detected a movement of the second user device at a second location and wherein the first location and the second location are within a predetermined distance.

14. The system of any of claims 8 to 13, wherein the hardware processor is further
configured to:

receive, from a user of the first user device, an indication that the second user device is not to be authenticated to the display device; and

transmit, to the server, a request to remove authentication permission for the second user device to the display device.

15. A non-transitory computer-readable medium containing computer-executable instructions that, when executed by a processor, cause the processor to perform the method of any of claims 1 to 7.
300

User Device 110

302
AUTHENTICATE USER DEVICE 108 TO A DISPLAY DEVICE

304
STORE A TOKEN ASSOCIATED WITH USER DEVICE 108

306
DETECT AND/OR INVITE USER DEVICE 110

308
TRANSMIT THE TOKEN

310
REQUEST PERMISSION TO PAIR WITH DISPLAY DEVICE BASED ON THE TOKEN

312
GRANT ACCESS TO USER DEVICE 110 TO PAIR WITH DISPLAY DEVICE

Server 102
1. Store an access control list that indicates user devices allowed to pair with a display device.

2. Receive, from a user device on the access control list, a request to present a media content item on the display device.

3. Transmit the media content item to the display device.

**FIG. 4**
500

DETECT, AT A FIRST USER DEVICE, A NEARBY SECOND USER DEVICE

502

TRANSMIT AN INVITATION TO PAIR WITH A DISPLAY DEVICE CURRENTLY PAIRED WITH THE FIRST USER DEVICE

504

IN RESPONSE TO RECEIVING CONFIRMATION OF THE INVITATION, TRANSMIT AN AUTHENTICATION TOKEN TO THE SECOND USER DEVICE

506

FIG. 5
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/44 H04L29/06 H04N21/258

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>EP 3 041 245 Al (SPOTIFY AB [SE])</td>
<td>1-15</td>
</tr>
<tr>
<td></td>
<td>6 July 2016 (2016-07-06)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0006]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0017] - paragraph [0018]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0049] - paragraph [0050]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0047]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0034] - paragraph [0035]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0042]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0054] - paragraph [0055]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>abstract</td>
<td></td>
</tr>
<tr>
<td></td>
<td>figures 1,4,6B,7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-/-</td>
<td></td>
</tr>
</tbody>
</table>

[X] Further documents are listed in the continuation of Box C.  

[X] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"S" document member of the same patent family

Date of the actual completion of the international search: 25 October 2017

Date of mailing of the international search report: 06/11/2017

Name and mailing address of the ISA:

European Patent Office, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel: (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer:

Dobre, Dan
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>
| A        | WO 2015/200535 A1 (GOOGLE INC [US])  
30 December 2015 (2015-12-30)  
paragraph [0054]  
paragraph [0056]  
paragraph [0010]  
paragraph [0028]  
abstract  
figures 3,4 | 1-15 |
| A        | US 2014/173695 A1 (VALDIVIA CARLOS [US])  
19 June 2014 (2014-06-19)  
abstract  
claim 2  
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>EP 3041245 A1</td>
<td>06-07-2016</td>
<td>CN 107113309 A</td>
<td>29-08-2017</td>
</tr>
<tr>
<td>WO 2015200535 A1</td>
<td>30-12-2015</td>
<td>CN 106462642 A</td>
<td>22-02-2017</td>
</tr>
</tbody>
</table>