Technical Disclosure Commons

Defensive Publications Series

November 19, 2017

Remote control of a kiosk device

Michael Siconolfi

Jonathan Deokule

Michael DePasquale

Remote control of a kiosk device

ABSTRACT

The techniques of this disclosure provide low-latency, access-controlled, secure bidirectional data channels for remotely controlling devices over a network, e.g., kiosk devices. The techniques of this disclosure enable remote users to communicate with and control a kiosk device, e.g., a video-conferencing system. Remote users can issue remote procedure calls (RPCs) to kiosk devices. Kiosk devices can provide state notifications to remote users. Communication between remote users and kiosk devices is governed by access control mechanisms. For example, access control policies can be deployed that restrict the RPCs a remote user sends to a kiosk device, and the state notifications that a remote user receives. Further, multiple independent channels can be established between pairs of remote users and kiosk devices, and a channel-specific access control policy can be provided.

KEYWORDS

- kiosk device
- data channel
- remote user
- access control
- Videoconference
- remote maintenance

BACKGROUND

Support and Maintenance

Kiosk devices, e.g., video-conferencing systems, may need periodic maintenance and/or servicing, which can impose costs if a technician needs to physically visit each device. Remote management of devices can reduce such costs.

Physical Proximity

Kiosk devices, are often physically deployed in fixed locations, which in the case of large rooms, severely limits the number of users that can operate the device to people that are located directly in front of the kiosk. Remote management of such devices can allow in-room participants to access the kiosk interface without needing to be in close proximity to the device.

Accessibility

Many kiosk devices may not provide any accessibility features for users who are unable to interact directly with the kiosk device (e.g., due to a physical disability). Remote management of such devices can integrate with accessibility technologies (e.g., screen readers) to provide a common experience for users of all abilities.

DESCRIPTION

This disclosure describes a low-latency, access-controlled, secure bidirectional data channel for remotely controlling devices, e.g., kiosk devices, over a network. For example, video-conferencing hardware can be remotely controlled using the described techniques.

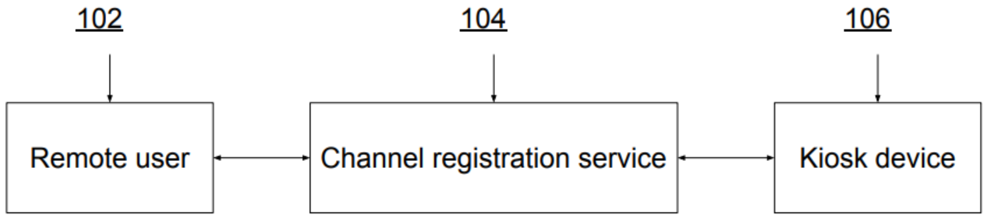

Fig. 1: Data channel registration

Fig. 1 illustrates an example of data channel registration between a remote user and a kiosk. The data channel is created using an access-controlled channel registration service (104) that is responsible for applying access control mechanisms to determine whether to authorize the data channel between a remote user (102) and a kiosk device (106).

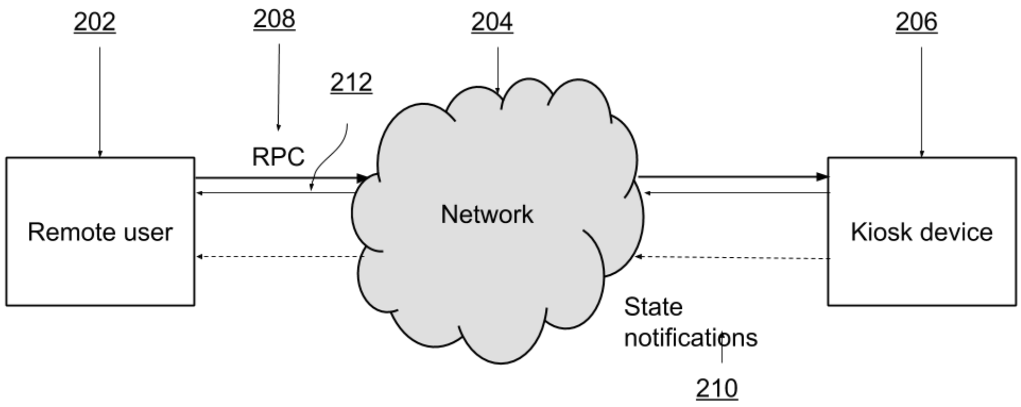

Fig. 2: Communication model between remote user and kiosk device

Fig. 2 illustrates an example of two endpoints securely communicating with each other. Once the data channel authorization is established, a remote user (202) and a kiosk device (206) can securely communicate with each other over a network (204) using the following communication patterns:

- **Remote Procedure Calls (RPCs):** A remote procedure call (208) is an invocation of a remote message request by a remote user to a kiosk device. The kiosk device receives the request, performs an action based on the request, and replies to the remote user with a response message (212). The remote user receives the response and can performs related actions.

- **State Notifications:** State notifications (210) are one-way notification messages that contain device state information and is sent by the kiosk device to the remote user, e.g., heartbeat, progress updates, response to external inputs, transition notification, initial state, etc.

The communication between the remote user and the kiosk device is configured such that the set of authorized RPCs and State Notifications are controlled by a policy mechanism, e.g., an access control policy. The access control policy allows different remote user/kiosk device pairs to have various levels or tiers of communication between them. For example, the level of control may depend on the level of security, and defined criteria for connection and resource types.

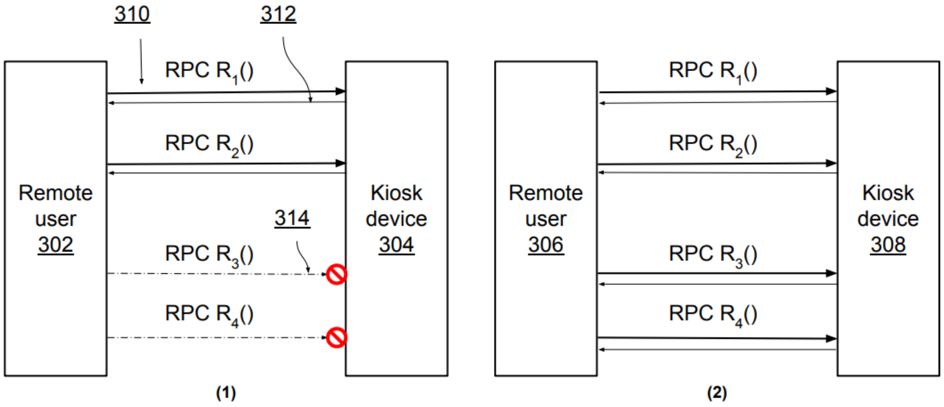

Fig. 3(a): Remote users with (1) restricted, and (2) unrestricted access control policies that affect the RPCs they may invoke

Fig. 3(a) illustrates an example where different remote users, one with restricted access control policy and another with unrestricted access control policy issue RPCs to a kiosk device. The access control policy controls the RPCs each remote user can invoke. As shown in Fig. 3(a), the communication between a first remote user (302) and kiosk device (304), and a second remote user (306) and kiosk device (308) is controlled by a respective policy. In this example, in Fig. 3(a)(1), the remote user (302) has a restricted access control that permits RPCs R_1 and R_2 and restricts R_3 and R_4. In Fig. 3(a)(2), the remote user (306) has unrestricted access to all RPCs R_1, R_2, R_3, and R_4.

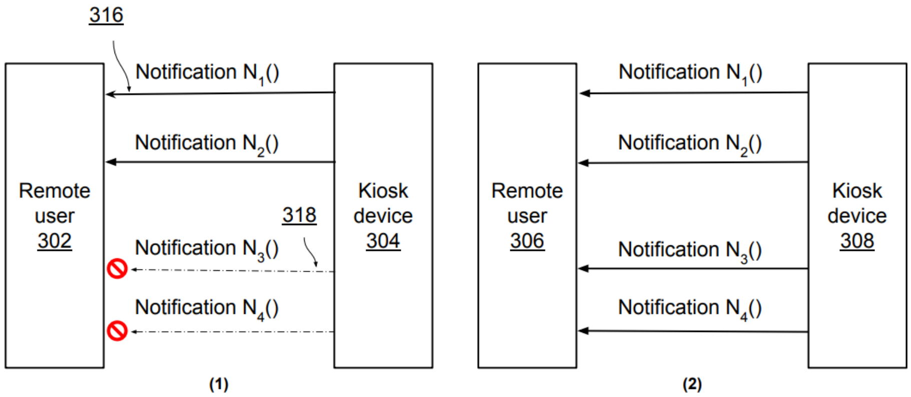

Fig. 3(b): Remote users with (1) restricted and (2) unrestricted access control policies that affect notifications they may receive

Similarly, Fig. 3(b) illustrates that state notifications between the remote user/kiosk device pairs are also controlled by the policy. In Fig. 3(b) (1), the remote user (302) receives state notifications N_1 and N_2 but not N_3 and N_4, per the access control policy. In Fig. 3(b) (2), the remote user (306) receives all state notifications N_1, N_2, N_3, and N_4.

A kiosk device per the techniques of this disclosure can support multiple independent channels for multiple users. Each individual channel can provide different access control policies and the communication is isolated from other remote channel users. Fig. 4 illustrates an example of multiple users communicating with a single kiosk device, each with different access control policies.

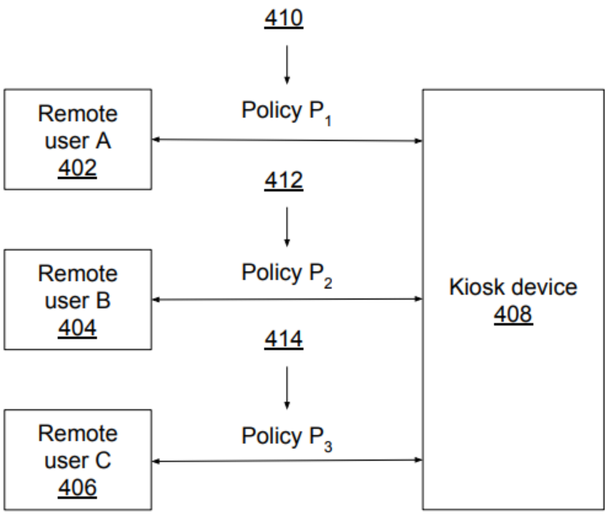

Fig. 4: Multiple users communicating with a single kiosk device, each user with a different access control policy

As illustrated in Fig. 4, each of remote users A (402), B (404), and C (406) communicate with kiosk device (408) via independent channels. Each of the channels have independent access control policies P_1 (410), P_2 (412), and P_3 (414). Additionally, a single user can establish multiple independent channels to multiple kiosk devices.

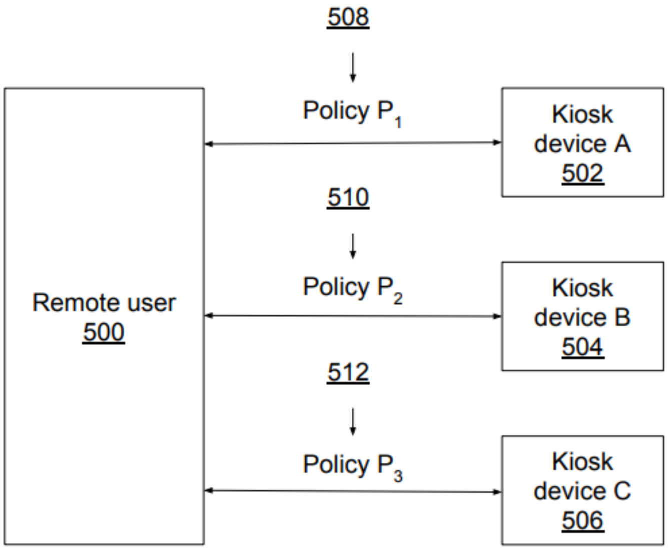

Fig. 5: Single remote user communicating with multiple kiosk devices, each of which may have different access control policies

Fig. 5 illustrates an example of a single user communicating with multiple kiosk devices, each of which may have different access control policies. Remote user (500) establishes a communication channel with kiosk device A (502), kiosk device B (504), and kiosk device C (506). Each of these communication channels are governed by respective access control policies. Policy P1 (508) governs the communication channel between the remote user and kiosk device A. Similarly, policy P2 (510) and policy P3 (512) are respective access control policies for the other two communication channels.

The techniques of this disclosure enable remote users to communicate with and control a kiosk device, e.g., a video-conferencing system. Remote users can issue remote procedure calls (RPCs) to kiosk devices. Kiosk devices can provide state notifications to remote users. Communication between remote users and kiosk devices is governed by access control mechanisms. For example, access control policies can be deployed that restrict the RPCs a remote user sends to a kiosk device, and the state notifications that a remote user receives. Further, multiple independent channels can be established between pairs of remote users and kiosk devices, and a channel-specific access control policy can be provided.

CONCLUSION

The techniques of this disclosure provide low-latency, access-controlled, secure bidirectional data channels for remotely controlling devices over a network, e.g., kiosk devices. The techniques of this disclosure enable remote users to communicate with and control a kiosk device, e.g., a video-conferencing system. Remote users can issue remote procedure calls (RPCs) to kiosk devices. Kiosk devices can provide state notifications to remote users. Communication between remote users and kiosk devices is governed by access control mechanisms. For example, access control policies can be deployed that restrict the RPCs a remote user sends to a kiosk device, and the state notifications that a remote user receives. Further, multiple independent channels can be established between pairs of remote users and kiosk devices, and a channel-specific access control policy can be provided.