May 2021

ENHANCED VIDEO AND WEB CONFERENCING SECURITY FOR DUAL ACCOUNT ENDPOINTS

Kevin Collins

Steve Connolly

Denis Mchugh

Alan Mccann

ENHANCED VIDEO AND WEB CONFERENCING SECURITY FOR DUAL ACCOUNT ENDPOINTS

AUTHORS:
Kevin Collins
Steve Connolly
Denis Mchugh
Alan Mccann

ABSTRACT

Dual account video and web conferencing endpoints have both a personal user account and a shared room account that are registered on the same device. When such an endpoint joins a meeting (e.g., after completing a pairing process) it raises a number of security, etc. challenges. To address these types of challenges, various solutions are presented herein through several techniques. In particular, the techniques may include support for devices utilizing proximity in a reverse fashion (i.e., personal mode endpoints may use ultrasound pairing to detect that the personal user is in proximity to a device and allow them to perform authenticated actions directly using the device’s user interface (UI)). The techniques may further provide a way of pairing personal devices with clients without the need for ultrasound or manual pairing.

DETAILED DESCRIPTION

Dual account video and web conferencing endpoints have both a personal user account and a shared room account that are registered on the same device. The personal user account has access to personally identifiable information (PII) data in the cloud, may store the user's PII, and can make requests to cloud services as the personal user.

When such an endpoint joins a meeting (e.g., after completing a pairing process) or accesses data in the cloud, it is important to ensure that the personal user is actually the one who is using the video endpoint and thus grant the owning user's privileges only where appropriate.

Presently, video and web conferencing device pairing is performed in one of two ways, ultrasound pairing and manual pairing.

Ultrasound pairing is achieved by transmitting tokens as ultrasound and validating them in the cloud. However, ultrasound proximity is not a completely (i.e., 100%) reliable means of connecting to devices. Among other things, ultrasound proximity can fail and be unreliable in certain conditions. For example, there are often problems with:

1. The microphone on a laptop or mobile device
2. The ultrasound volume may be set too low on a device
3. Organizations may choose to have ultrasound turned off by default
4. Having many devices in the same space (e.g., an open office) can cause interference with ultrasound transmission. This can also lead to pairing jumping between devices.

Manual pairing as a back up to ultrasound pairing is slow and cumbersome to perform, requiring device look ups, multiple cloud requests, and the manual entry of a personal identification number (PIN). Manual pairing may be done from a client and may involve, for example:

1. Typing the name of the device that the user wants to pair with and performing a search.
2. Selecting the device, resulting in the sending of a request to the cloud.
3. The cloud notifying the device to display a PIN number.
4. A user manually entering the PIN on the client.
5. The cloud then validating the PIN and marking the client and device as paired.

Additionally, often users do not realize that they are not paired until they want to perform some paired action such as, for example, making a call.

To address challenges of the types that were described above, various solutions are provided herein through several techniques. A first technique, as presented herein and as discussed and illustrated below, supports devices utilizing proximity in a reverse fashion. A second technique, as presented herein and as discussed and illustrated below, supports, among other things, a way of pairing personal devices with clients without the need for ultrasound or the existing manual pairing.

Turning to the first technique, aspects of this technique support, among other things, devices utilizing proximity in a reverse fashion. Typically, ultrasound has been used by video and web conferencing clients to detect and pair with devices and perform actions on paired devices. According to aspects of the first technique, personal mode endpoints may use ultrasound pairing to detect that the personal user is in proximity to a device and allow them to perform authenticated actions directly using the device's UI.

Traditionally, ultrasound proximity has been used by video and web conferencing clients to control shared devices in a meeting room. But it is more common when using small and home office devices to interact with the device directly through its UI. According to aspects of the first technique, devices in dual mode may use proximity to detect that the personal user is using the device directly and therefore give authenticated access to features of the device. Such detection and determination may encompass a number of steps, including, for example:

1. A video endpoint has the personal identity of a specific human user.
2. The same endpoint also registers a public shared identity that is associated in the cloud, upon creation, with the owning personal user.
3. A back-end cloud service knows the identity of the owning user that created the public shared identity.
4. The endpoint uses a proximity pairing mechanism to detect when the owning user is nearby.
5. When the endpoint detects its owner:
    a. It allows the user to access PII through its local interface.
    b. It sends requests to cloud services with the public shared identity. Such requests include another field that indicates it is acting on behalf of the owning user.
    c. When a cloud service gets a request with the additional field, it looks up the owning user's identity that is associated with the public shared identity and allows the endpoint to take actions that are available to the owning user.
    d. This affirms the authenticity of the human user using the device through its user interface.
6. Otherwise:
    a. The endpoint blocks access to any locally stored PII.

b. The endpoint sends requests to cloud services with its generic identity without the additional field indicating it is acting on behalf of the owning user.

It is important to note that under aspects of the first technique no reboot is required, there is no blind broadcast of tokens to an unknown device, and there are no extra round-trips between a client and a server. Instead, the client request to the server carries the necessary information to allow the server to securely verify that the endpoint's owner is in proximity and, accordingly, the endpoint may act as the owner.

Aspects of the first technique may be used by a vendor to unlock features on dual mode devices that have detected the proximity of the personal user. Proximity is available on the shared account stack and will detect the personal stack user thus authenticating the personal user and granting access to features that the user will perform on the personal account stack through the UI on the device.

Such an approach is particularly beneficial for home and small office scenarios where a device is interacted with directly, unlike shared systems used in meeting rooms that would be at a distance and controllable from a client application.

Video and web conferencing clients have a login flow that authenticates the user with the cloud and only then can a video and web conferencing device and client detect and pair with each other. This ensures the personal user’s physical proximity to the device which proves integrity and the authenticity of the user.

Aspects of the first technique provide a number of benefits including, for example, increased secure use of personal devices, enhanced privacy of whiteboards, guaranteed integrity of a call (in terms of roster), authenticity within a call, enhanced privacy of call history, etc.

In connection with the first technique, it is important to note the distinctions between that technique and a guest mode on a device. Guest mode requires profile switching by thumb print or some other mechanism. Once a profile is activated it is then a device belonging to a user, all actions are on behalf of that user, and data is stored on the device and partitioned from other profiles.

Under aspects of the first technique there are no profiles. The device is a personal device. But as it may have a desk device in an office space or at home, it can be approached by people and its contents read or calls made. But by using cloud-based ultrasound proximity the device can validate the proximity of a user and then, as needed, hide away any PII data and authenticate in meetings that the personal user is actually using the device.

Additionally, a major advantage of the first technique is that the approach is 'touch-less' for a user. The 'magic' just happens, without the user needing to login, use a fingerprint, etc. In connection with the first technique, it is also important to note the distinctions between that technique and extension mobility via proximity. Extension mobility is a way of getting a profile onto a desk phone (e.g., provisioning a device to be a user's device).

Aspects of the first technique are not based around provisioning. There is no login. Devices are already provisioned in personal mode and subsequently use cloud proximity to validate and authenticate the personal user. Additionally, a personal solution is rather slow and has security limitations. For example, when the process succeeds the enterprise phone must reboot to assume the paired user's identity. As well, the mobile device receives the base station's device token and passes it to a telephony server. However, a malicious device could implement an internal audio protocol that facilitates connection to devices using ultrasound, collect device tokens, and attempt various types of attacks (such as, for example, a man-in-the- middle attack).

Cloud registered desk devices are more feature rich then on-premise devices. They can access cloud services to retrieve PII information and can be used similarly to mobile devices. But they are not mobile, and thus can potentially be used by users other than the personal account user.

Accordingly, aspects of the first technique add a level of security to device actions that the device can apply to its feature set. And it all happens without the user having to re-provision, login via touch, or switch profiles.

Aspects of the first technique allow a device to be used as a shared cloud endpoint or a user's personal endpoint based on proximity. The endpoint offers many features even in public mode, such as the ability to join meetings or be used in wireless share sessions. In other examples, it looks like a mobile phone or an enterprise phone that is unusable by anyone who is not specifically provisioned to have access.

Turning to the second technique, as referenced above, aspects of this technique support, among other things, a way of pairing personal devices with clients without the need for an ultrasound token exchange between a device and client or the existing manual pairing.

On a personal device with dual registration the shared account knows of its personal account identifier (ID) and can signal the cloud to set the paired status for clients in which the user is logged in.

A personal device pairing with clients may encompass a number of steps, including, for example:

1. The shared account knows the user identity of the personal registration
2. The shared account sends a request to the cloud to pair with clients.
3. In the request will be the identity of the personal user of the device.
4. The cloud service performs a look up to find what registered clients belong to the user.
5. The identified clients are marked as verified and paired with the device.
6. Finally, the cloud service will notify each of the clients of the pairing.

Aspects of the second technique offer many advantages over the existing methods, including, for example:

1. A single click of a button on the device initiates a single request to the cloud.
2. Clients are instantly paired.
3. The pairing of personal devices is guaranteed.
4. Manual pairing entails a multi-click operation.
5. Ultrasound proximity pairing sometimes does not work, whereas aspects of the second technique work reliably.

In connection with the second technique, it is important to note that a user is employing their personal device. Thus, only their personal clients will become paired with that device. Accordingly, pairing with devices that are not in proximity is not necessarily a security issue as pairing alone can entail no malicious action. Clients that pair are installed on a user’s own password-protected device (e.g., a mobile device, a laptop, etc.). The new pairing action simply sets the personal user's clients as paired. Any other user which is in proximity may still pair through, for example, an ultrasound mechanism.

In brief, aspects of the second technique provide an on-demand pairing which is actioned via one button on a device, which eliminates all of the problems with microphones, etc. and all of the other issues that can occur during ultrasound-based pairing, and which eliminates the cumbersome manual pairing process.

For purposes of exposition, Figure 1, below, depicts aspects of the proximity techniques that were described in the above narrative.

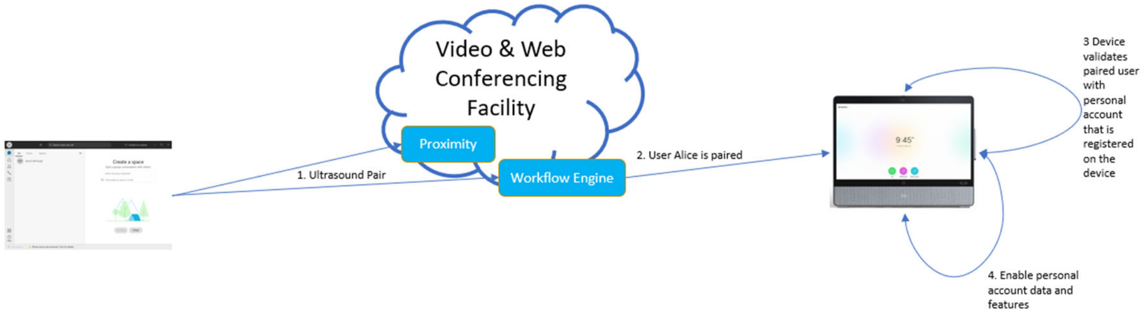
Video & Web Conferencing Facility
Proximity
Workflow Engine
1. Ultrasound Pair
2. User Alice is paired
9:45
3 Device validates paired user with personal account that is registered on the device
4. Enable personal account data and features

Figure 1: Exemplary Personal Proximity Feature Enablement

As depicted in Figure 1, above, a proximity-based enablement process in accordance with the techniques presented herein may comprise a number of steps, including:

1. A collaboration client pairs with a device using ultrasound proximity.
2. A workflow engine notifies the device what user has paired.
3. The device compares the paired user with the personal identity that is registered on the device.
4. If the values match, the device can then enable certain features which expose personal content such as, for example, whiteboards, call history, etc.

In brief, a device can utilize proximity pairing to identify the personal identity that is registered on the personal device thus exposing data or information on the device that is PII to the user.

For purposes of further exposition, Figure 2, below, depicts aspects of the pairing techniques that were described in the above narrative.

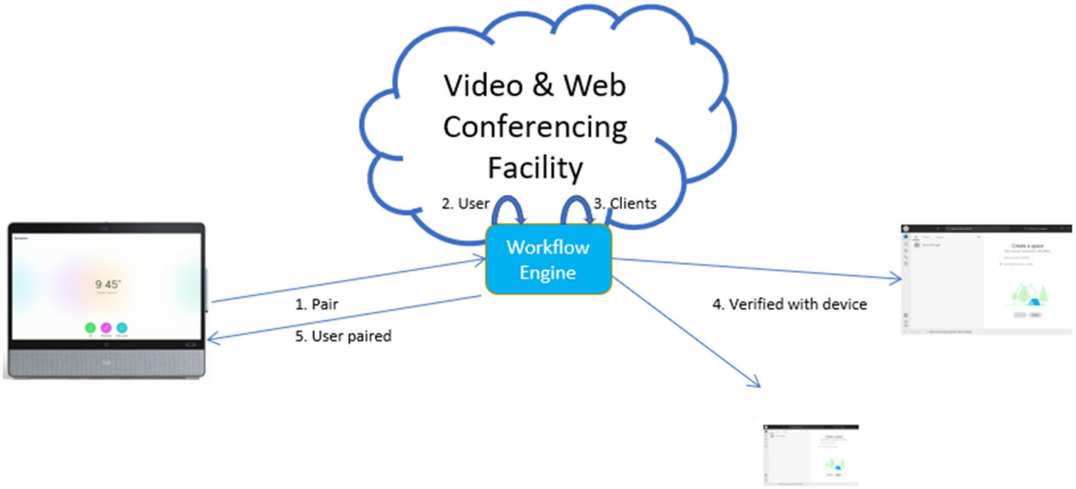

Figure 2: Exemplary Pairing Process

As depicted in Figure 2, above, a pairing process in accordance with the techniques presented herein may comprise a number of steps, including:

1. A user clicks or selects a ‘pair’ button on a video and web conferencing device;
2. A workflow engine performs a lookup operation to identify the owning user;
3. The workflow engine performs a lookup operation to identify the collaboration clients that belong to that user;
4. The workflow engine sets all collaboration clients as verified and notifies them; and
5. The workflow engine notifies the device of the paired collaboration clients and the device may display such pairing notification through its UI.

In summary, techniques have been presented herein that include support for devices utilizing proximity in a reverse fashion (i.e., personal mode endpoints may use ultrasound pairing to detect that the personal user is in proximity to a device and allow them to perform authenticated actions directly using the device’s UI). The techniques that have been presented herein may further provide a way of pairing personal devices with clients without the need for ultrasound or manual pairing.