October 16, 2019

Pre-Provisioning For Protected Content Playback In Closed Network Environments

Xiaohan Wang

Pre-Provisioning For Protected Content Playback In Closed Network Environments

ABSTRACT

Closed network environments, such as in-flight entertainment (IFE) where users connect their own devices such as smartphones, tablets, laptops, etc. are becoming common. In such environments, playback of protected content on devices is made possible by the presence of streaming and licensing servers that are present within the closed network environment, e.g., aboard a flight. The provisioning server for such content, however, is hosted by a third party and is generally unavailable within the closed environment, which causes playback to fail. This disclosure describes techniques of pre-provisioning without imposing a requirement on the user to download additional applications, such that different content websites get different certificates that don't cross-reference on the same device. In this manner, protected content is delivered to closed-environment users in a convenient, privacy-preserving manner.

KEYWORDS

- In-flight entertainment (IFE)
- Closed network
- Content playback
- Protected content
- Content decryption module (CDM)
- Pre-provisioning

BACKGROUND

Closed network environments, such as in-flight entertainment (IFE) where users connect their own devices such as smartphones, tablets, laptops, etc. are becoming common. In such environments, an isolated, in-flight WiFi network that has a low-bandwidth external connection (or no external connection) is provided. The term IFE is used henceforth to refer to any closed network environment. Playback of protected content on user devices is made possible by the presence of onboard streaming and licensing servers. The provisioning server, however, is hosted by a third party and is generally not available within the closed environment. Playback of protected content is enabled by the provisioning of a content decryption module (CDM) to authenticate the device. Without access to the provisioning server, playback fails.

For native applications, it is possible to perform pre-provisioning when the device has internet access, e.g., prior to and in preparation for playback during the IFE phase. However, it is an unreasonable burden to expect users, e.g., passengers on a flight, to have a pre-installed, pre-provisioned application, or to download additional applications prior to entering the IFE environment. A browser-based solution is attractive since browser applications are available on most user devices. However, CDM provisioning on a browser is performed on a per-website (origin) basis such that different websites get different certificates that cannot be cross-referenced on the same device. Since it is generally not possible to predict the web origin of the next IFE playback, it is not possible to pre-provision for such playback.

Certain older browsers, operating systems, or devices support per-device provisioning. In such devices, once provisioning is triggered and completed by one application, other applications on the same device do not need to perform provisioning again.

DESCRIPTION

Per the techniques of this disclosure, a mobile device is classified based on whether or not it supports origin-specific identity. Under origin-specific identity, different websites get different certificates that cannot be cross-referenced on the same device. Pre-provisioning is carried out differently for devices where provisioning does, or does not, involve a stable identifier, as follows.

Pre-provisioning on devices where provisioning does not involve a stable identifier

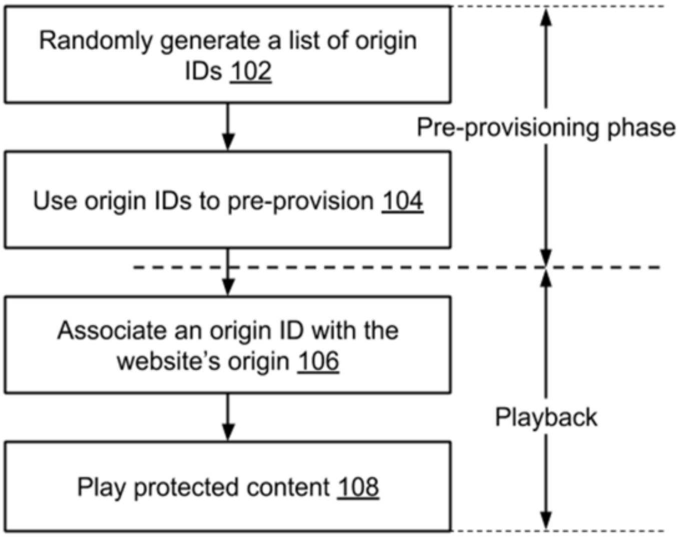
Randomly generate a list of origin IDs 102
Use origin IDs to pre-provision 104
Associate an origin ID with the website's origin 106
Play protected content 108
Pre-provisioning phase
Playback

Fig. 1: Pre-provisioning and protected content playback for devices where provisioning does not involve a stable identifier

Fig. 1 illustrates pre-provisioning on devices where provisioning does not involve a stable identifier, per techniques of this disclosure. In a pre-provisioning phase, a list of origin identifiers, which may be strings, is generated (102). The origin identifiers are used in pre-provisioning (104). In a playback phase, e.g., during in-flight entertainment, an origin identifier is associated with the website's origin at runtime (106). The protected content is played (108).

The pre-provisioning process attempts to provision all origin identifiers in the list such that they can be used during playback. Pre-provisioning starts upon browser startup. For devices where pre-provisioning does not involve a stable identifier, the identifier involved in the provisioning process can be reset by users; therefore pre-provisioning, as described herein, preserves user privacy.

Pre-provisioning on devices where provisioning involves a stable identifier

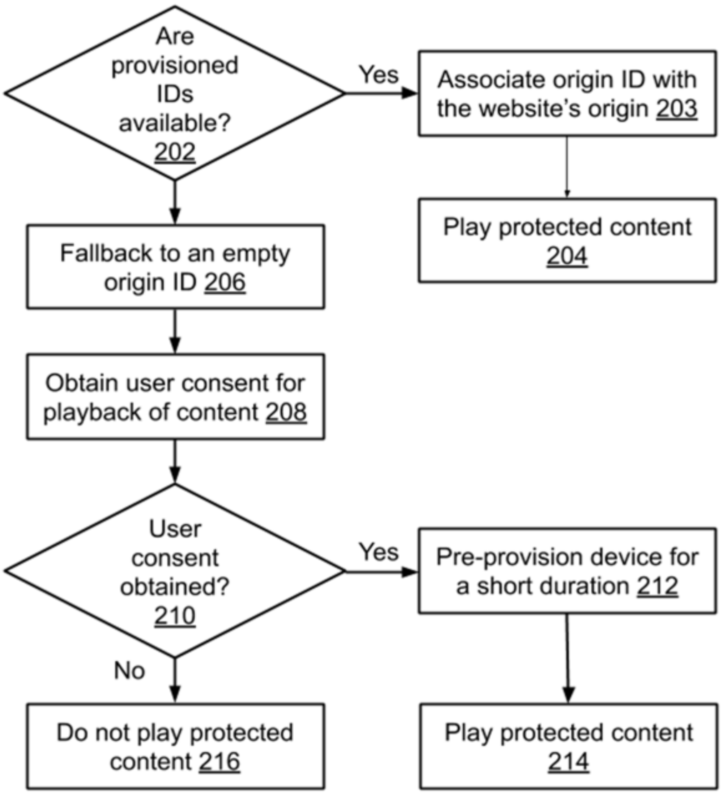
Are provisioned IDs available? 202
Yes
Associate origin ID with the website's origin 203
Play protected content 204
Fallback to an empty origin ID 206
Obtain user consent for playback of content 208
User consent obtained? 210
Yes
Pre-provision device for a short duration 212
No
Do not play protected content 216
Play protected content 214

Fig. 2: Pre-provisioning and playback of protected content for devices where provisioning involves a stable identifier

Pre-provisioning and playback of protected content for devices where provisioning involves a stable identifier is illustrated in Fig. 2. The device is checked for the availability of provisioned origin IDs (202). If provisioned IDs are available, the origin ID is associated with the website's origin (203), and protected content is played (204). If the device is not provisioned, the method falls back to an empty origin identifier (206). User consent for playback of content is obtained (208). If user consent is not obtained (210), the protected content is not played (216).

When the user provides consent, the browser attempts to pre-provision the device (212). Protected content is played (214). Since user interest in the content eventually fades and expires, any protected content playback, a sign of legitimate user interest, triggers pre-provisioning of a list of origin IDs for a short duration, e.g., 24 hours, such that provisioned IDs are available for the duration. In this approach, the user's attempt to play protected content is a signal of the user's interest in protected content playback, and the device is pre-provisioned based on this interest.

For example, if a user watches protected content while the device has internet access, pre-provisioning is started and completed right away. As another example, if a user attempts to watch protected content on a flight on a device that is not provisioned, the device falls back to an empty origin identifier with user consent. Pre-provisioning of a list of origin IDs is performed for a 24-hour duration, and content played on the user's device. If the user leaves the closed network environment, e.g., on a flight, and continues to have internet access, pre-provisioning is triggered and completed within the 24-hour window. In both examples, IFE playback works on the device, since it is pre-provisioned.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of 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), and if the user is sent content or communications from a server. 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 what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes techniques of pre-provisioning a user device without imposing a requirement on the user to download additional applications, such that different content websites get different certificates that do not cross-reference on the same device. In this manner, protected content is delivered to closed-environment users in a convenient, privacy-preserving manner.