November 2021

Using xAU Tokens to Count Unique Active Users Per Epoch Without Cookies

Adrian Isles

Using xAU Tokens to Count Unique Active Users Per Epoch Without Cookies

ABSTRACT

User engagement and adoption is typically measured in terms of the number of users active during a given period, generally termed as xAU where x stands for the measurement time interval. Without third-party cookies, it is difficult to obtain xAU measures, especially when content is embedded within other applications and services.

This disclosure describes cookieless techniques to determine a lower bound for various xAU measures. Upon receiving a request for content, a xAU token for the user agent is generated and cryptographically signed on the server and relayed to the user agent for local caching. Each xAU token can be a tuple of the form (period, nonce, cryptographic signature). Once the epoch corresponding to the period in the xAU token expires, the corresponding xAU token is sent back to the server via an out-of-band channel. The number of unique active users per epoch is obtained by counting the number of unique xAU tokens seen over the corresponding epoch. Implementation of the techniques with user permission enables reasonably accurate counts for unique active users during a given period, without requiring the use of third-party cookies.

KEYWORDS

- Unique visitors
- Third-party content
- Third-party cookies
- Visitor count
- Embedded video
- Embedded content
- Daily active users (DAU)
- Weekly active users (WAU)
- Monthly active users (MAU)

BACKGROUND

User engagement and adoption for a website, service, or application is typically measured in terms of the number of users active during a given period, such as Daily Active Users (DAU), Weekly Active Users (WAU), Monthly Active Users (MAU), etc., referred to in this document as xAU where x stands for the measurement time interval. These measures are often obtained using third-party cookies within the web browser.

Web browsers are increasingly phasing out support for third-party cookies or enabling users to prohibit sites from setting third-party cookies. While some users and applications may avoid the use of third-party cookies for privacy reasons, non-availability of such cookies makes it difficult for sites and service providers to obtain xAU measures for their products and services. For instance, these issues are particularly salient in cases where a site or app embeds content from third parties, such as embedded videos from social media or video-hosting platforms. Without third-party cookies associated with content display/playback, providers of the content cannot count unique views of the content.

Instead of cookies, a trusted third-party server can be used to aggregate xAU counts and relay the corresponding report to the providers of products and services. However, such an approach can be expensive and difficult to implement.

DESCRIPTION

This disclosure describes cookieless techniques to determine a lower bound for various xAU measures for user engagement with third-party content embedded within an application, website, or service. With user permission, the server that hosts the content can generate one or more unique tokens, called xAU tokens, for each user agent (e.g., browser or application) that corresponds to an embedded origin for the content. Only one xAU token is ever sent to the user agent per epoch, thus permitting server-side computation of unique active users per epoch by counting the number of unique xAU tokens seen over the corresponding epoch.

Each xAU token is a tuple of the form (period, nonce, signature) where:

- **period** is an integer enumeration indicating the number of days in the xAU type (e.g., 1,7, and 30, for DAU, WAU, and MAU, respectively).
- **nonce** is a randomly generated 64-bit value.
- **signature** is a cryptographic signature signed by the server that generates the token (using a private key stored on the server) to signify its authenticity and guard against forged tokens. For example, the signature can be generated via RSA or ECDSA signing.

The epoch corresponding to each xAU token is defined using a fixed reference scheme. For instance, for period=1, GMT+0 can be used as the start of the daily epoch. For each request for embedded content, one or more xAU tokens can be randomly generated and cryptographically signed on the server hosting the content and then relayed to the user agent requesting the content.

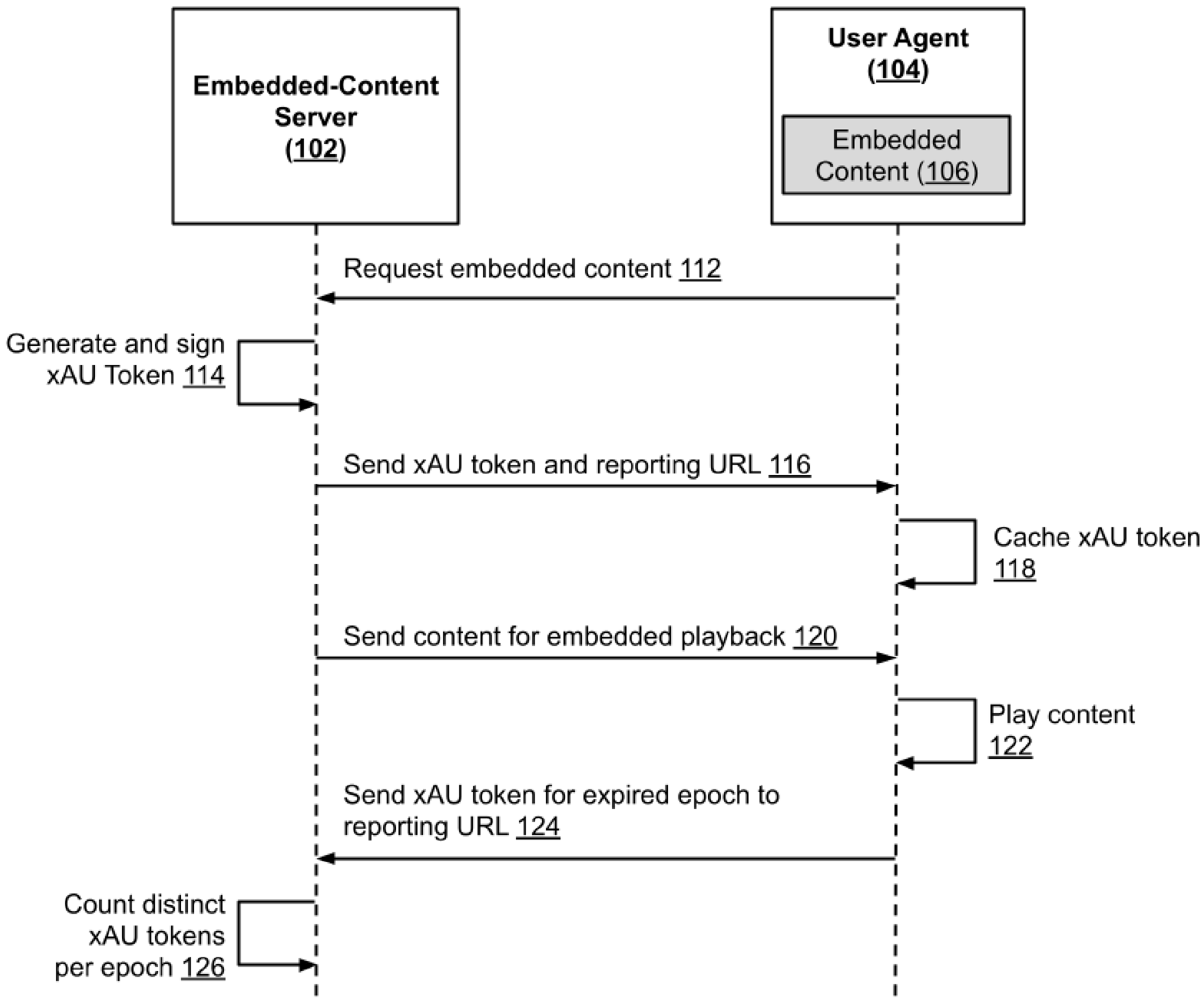

Fig. 1: Setting and counting xAU tokens for server-side computation of xAU metrics

Fig. 1 shows an example of operational implementation of the techniques described in this disclosure. A user agent (104) for an application requests playback (112) of content embedded within it (106) from the server that hosts the content (102). Upon receiving the request, a xAU token for the user agent is generated and cryptographically signed (114) by the server.

The token is provided to the user agent (116) using any suitable technique, e.g., via a special header called *set-xau-token*. In addition, the user agent is provided a reporting URL that the user agent can use later to send xAU tokens back to the server out-of-band, using HTTP

POST or another suitable method. A server may set multiple xAU tokens for a given client. However, at most one xauToken (of each type) can be sent back to the server for a given time period. The received xAU token(s) are cached to local storage on the client side (118) along with the time at which it was assigned. The embedded content is then sent to the user device (120) and content playback is provided to the user (122) as usual.

Once the epoch corresponding to the period in the xAU token expires, the corresponding xAU token is sent back to the server via the out-of-band reporting URL (124). The number of distinct xAU tokens over a given epoch can be counted on the server side (126) to compute metrics for unique active users over that epoch without needing to identify the specific users who are being counted. The described process of providing an xAU token to the user device and the device sending the token via out-of-band reporting is performed with specific user permission and does not include any user/device-specific information.

The protocol as described with reference to Fig. 1 can be implemented in a robust manner that can gracefully handle any transient issues. For example, a client is able to send the same xAU token to the reporting URL multiple times. In such cases, the nonce within the token is used to detect and remove duplicates of the same xAU token. If network or other issues cause tokens to be dropped, the loss can result in undercounting, but not overcounting, unique users in a given epoch. If a user agent receives multiple tokens for the same epoch, these can be optionally pruned at any time since only one xAU token for a given epoch needs to be cached on the client side at any given time. For example, once a DAU token is cached, other DAU tokens for the same day can be ignored. The robust operation is private by default because incorrectly generating multiple xAU tokens for the same epoch has no impact on the user. It can, however, result in incorrect server-side counts for the number of unique users during the epoch corresponding to the incorrect xAU tokens.

The techniques described in this disclosure can be implemented to obtain user engagement metrics aggregated over a given period for any type of third-party embedded content, such as videos, within any website, application, or platform. For instance, the techniques can support obtaining aggregate periodic user counts of viewers of a video embedded within a messaging app. The techniques can be deployed as a custom integration between applications and content servers. Alternatively, or in addition, the techniques can be packaged in the form of a standard implemented within web browsers. Implementation of the techniques enables reasonably accurate counts for unique active users during a given period, without requiring the use of third-party cookies.

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 content requests, tokens, 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 cookieless techniques to determine a lower bound for various xAU measures. Upon receiving a request for content, a xAU token for the user agent is generated and cryptographically signed on the server and relayed to the user agent for local caching. Each xAU token can be a tuple of the form (period, nonce, signature). Once the epoch corresponding to the period in the xAU token expires, the corresponding xAU token is sent back to the server via an out-of-band channel. The number of unique active users per epoch is obtained by counting the number of unique xAU tokens seen over the corresponding epoch. Implementation of the techniques with user permission enables reasonably accurate counts for unique active users during a given period, without requiring the use of third-party cookies.