Technical Disclosure Commons

Defensive Publications Series

January 2020

USING A CLOUD-BASED ENTERPRISE NETWORK SECURITY SYSTEM TO PROVIDE DECENTRALIZED BUT UNIFIED GENERAL DATA PROTECTION REGULATION (GDPR) CONSENT MANAGEMENT

Thomas Vegas

Anirban Karmakar

Giacomo Trifilo

USING A CLOUD-BASED ENTERPRISE NETWORK SECURITY SYSTEM TO PROVIDE DECENTRALIZED BUT UNIFIED GENERAL DATA PROTECTION REGULATION (GDPR) CONSENT MANAGEMENT

AUTHORS:

Thomas Vegas
Anirban Karmakar
Giacomo Trifilo

ABSTRACT

Techniques presented herein provide a decentralized, yet unified, General Data-Protection Regulation (GDPR) consent management platform functionality that may utilize Domain Name System level (DNS-level) interposing capabilities of a cloud-based enterprise network security system to collect detailed user privacy preferences, which can be stored locally via a user's browser. Thus, websites may not manage consent, but rather may simply process user requests with inline added consent parameters.

DETAILED DESCRIPTION

The European Union's GDPR has significantly impacted the manner in which businesses may collect, store, and manage personal information about an end user. Under Article 6 of the GDPR, collecting and using personal data from European Union (EU) and European Economic Area (EEA) citizens and residents must follow relevant notices for data processing. For this reason, publishers and website owners must obtain freely given, specific, informed, and unambiguous user consent when collecting and using cookies for advertising and/or marketing purposes.

Typically, internet websites use an existing GDPR consent management platform or implement their own to obtain such user consent. The collected user consent can be stored in a centralized database and may contain detailed information. Actual consent variables are to be mapped on-demand to a user pseudo identifier. When a cookie is stored in a client's browser, it is stored as a per-website cookie, which involves gathering user consent for each and every website that may be visited by a user. From the user perspective, a pop-up can generally be seen with the provision to specify preference and express consent.

This proposal provides techniques for providing provide a decentralized, yet unified, GDPR consent management platform functionality that may utilize DNS-level interposing capabilities of a cloud-based enterprise network security system to collect detailed user privacy preferences, which can be stored locally via a user's browser. Thus, websites may not manage consent, but rather may simply process user requests with inline added consent parameters.

During operation, the cloud-based enterprise network security system can be configured to store website hostname(s) that may utilize the functionality of a GDPR consent management server (GDPR-CMS) in order to redirect clients based on DNS request matches. The cloud-based enterprise network security system may be in a unique position to provide this service and operate as a broker to facilitate the overall consent management process, which is shown below in Figure 1.

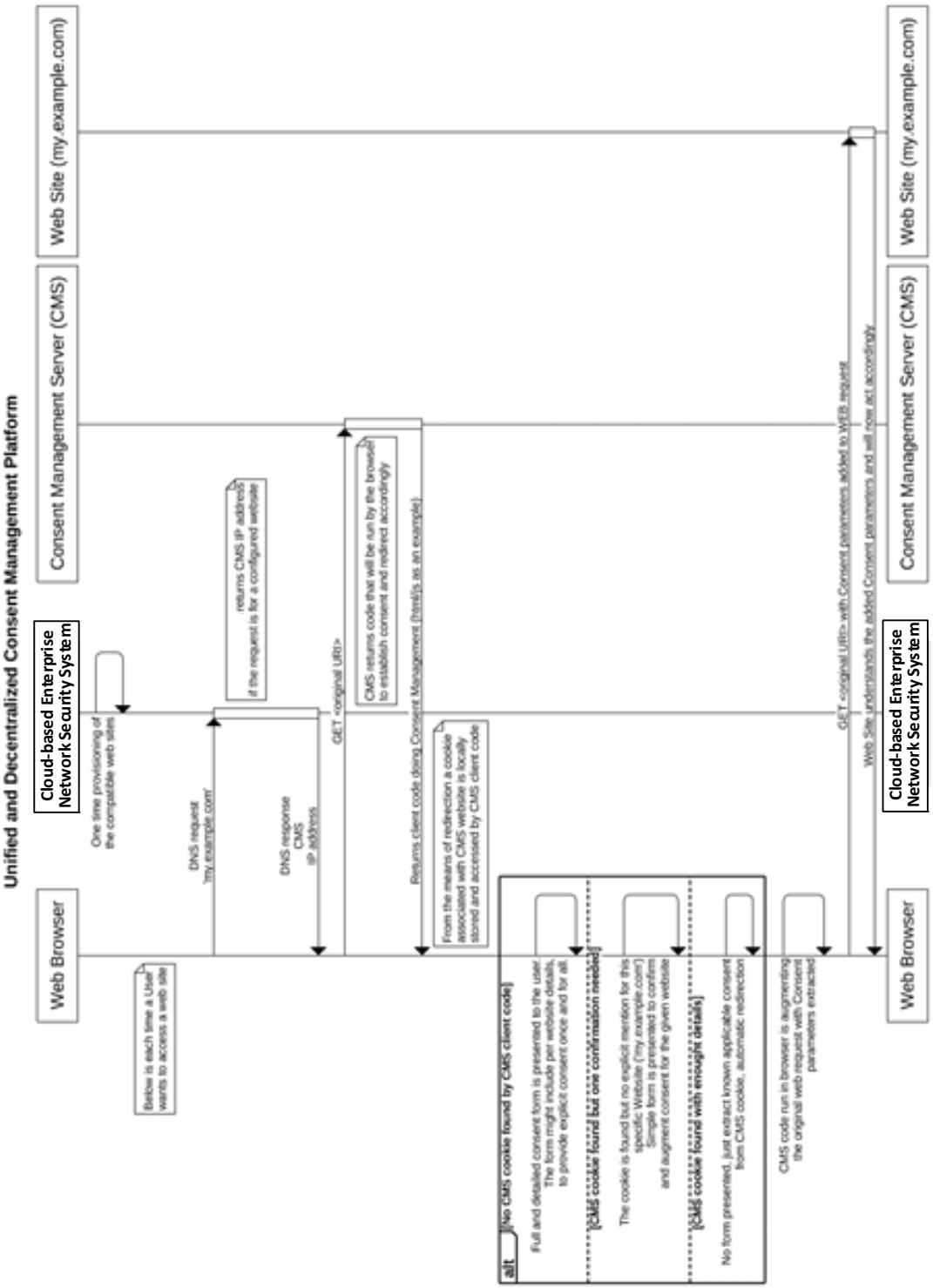
Unified and Decentralized Consent Management Platform
Web Browser
Cloud-based Enterprise Network Security System
Consent Management Server (CMS)
Web Site (my.example.com)
Below is each time a User wants to access a web site
One time provisioning of the compatible web sites
DNS request 'my.example.com'
DNS response CMS IP address
returns CMS IP address if the request is for a configured website
GET <original URI>
CMS returns code that will be run by the browser to establish consent and redirect accordingly
Returns client code doing Consent Management (html/js as an example)
From the means of redirection a cookie associated with CMS website is locally stored and accessed by CMS client code
alt
[No CMS cookie found by CMS client code]
Full and detailed consent form is presented to the user. The form might include per website details, to provide explicit consent once and for all.
[CMS cookie found but one confirmation needed]
The cookie is found but no explicit mention for this specific Website ('my.example.com') Simple form is presented to confirm and augment consent for the given website
[CMS cookie found with enought details]
No form presented, just extract known applicable consent from CMS cookie, automatic redirection
CMS code run in browser is augmenting the original web request with Consent parameters extracted
GET <original URI> with Consent parameters added to WEB request
Web Site understands the added Consent parameters and will now act accordingly

Figure 1

During an interpose phase, as illustrated in Figure 1, the cloud-based enterprise security system can, for applicable DNS queries, redirect a client (web browser) to the GDPR-CMS. The client may fetch the corresponding webpage (e.g., a HyperText Markup Language (HTML)/JavaScript (js) page) from the GDPR-CMS rather than from the originally requested server. The GDPR-CMS website may not considered to be a consent management platform (CMP) in the sense that it does not store consent data of a client. Thus, the GDPR-CMS is not subject to potential GDPR issues.

Continuing with the present operational example, the fetched code (e.g., webpages) from the GDPR-CMS can be utilized to determine whether a corresponding cookie is already stored on the client browser in which the cookie corresponds solely to the GDPR-CMS webpage. The client side web script can evaluate the presence of the cookie.

Different results from the cookie evaluation may be possible. For example, in a first phase, if the cookie is not present or does not contain the general and detailed user consent, the webpage may request the user to complete a displayed GDPR form. In one implementation, the first phase form content may be stored in the cookie of the GDPR-CMS website and may cause a redirection to the originally requested website, as discussed in further detail below.

Otherwise, if the cookie is present, the GDPR-CMS webpage script may, in a second phase, present a secondary form to the user and/or may directly redirect the browser to the originally requested website.

Various forms are noted above for the first and second phases. For the first phase, if the GDPR-CMS cookie is not present, the presented form may include very detailed requests as to what the user is consenting. Various detailed requests may include, but not be limited to, consent for specific classes of data, consent for various location capabilities/services, etc. In some implementations, the first phase form could also contain a full list of the websites (e.g., a list as configured/stored for the cloud-based enterprise network security system) along with tick boxes through which the user may provide explicit and informed, per-website consent.

In some implementations for the second phase, as noted above, an optional form may be presented to the user if, for example, the GDPR-CMS cookie is present but the user has not had an opportunity or did not previously provide explicit consent for a given

website. In one example for the second phase, a streamlined form may be presented to the user to confirm that all previously provided detailed consent is to be readily applicable to the requested website before final redirection.

For redirection, the GDPR-CMS webpage may extract from its own cookie and/or the second phase form, the applicable user consent in order to augment the original HyperText Transfer Protocol (HTTP) requests before proceeding with final redirection. Thus, GDPR-CMS logic operating on a client browser may enhance, in an inline manner, original requests with the consent applicable for a given final web site requested.

Accordingly, techniques of this proposal may eliminate operations involving a per-website cookie and/or may eliminate remote centralized platform queries in order to manage user consent in compliance with the GDPR. In some instances, a user may potentially provide, only once, a detailed preference and consent, thereby enabling the user to express privacy preferences in a consistent or unified manner. By utilizing DNS-level interposing techniques, consent gathering can be performed before accessing an originally requested website. This consent may be reused for an arbitrary number of websites, thereby enabling unified consent management.

The techniques of this proposal further provide that detailed consent can be stored locally via a user's browser rather than on a server where GDPR compliance issues might be triggered; thus, consent is decentralized yet unified. By leveraging website interposing capabilities at the DNS-level, these techniques provide a decentralized yet unified GDPR consent management platform functionality in which a cloud-based enterprise security system may not be involved in the management of GDPR user consent.

In summary, techniques of this proposal provide a decentralized, yet unified, GDPR consent management platform functionality utilizing DNS-level interposing capabilities of a cloud-based enterprise network security system in order to collect detailed user privacy preferences that can be stored locally via a user's browser. Thus, websites may not manage consent, but rather may simply process user requests with inline added consent parameters.