


This repository


Search


Pull requests


Issues

Gist










 LegalPhysics


/ ClearButton

 Watch





3

 Star





0


 Fork





2


 Code


 Issues 0

 Pull requests 0


 Wiki

 Pulse

 Graphs



 Settings

Branch: master ▾ ClearButton / Legal / ClearButtonBrief.md Find file Copy path

 linakaisey

Update ClearButtonBrief.md

d611acb on Jan 20, 2014


2 contributors  


170 lines (99 sloc) | 9.29 KB


Raw

Blame

History







ClearButton Overview and Assessment Brief

Problem

Proposed Solution

Method of Implementation

Scenarios in Context

Possible Issues

Ways to Mitigate Possible Issues

Further Considerations

Briefing

ClearButton is a service that enables individuals to know where and by whom their personal data is being stored.

Authoritative Sources: [TBD]

Problem

- While individuals are aware that their data is continually being held and transferred among corporate and government bodies, there is no centralized and easy-to-access means by which an individual may find out which entities store an individual's personal data, and what data in particular is being stored.
 - Individuals click "I Agree" to convoluted Terms of Service that give entities broad access to an individual's personal data
 - Individuals' personal data are transferred among entities who may not have agreed to the original Terms of Service governing use of the individual's data

Proposed Solution

- ClearButton is a service allowing individuals to know when and where their personal data is stored. Individuals may sign up for the service in a manner similar to signing up for the Do Not Call registry. Once signed up for the service, an individual will receive notification each time a new Information Holder (usually a corporation) comes to possess her data. The individual may consult the ClearButton Notifications Center and the individual Information Holder's website to determine what type of data is being stored, and the way the data is being used. At that point, the individual chooses how to manage her data: she may download her data to her Personal Data Store, update and correct the data, share the data with other Information Holders, or revoke permission for the Information Holder to use her data.

[the following will be split up and moved to the "steps" section:]

-
- When an individual receives a notification and wants to follow up on who now stores her data, she can click the notification provided to her to be taken to the ClearButton service. Upon login, she will be met with ClearButton Notifications Center. For each entity storing the individual’s data, the Notifications Center will detail the Information Holder name, type of data held, and time at which the data came to be held by the Information Holder. (TBD: It may also include a label indicating how the data is being used).
- From the ClearButton Notifications Center, the individual may then click through to any individual Information Holder's website. She will at this point leave the ClearButton domain and authenticate her identity on the Information Holder’s site. The Information Holder site presents what data it holds with respect to the individual. Depending on the Information Holder's preferences (and legal obligations), the Information Holder may choose to only display general metadata as to the information it stores for a particular individual, or it may provide the individual with a full description of the data that the Information Holder stores for that individual. If the Information Holder provides the individual with their full data, that data can be downloaded into the individual’s Personal Data Store. This Personal Data Store may be hosted through independent parties meeting regulatory minimums of safety and security, or it may be hosted on the ClearButton site itself.
- Once the individual holds her information in a Personal Data Store, she has the opportunity to update and correct it. Then, the individual may elect to share her corrected data with new and different Information Holders as she sees fit. Because the individual is best able to compile accurate data about herself, Information Holders will significantly prefer to use this current and correct data. Information Holders must therefore provide some sort of benefit to individuals in return for their data, in many cases the promise of better services as a result of the analytics that each individual’s data makes possible.

Method of Implementation

- ClearButton steps:

[NOTE: Below is a placeholder from the OAuth2 Brief]

(A) An Individual signs up for the ClearButton service in a manner similar to signing up for the Do Not Call registry.

(B) An individual will receive notification each time a new Information Holder (usually a corporation) comes to possess her data. Depending on the individual’s preferences, she may receive a notification whenever a new Information Holder comes to possess her data, whenever there is a significant shift in the type of data held or the type of Information Holders storing the data, or according to a schedule in line with the individual’s preferences.

(C)

(D)

(E)

(F)

Scenarios in Context

Roles

[NOTE: Below is a placeholder from the OAuth2 Brief]

- “Individual” – Civilian (in the government sense); Customer (in the business sense); Principal (in the legal sense); Resource Owner (in the technical sense). This party owns the information (stored by the Information Holder), and utilizes

the ClearButton service to understand which information is being stored.

- “Information Holder” - Corporation or government agency (in the government sense); Information Host (in the business sense); Agent (in the legal sense). This party stores the information belonging to the Rights Holder.
- “ClearButton Service" - Government agency (in the government sense); Agent (in the legal sense); [Broker](#).

General Description of Interactions

[TBD]

Specific Scenario 1

[NOTE: Below is a placeholder from the OAuth2 Brief]

Scenario 1: People:

[TBD]

Scenario 1: Interaction:

[TBD]

Illustrative Scenario 2

[TBD]

People:

[TBD]

Interaction:

[TBD]

Possible Issues

[NOTE: Below is a placeholder from the OAuth2 Brief]

- There are inherent privacy risks with protocols that allow the communicating parties to store personal data, transport personal data, or are vulnerable to other parties observing the personal data in the exchanged communications. Most Internet communications involve such risks, which can allow entities to build large databases of information that by themselves or in conjunction with other databases can identify people and their actions in invasive ways.
- Token manufacture/modification: An attacker may generate a bogustoken or modify the token contents (such as the authentication or attribute statements) of an existing token, causing the resource server to grant inappropriate access to the client. For example, an attacker may modify the token to extend the validity period; a malicious client may modify the assertion to gain access to information that they should not be able to view.
 - Token disclosure: Tokens may contain authentication and attribute statements that include sensitive information.
 - Token redirect: An attacker uses a token generated for consumption by one resource server to gain access to a different resource server that mistakenly believes the token to be for it.
 - Token replay: An attacker attempts to use a token that has already been used with that resource server in the past.

Ways to Mitigate Possible Issues

[NOTE: Below is a placeholder from the OAuth2 Brief]

- Recommending that IETF protocols define mechanisms for opportunistic encryption can increase the availability of confidentiality protection to legitimate users without significantly changing the set of tools that attackers already use to shield their traffic from being identified and their attacks from being thwarted.

- To the extent consistent with basic protocol operation and management, standards-track IETF protocols that involve transmission of personal data:
 - i. MUST minimize their use of such personal data, and
 - ii. where personal data is sent, MUST have well-defined and interoperable ways to send such data encrypted for the intended recipient(s).
- opportunistic encryption MUST be well- defined for new IETF standards track protocols. This requirement can be waived only in exceptional circumstances where the protocol's utility would be eliminated or severely diminished if opportunistic encryption were defined.
- A large range of threats can be mitigated by protecting the contents of the token by using a digital signature or a Message Authentication Code (MAC). Alternatively, a bearer token can contain a reference to authorization information, rather than encoding the information directly.
- Safeguard bearer tokens by ensuring that bearer tokens are not leaked to unintended parties,
- Validate TLS certificate chains, and always use TLS (https) when making requests with bearer tokens.
- Don't store bearer tokens in cookies:
- Issue short-lived (one hour or less) bearer tokens, particularly when issuing tokens to clients that run within a web browser or other environments where information leakage may occur
- Issue scoped bearer tokens that contain an audience restriction, scoping their use to to intended relying party or set of relying parties.
- Don't pass bearer tokens in page URLs

Further Considerations

[TBD]

