Voucher Web Metering Using Identity Management Systems

Fahad Alarifi

Abstract

Web Metering is a method to find out content and services exposure to visitors. This paper proposes a visitor centric voucher scheme that uses an identity management systems solution to incorporate a Web Metering function. The proposed scheme runs transparently to the visitor and utilises security properties available in identity management systems. On a higher level, the scheme introduces the use of authentication protocols to provide Web Metering evidence.

1: Introduction

1.1: Web Metering Description And Terminology

Web Metering is defined here as a method to measure the interactions done between the visitor and the Webserver over a specific period of time. Web Metering became a valuable measurement tool when "Online Advertising" services played an important role in the Internet. There is an enquirer party which is an entity interested in measuring the interactions between the visitor and the Webserver. The Web Metering operation can be provided by an Audit Agency or a Service Provider. More specifically, voucher Web Metering schemes are schemes where the Audit Agency or the Service Provider has to distribute vouchers to visitors (or Webservers). A voucher is a piece of information that is sent to one entity so that it can be redeemed at another entity.

A Web Metering scheme is defined here as a transparent if it executes inside or behind another action or property in the web interaction so it does not require an explicit action from visitor. That is, the scheme does not require the visitor to change browser "structure" by installing hardware or software not needed during a "normal" interaction between visitor or Webserver. Also, the scheme does not require the visitor to change his behaviour (experience) to access the Webserver by executing an explicit human action (e.g. clicking on a specific button).

We believe this visitor transparency property as an important aspect of a broader usability requirement. Usability requirement can be defined as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" [9]. So, usability in Web Metering can be defined as the extent to which a Web Metering scheme can be used to produce evidence for number of visits, with visitors satisfaction.

1.2: Threats To Web Metering

We consider here the following three threats: threats to the Web Metering scheme (which includes metering operation and metering result), threats to communication channels and

threats to visitor privacy. We define an adversary as a corrupt Webserver or any outside entity that does harm to the Web Metering scheme.

Threat to metering operation is related to a corrupt Webserver which does not follow the required Web Metering operations from its side. A corrupt Webserver is inherently motivated to increase number of visits or change some metering operations without changing number of visits. For example, a corrupt Webserver intentionally changes a webpage identifier, which is going to be recorded in the Web Metering evidence, to a different webpage that charges higher fees for advertisements. The other part of threats to the Web Metering scheme is a threat to metering result which is related to a corrupt Webserver which changes the evidence. For example, a corrupt Webserver changes the time of visit included in Web Metering evidence to match peak hour time for an advertising purpose.

Regarding threats to communication channels, we consider Dolev-Yao threat model [7] where an adversary has control over data in communication channels. In particular, the adversary can obtain data sent in the communication channels and can receive data from other entities. Using these capabilities, a successful attack can be replay, impersonation or man in the middle attack as follows. A replay attack is where an adversary captures data sent from visitor or Webserver and sends it again. In impersonation attack, an adversary creates fake data and sends it to Service Provider or Audit Agency impersonating a visitor or a Webserver. Or an adversary creates a fake request to a Webserver impersonating a valid visitor. In man in the middle attack, an adversary receives data from visitor or Webserver not intended to him and modifies it before forwarding it to the intended party.

Regarding threats to visitor privacy, a corrupt Webserver which has access to Web Metering evidences can invade visitors privacy by correlating different evidences together. Also, a corrupt Webserver can increase the requested information from the visitor side. Also, an adversary (using his capabilities described in threats to communication channels) can impersonate a valid visitor and receive private replies. Or the adversary can capture (and possibly correlate) data sent to and from the visitor.

1.3: Previous Work

The majority of Web Metering schemes is based on Secret Sharing schemes and one of the early published schemes was by Naor and Pinkas [11] which is based on Shamir Threshold Secret Sharing scheme [13]. The Webserver here needs to receive a specific number of shares (or vouchers) from visitors to be able to compute a required result using a Secret Sharing scheme as evidence of the visits. Further research continued on Naor and Pinkas work, for example, Masucci work on Web Metering schemes [2, 3]. Using such schemes necessitates the visitors to securely receive or generate required shares. For visitors receiving shares from the Audit Agency, the visitor has to be authenticated to stop an adversary from receiving the shares and consequently inflating number of visits. This entity authentication poses privacy and transparency concerns. For the case of the visitor generating the shares, the visitor has to be explicitly involved in the scheme which does not make it transparent.

Another visitor centric scheme is the use of hash chaining and digital signature for constructing non-repudiation evidences of visits as proposed by Harn and Lin in [8]. In such scheme, the visitor hashes the result of the hash chain with additional information and sends a signature of the hash to the Webserver. The scheme provides a Web Metering evidence using a signature by the visitor. To alleviate the visitor from producing a costly signature for each visit, a hash chain is proposed. That is, the Webserver uses received

signature (which reveals visitor identity) and hash values as evidence for number of visits. This visitor signature is a privacy concern and its production does not run transparently nor efficiently.

One Webserver centric Web Metering scheme uses e-coupons [10] as an attempt to map traditional advertisements models into the electronic ones. There is evidence for visits if the visitor explicitly passes the received e-coupon (or voucher) from the Webserver back to the issuing party. Such schemes can be used when a corrupt Webserver is motivated to deflate number of visits because the visitor in this scheme will forward the voucher to Audit Agency without Webserver involvement.

Another Webserver centric Web Metering scheme was proposed by Chen and Mao [4] which uses computational complexity problems including prime factorisation, presumed difficulty of computational Diffie Helmann and one way hash functions. These computational problems attempt to force the Webserver to transparently use the visitor resources in order to solve an equation and consequently provide a Web Metering evidence via the produced result. However, a corrupt Webserver can still use its processing capabilities to produce required results.

One third party centric scheme was proposed in [1] to track the visitor using HTTP proxy. Initially, the visitor is set to access a specific HTTP proxy to access the Webservers. Then, the HTTP proxy adds tracking code to the requested HTML pages that transparently track visitors actions like mouse movements and keyboard strokes.

1.4: Problem Description

Web Metering schemes are vital for measuring today's Internet visits. However, many voucher schemes lack visitor transparency and have integrity problems. Generally, the majority of Web Metering schemes approached the integrity issue without paying more attention to the transparency part. A transparency property is important in order for a scheme to be usable as there will be no actions required from the visitor side. An example of a transparent operation is tracking the visitor using HTTP proxy described in [1]. However, in the scheme setup, the visitor has to be explicitly set to access a specific third party. A more transparent scheme is the processing based scheme described in [4], provided the used resources do not affect the visitor experience. However, visitor impersonation is possible in such schemes where the computational challenge is solved by the Webserver alone.

For visitor centric voucher schemes, a straightforward non-transparent solution, where vouchers can be securely redeemed, would involve an Audit Agency generating vouchers for each visited Webserver. In such a scheme, the Audit Agency initially produces a signature on each voucher which contains the intended Webserver identifier and sends the voucher to the visitor. Then, the visitor forwards the voucher to the Webserver upon his visit so the Webserver can redeem it from Audit Agency.

In this paper, we propose a novel solution based on integrating Web Metering schemes with identity management systems. We show how to solve this problem by designing a Web Metering scheme which utilises existing vouchers to securely carry Web Metering evidence. On a higher level, this research also addresses the feasibility of hiding Web Metering feature behind another existing application. The result of this can be used to encourage the idea of "piggybacking" Web Metering function to other existing applications.

At the same time, as there are some flaws including usability of identity management systems which were pointed out in [6], our proposed solution will provide an incentive to

use identity management systems for an additional feature (Web Metering function). That is, in order for relatively smaller Webservers federate with other "stronger" Webservers, the former have to have many active visitors. And in order to have many active visitors, an identity management service has to be already in place. This usability dilemma of identity management systems can be addressed by providing the proposed Web Metering feature to Webservers.

2: Proposed Web Metering Scheme

2.1: Possible Approaches

The proposed scheme depends on protocols that are already used between the visitor and the Service Provider and have padding capability to carry Web Metering evidence transparently to the visitor. Such "flexible" ticket-based protocols are authentication protocols described in ISO/IEC 10181-2 and ISO/IEC 9798 where tickets (or vouchers) can be redesigned to carry the evidence. For example, identity management systems and Kerberos protocol fit in this category. In these authentication protocols, a third party authenticates the visitor and embeds the Web Metering evidence in a ticket which is sent to the Webserver. The addition of a Web Metering feature is possible here because ISO/IEC allows additional information to be carried in *text* fields in authentication protocols [5]. Consequently, the scope of these possible solutions is limited e.g. a casual visitor who is not using an authentication mechanism is excluded.

2.2: Proposed Solution

The proposed scheme utilises the ability to extend attribute statement in SAML messages [12]. This feature affects accuracy as well because granularity of metered data can be increased by the Webserver extending the requested attributes in the attribute statement. Regarding integrity of Web Metering, there is a cryptographic binding of assertion and IdP through a digital signature and since IdP is a trusted entity, the signature will enhance the reliability of the metering process. The IdP is regarded here as a Service Provider that provides visit evidence transparently to visitors. The following are the metering and post processing phases for the proposed Web Metering scheme using Microsoft CardSpace.

2.2.1: Metering Phase

There are five steps during visitor-Webserver interaction. In step 1, the Webserver policy, listing the requested claims inside the object tag (e.g. "trusted IdP is Yahoo!" and "visitor date of birth is required"), is downloaded into the visitor device. The visitor chooses the right Information Card and sends a token request to the relevant IdP in step 2. In step 3, the visitor is authenticated to the IdP using the stored username and password for additional visitor transparency (or X.509 certificate if available). In step 4, the IdP creates a SAML 2.0 token and lists all the requested claims and fields in the attribute statement as detailed later in post processing phase. After that, the IdP signs the token using the IdP private key. The relevant SAML fields inside the assertion are shown in Figure 1. In step 5, the visitor forwards the received token to the Webserver. The Webserver checks the signature and if valid (the token was sent by IdP and there was data integrity), the Webserver stores the token.

```
<!-- IdP identifier is included inside signed part of SAML -->

<Issuer>
IdP.com
</Issuer>

<!-- Stating registered visitor email address -->

<Subject>
<NameID Format= "urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">
visitor1@metering.com </NameID>

<!-- Specifying proof of rightful possession method -->

<SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
</Subject>

<!-- Conditions set by IdP against the Webserver re-using
previous evidences, the timeout is 1 minute -->

<Conditions NotBefore="2012-03-03T14:30:00Z"
NotOnOrAfter="2012-03-03T14:31:00Z"> </Conditions>
```

Figure 1. Web Metering information in SAML Token

2.2.2: Post Processing Phase

After the Webserver receives and stores the assertion, the Webserver constructs Web Metering evidence in a readable format which interested parties can query. There are two requested fields in an attribute statement: MeteringStatement and StatementSignature. The MeteringStatement field represents a statement from the IdP, assuring that the Webserver has been visited at a specific time. Optionally, the statement can include further details about the visitor. The StatementSignature is a signature on the Metering Statement using the IdP private key. Those two statements can be used to reveal Web Metering results. The Metering Statement can be published by the Webserver to interested parties and the Statement Signature serves as an evidence. An example of Web Metering evidence extracted at the Webserver is shown below.

- **MeteringStatement** = *IdP.com assures that a visitor over 18 years old has accessed webserver1.com at 14:29 on* 3^{rd} *of March 2012.*
- **StatementSignature**= Sig_{IdP} (MeteringStatement)
- **MeteringEvidence**= MeteringStatement | StatementSignature

We tested a simplified version of the scheme on a server with 1024 MB memory and 1.6GHz processor. This server was hosting both the Webserver and the IdP. The signature on the metering statement is produced using open source PKCS#1 (v2.1) RSA compliant library[1]. Execution time from IdP side is around 40 seconds and generated evidence is 204 characters. The inefficiency of the proposed scheme centres around the on-fly digital signature from IdP side and the dynamic text (as time is included) that has to be signed. As a result, the efficiency can be improved by signing a smaller pointer message (e.g. a number) which can be used as a signed reference at the Webserver side.

3: Conclusion

Secure Web Metering schemes are needed to address today's Internet challenges. In this paper, we proposed a Web Metering scheme by utilising an identity management system to transparently carry a Web Metering evidence. We described a scheme that uses CardSpace to incorporate a Web Metering function. The scope of other interesting Web Metering

[1]http://phpseclib.sourceforge.net

functions that could benefit from the leverage of IdPs is more than the produced Statement Signature e.g. IdPs can be Audit Agencies that publish Web Metering results.

We used an established threat model to point to the gap between previous schemes and desired ones that motivated the proposed scheme. However, we believe that visitor privacy is still a challenge especially in environments where visitors identities are linked to their visits. Future work includes researching the possibility of securely incorporating a Web Metering function to existing non-authentication protocols e.g. web syndication protocols where an embedded content provider meters the visits to the Webserver.

References

[1] R. Atterer, M. Wnuk, and A. Schmidt. Knowing the user's every move: user activity tracking for website usability evaluation and implicit interaction. In *WWW '06: Proceedings of the 15th international conference on World Wide Web*, pages 203–212, New York, NY, USA, 2006. ACM.

[2] C. Blundo, A. D. Bonis, and B. Masucci. Metering schemes with pricing. In *DISC*, pages 194–208, 2000.

[3] C. Blundo, A. D. Bonis, and B. Masucci. Bounds and constructions for metering schemes. In *Communications in Information and Systems 2002*, pages 1–28, 2002.

[4] L. Chen and W. Mao. An auditable metering scheme for web advertisement applications. In *ISC*, volume 2200 of *Lecture Notes in Computer Science*, pages 475–485. Springer, 2001.

[5] A. W. Dent and C. J. Mitchell. *User's Guide To Cryptography And Standards (Artech House Computer Security)*. Artech House, Inc., Norwood, MA, USA, 2004.

[6] R. Dhamija and L. Dusseault. The seven flaws of identity management: Usability and security challenges. *IEEE Security & Privacy*, 6(2):24–29, 2008.

[7] D. Dolev and A. C. Yao. On the security of public key protocols. Technical report, Stanford, CA, USA, 1981.

[8] H. Harn, L. Lin. A non-repudiation metering scheme. *Communications Letters, IEEE*, 37(5):486–487, 2001.

[9] International Organization for Standardization. ISO 9241-11:199. *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability*, 1998.

[10] M. Jakobsson, P. D. MacKenzie, and J. P. Stern. Secure and lightweight advertising on the web. *Comput. Netw.*, 31(11-16):1101–1109, 1999.

[11] M. Naor and B. Pinkas. Secure and efficient metering. In *EUROCRYPT*, pages 576–590, 1998.

[12] OASIS Standard Specification. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005.

[13] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.