Why HTTPS Is Not Enough – A Signature-Based Architecture for Trusted Content on the Social Web

Matthias Quasthoff, Harald Sack, Christoph Meinel
Hasso Plattner Institute,University of Potsdam
{matthias.quasthoff, harald.sack, meinel}@hpi.uni-potsdam.de

Abstract

Easy to use, interactive web applications accumulating data from heterogeneous sources represent a recent trend on the World Wide Web, referred to as the Social Web. There however, security standards are often disregarded in favor of interface design or brand new features. This prevents the new services from gaining ground in the enterprise, in medical or e-government environments. We propose the deployment of XML Digital Signatures on web content and demonstrate how an architecture enabling for various security properties would look like. The solution proposed will benefit from the research on security engineering in Service-Oriented Architectures and thus allows for an in-depth analysis on the results.

1. Introduction

Very often in the history of computing, solutions intended for a small audience only were opened to a large user base and encountered new challenges or threats. Before web sites started exchanging information without user action, every site was assumed to have a small number of editors only. Hence, it was sufficient to include the site's identity in the security measures leading to transport layer security (TLS) protection [15]. Besides the fact that this type of identity information does not prevent attackers from modifying content on the web server, the model does not fit well in situations in which the relation of a web site and the individuals creating content for that site is unclear. With the recent advent of user generated content and syndication, existing security standards for the World Wide Web (WWW) do not protect against the new security threats.

Site owners may not want to guarantee the correctness of information displayed on their site in good faith anymore. We propose protecting the integrity of the information itself, not only its transportation. To achieve this goal, we incorporate XML Signatures [10] on web content. Building completely upon existing standards, the architecture we propose is very easy to adopt and does not interfere with existing tools. Besides enabling all participants in a security-enabled infrastructure for analysis on the security properties of the information processed, even new applications can be built on top of this architecture. Among them are new filter mechanisms, authorization methods and larger security architectures suitable for environments with rigid legal constraints [14].

The paper is organized as follows. The recent technologies found on the WWW are introduced in Section 2. In Section 3, the general IT security objectives are outlined including how they are met in the existing WWW and why the Social Web introduces new challenges in that area. Our architecture guaranteeing integrity protection for the Social Web is presented in Section 4. Finally, Section 5 relates our approach to the current state of the art and Section 6 gives an outlook on future work.

2. Recent trends on the WWW

Many aspects of recent technology in the WWW are referred to as *Social Web* or more popular as *Web 2.0* [12]. We categorize the different web sites by their most notable features. Most of the web sites are content-oriented, designed for publication, storage, aggregation, and syndication of information. The majority of content on the Social Web is made of text—be it created in various blog posts, wiki pages, or comments on various types of resources like photos or videos. While text content is mainly distributed over myriad web sites, the number of web sites offering photo or video storage—usually organized as huge portals—is much smaller. The content discussed so far is usually being referred to as *user generated* or *user driven* content.

The reuse of data on remote sites is another main feature of the Social Web: aggregation and the set up of composite applications, which are also known as

mash-ups. Most sites on the Social Web syndicate their content with Really Simple Syndication (RSS) or ATOM feeds. Obviously the quality of the processed information heavily depends on the good nature of all participants.

Besides this, the Social Web features community sites offering user profiles. Those might act as identity providers using e.g. OpenID [11]. Also, many Social Web sites are realized as *Rich Internet Applications* [6], offering intuitive and desktop-like user interfaces. Finally, many web sites on the Social Web allow users to annotate resources—articles, pictures, videos, or user profiles of other participants—and are referred to as *Social Tagging Systems*.

3. Objectives of IT security

There are three superordinate security objectives: confidentiality, integrity, and availability [16]. There is no common way to support these objectives in HTML. Up to now, they are partially achieved by protecting the Hypertext Transfer Protocol (HTTP) transport with TLS tunnelling (HTTPS). However, this kind of protection is only sufficient if the information being transported is strongly related to the particular web site. This holds true e.g. for online banking or shopping sites. On the contrary, web sites aggregating information from various other sites cannot "preserve" this type of protection.

Voices in the Social Web often refer to openness, self-regulation and simplicity of technologies. This approach allows for rapid creation of new services. But to bring these services to the enterprise and other domains with strict legal constraints, it requires a trust framework for the Social Web, focusing on the new layer of abstraction originating from the WWW's development from an application itself to a platform for various applications, which actually form the Social Web.

As one of the main characteristics of the Social Web is the *user generated content* paradigm, the security objectives can hardly be achieved in a site-centric manner [2]. Instead, confidentiality, integrity and availability must be bound directly to the information created by users [14].

3.1. Confidentiality and availability

Protecting information from unauthorized disclosure contradicts the openness of the Social Web; strong links between different sites turn management of confidential information within the Social Web in a hassle.

Yet there are clear scenarios requiring authorization. Wikis e.g. require access control solutions hard to build upon traditional web sites' authorization models. Community-driven encyclopaedia sites need authorization models totally different from that of a project management sites restricted to a well-defined number of participants.

Ensuring availability of information could also be a new feature of the Social Web. Through syndication, content will be available even if the original resource is not available for any reason.

3.2. Integrity

Many Social Web sites collect and aggregate information from other sites and add value to the underlying information. These web sites are just responsible for the added value, not for the underlying content. This situation requires for a new solution regarding the protection of the integrity and authentication of information.

Hence, digital signatures, which are commonly used for integrity protection and authentication [16], have to be combined with the information found on the Social Web. Note that there are various types of entities: text, image, audio and video content, URIs pointing to other resources, and tags used for annotation of the former. In the Section 4 we propose an architecture for the protection of textual information. The architecture can then be extended to enable protection of the aforementioned several types of information.

Consider e.g. a scenario where several sites introduce content into the system, other sites subscribe to these sites to aggregate, filter, or combine information, and several end users subscribe to any of those sites. In a traditional web environment, any of the participants could introduce forged information into the system. While this might be detected in a huge community, for a smaller group of people this could be a serious threat. If on the other hand the sites introducing new content into the system protect their information using digital signatures, none of the other participants could do anything except trying to conceal large pieces of information from their audiences.

3.3. Further security objectives

There are some other security objectives for the Social Web that either can be related to one of the three aforementioned security objectives (confidentiality, availability, and integrity) [16], or to properties of identity management systems [3]. Accountability e.g. builds upon authentication and integrity.

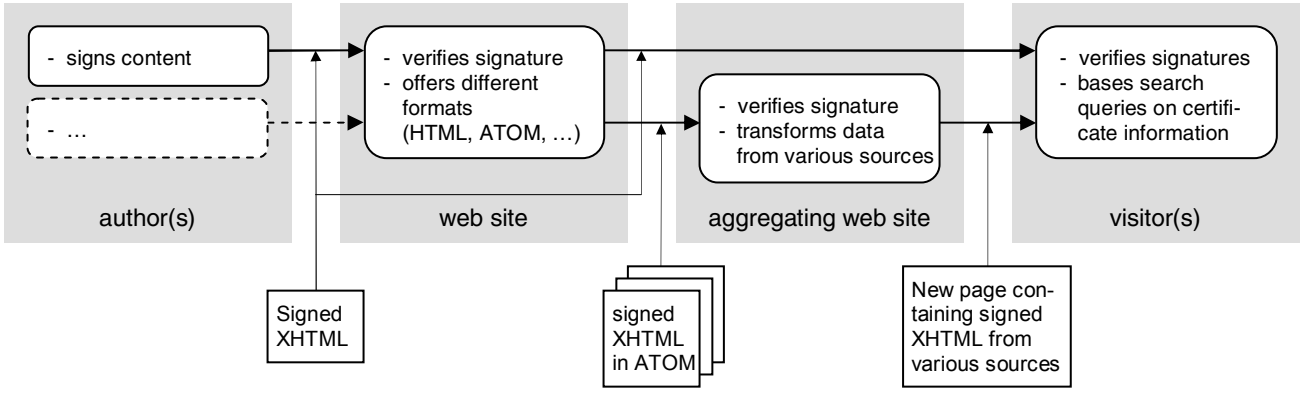

Figure 1. Signature creation and verification process in the proposed architecture

But for the democracy found in Social Web communities, anonymity is important. There already exist cryptography-based anonymization technologies for e-mail and web-browsing [5] that could be extended to support user generated content. Eventually, the security objectives that need to be mapped on the Social Web technologies will also include service protection, content revocation, and privacy policies [3].

4. A signature-based architecture for trusted content on the Social Web

As outlined in the previous section, our proposal focuses on integrity protection and authentication of text-based web content. This approach helps to understand the unique security requirements for Social Web applications. We use XML Signatures [10], which are quite common for integrity protection and authentication for structured data, to protect textual information. As most web browsers already support public key cryptography due to their TLS and Java support, our solution does not introduce much overhead to existing systems. The workflow induced by our architecture is outlined in figure 1.

4.1. Prerequisites

Accurate verification of digital signatures is not an easy task [16]. Users need to trust in the software and hardware computing hash values and comparing encrypted values. Also, data visible to the user must be displayed correctly. As an example, malicious CSS could insert or remove text from HTML documents, using ":before" and ":after" elements (fig. 2). Hence, signature verification involves serious user interaction. But also, the signing party needs to verify the information being signed.

Both Content Management Systems (CMS) and web browsers need to be extended allowing for storage, transport, and evaluation of digital signatures. CMS need the capability of accepting signed content from their authors. Also, they will have to pass on the signatures via their different interfaces like HTML, feeds and other formats for automated processing.

4.2. XML Signature for XHTML content

The architecture we are proposing uses XHTML 1.1 modules [8] to embed XML Signatures in XHTML conforming documents. That way, the architecture is also suitable for the upcoming XHTML 2.0 standard [1]. Embedding XHTML in ATOM requires all XHTML content to reside in a single element. Hence, it is wise to sign elements or content within elements. That way the signed XHTML can be published in ATOM feeds (fig. 3).

Being quite valuable information in a sender/recipient scenario, the full consequences of integrity pro-

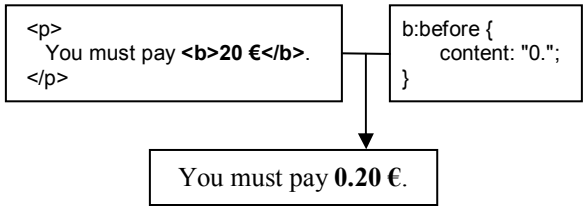

Figure 2. Forgery of web content by CSS

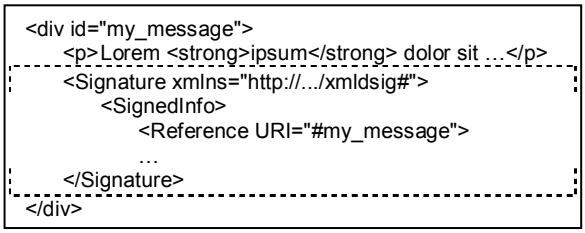

Figure 3. XML Signatures in XHTML

tection become clear in a more complex environment, where data from multiple sources are combined in a composite application. Now, data integrity can be verified by all participants for all information sources. Up to the present using HTTPS only, participants were only able to verify the information of their direct inputs.

When it comes to HTML signing, it is questionable whether to sign presentation-related information along with the HTML code. E.g., if formatting is achieved with CSS classes, class names are surely bound to a site's layout. Hence, we suggest using a transform when creating the signature that removes the `class` attributes from the HTML code. Second, as the `id` attributes are necessary for the references within the XML Signature, they need to remain the same in all HTML documents they occur. As a consequence, `id` attribute values need to be assigned in a collision-avoiding manner. Also, for each hyperlink embedded in signed HTML, the decision whether to use relative or absolute URIs depends on the further use of the given piece of HTML.

4.3. Prototype implementation

We implemented an extension for Mozilla Firefox and a plug-in for the WordPress blogging engine. The Firefox extension analyzes web pages during load and signals the presence of signed content. (fig. 4).

To verify the content, users have to click on the icon in the status bar. From a menu showing summaries of each item equipped with a signature, users chose which part to view. In a separate dialog window the representation and the signature details are displayed. By viewing the content in a separate window, no web page can pretend to contain some signed information that is not really signed.

We kept our plug-in for the WordPress blogging engine very simple at this time. It just offers the possibility to pass a block of signed XHTML along with a blog post. When the respective article is viewed on the blog's web site, the signature itself is not visible in the browser window but is evaluated by our plug-in. The signatures are created outside from WordPress using a small desktop application we implemented as a prototype.

5. Related work

The idea of signing information using public key approaches is not new. Also, very much thought went into various standards securing SOAP Web Services. Compared to that, very little has been done around the technologies on the WWW. In [13], Pöhls proposed embedding digital signatures using microformats similar to XML Signatures into HTML in order to sign parts of web sites. His approach is strongly tied to HTML by the focus on microformats. For true interoperability, a more generic approach basing on accepted standards is vital, but is not considered in detail. In contrast, our approach just builds upon mature XML Signatures. By doing so, our solution is way more open to reuse of data on different communication channels like XMLRPC or SOAP. It is even possible to mimic the signing of microformats or RDFa data with the help of transforms during the signature creation process without introducing any non-standard elements.

Besides the use case presented throughout the paper we see a strong connection to the research on security engineering in the Service Oriented Architecture. Although web-based services like mash-ups are conceded requiring much less operating expense compared to more complex SOAP-based infrastructures, much of the reduced complexity originates from avoiding any security architecture. While those promoting web-based, or ReST-based [4], services claim that HTTPS helps fulfilling sufficient security properties, we would rather refer to the indeed complex security considerations around OASIS' SOA Reference Model [7], [9]. Hence, we contribute to the security of the ReST architecture model and to the research on its security properties.

Also, our work is related to user-centric identity management solutions [3]. User centricity led to new approaches on identity management [11]. Our work strongly relies on the development in the area of Public Key Infrastructures (PKI). Furthermore, it reveals the actual impact a working wide-spread identity management will have: The effect will be much more than just convenience as stated by different authors but instead will bring confidence, reliability and availability to various scenarios.

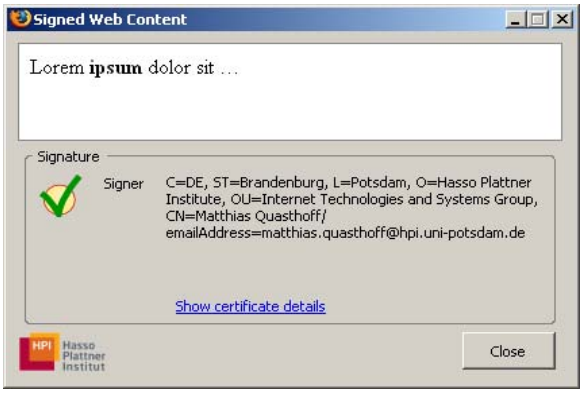

Figure 4. A Firefox plug-in for XML Signature validation

6. Conclusion and further research

We have analyzed security requirements for web applications and identified the limitations of the security measures taken in today's web applications. As a simple yet standardized and easy-to-adopt solution for decentralized scenarios, we proposed the use of XML Signature in order to protect arbitrary pieces of XHTML content. Our implementation of a very simple yet sufficient plug-in for the WordPress blogging engine and for the Mozilla Firefox web browser analyzing and displaying signed content embedded in web pages showcases the feasibility and efficiency of our approach. Keeping the desire for simple solutions in mind, we are convinced that a security architecture based on existing standards will allow for new opportunities and even new business models tapping the full potential of fast-paced interconnected web applications.

We have not yet defined how other data types like tags—which don't have a canonical representation—will be integrated in our solution. So, one goal is definitely to capture the whole world of web-based applications and integrate them in a homogenous yet simple solution. In parallel, we are also looking on policy and best practice aspects. Policies will become necessary if web sites want to connect the use of their content to some kind of authorization. Finally, an extension to the remaining security objectives with all the influence on the infrastructure is the main stream of research in our project. Additional standardized technologies and existing as well as upcoming identity management solutions will form parts of further research. For all of those aspects there is one clear constraint: any solution on web security should pick up the easy feel of the Social Web sites, and thus allow for quick and mostly invisible adoption of security-enhancing technologies in that area.

7. References

[1] J. Axelsson, M. Birbeck, M. Dubinko, B. Epperson, M. Ishikawa, S. McCarron, A. Navarro, S. Pemberton (Eds.), "XHTML 2.0", http://www.w3.org/TR/xhtml2/, July 26, 2006.

[2] H. Beyer, K. Holtzblatt, "Contextual Design: Defining Customer-Centered Systems", Morgan Kaufmann, 1998.

[3] A. Bhargav-Spantzel, J. Camenisch, T. Gross, D. Sommer, "User Centricity: A Taxonomy and Open Issues", *DIM'06*, November 3, 2006, Alexandria, Virginia, USA.

[4] R. T. Fielding, "Architectural Styles and the Design of Network-based Software Architectures", *Ph.D. Thesis*, University of California, Irvine, Irvine, California, 2000.

[5] D. M. Goldschlag, M. G. Reed, P. F. Syverson, "Onion Routing", *Communications of the ACM*, Vol. 42, No. 2, February 1999, 39-41.

[6] C. Loosley, "Rich Internet Applications: Design, Measurement, and Management Challenges", Keynote Systems, 2006.

[7] C. M. MacKenzie, K. Laskey, F. McCabe, P. F. Brown, R. Metz (Eds.), "Reference Model for Service Oriented Architecture 1.0", OASIS, August 2, 2006.

[8] S. McCarron, M. Ishikawa (Eds.), "XHTML 1.1 – Module-based XHTML – Second Edition", http://www.w3.org/TR/xhtml11/, February 16, 2007.

[9] M. Menzel, "Security Engineering in Service Oriented Architectures", *Proc. of the Spring 2007 Workshop of the HPI Research School on Service-Oriented Systems Engineering*, 2007.

[10] K. Miyauchi, "XML Signature/Encryption – the Basis of Web Service Security", *NEC Journal of Advanced Technology, Vol. 2, No. 1*, NEC Corporation, Tokyo, 2005, pp. 35-39.

[11] "OpenID: an actually distributed identity system", http://openid.net/, 2007.

[12] T. O'Reilly, "What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software", http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html, September 30, 2005.

[13] H. C. Pöhls, "Authenticity and Revocation of Web Content using Signed Microformats and PKI", *Technical Report*, University of Hamburg: Computer Science Department, Hamburg, February 5, 2007.

[14] M. Quasthoff, C. Meinel, "User Centricity in Healthcare Infrastructures", *Proc. of the SIG on Biometrics and Electronic Signatures*, Darmstadt, 2007.

[15] T. Dierks, E. Rescorla (Eds.), "RFC 4346 - The transport layer security (TLS) protocol, Version 1.1", http://www.ietf.org/rfc/rfc4346.txt, April, 2006.

[16] B. Schneier, "Applied Cryptography. Second Edition", John Wiley & Sons, 1996.