Authenticity: The missing link in the social semantic web

Bastian Braun Henrich C. Pöhls
University of Passau, Institute of IT-Security and Security Law (ISL), ITSEC
Innstrasse 43, D-94032 Passau, Germany
bastian.braun|henrich.poehls@uni-passau.de

Abstract: Especially data on social network services (SNS) is linked to online personas. Our analysis has shown that no reliably solution for origin authentication is in widespread use. We will show the risk and threats resulting from this gap and analyse and contrast several approaches from the live web and research papers.

1 Introduction

The number of social network services (SNS), like MySpace, Facebook, or XING, and their number of users, forming their "digital footprint" [MFSV07] by submitting personal data is increasing. In the best case you yourself created the profile, the social-links, and all the data stored there about you. In the best case you know that the data must be regarded as freely-accessible data, can not be deleted [fac07], and has privacy issues. In this paper we concentrate on a different, often overlooked, problem: **Missing authenticity** due to missing origin authentication.

The threat: "Unwanted" profile data and social-links, or more general: Any data that is linkable to your digital persona can negatively influence your digital reputation, and thus have a negative impact on your real life. The threat lies not inherently within one SNS, but comes from services accumulating publicly available information. They offer meta-searches across various sources (including SNS) and have no way to distinguish between fake, wrong data and your version of the data. Already emerged aggregation services like ZoomInfo.com, Spock.com, Yasni.de, or Pipl.com follow a greedy matching strategy: They try to relate all the data they find linked to a name. "Unwanted" data can be associated to an online persona either by self-upload, error, or malicious intent. Most confirmed real life impacts [Jus07] fall into the self-upload category. An example for an error: flickr's cache [fli07] displayed other peoples', sometimes indecent, photographs in a user's flickr portfolio. Arguing for more privacy awareness or minimize the data submitted to these services, does not count for malicious attacks. Creating false profiles containing inappropriate content in order to harm people was recently described [vS08]. The risk is now the opposite: Not having a profile in a SNS yourself, as someone else can take your name.

To solve this problem we propose to bind the data to an identity token. So given a set of data items, a verifier can automatically separate this set into partitions distinguished by the identity token each data item was bound to. Each identity token corresponds to a digital persona. It shall be computationally infeasible to bind content to an identity token without

the consent of the token owner. Thus, solving more than name clashes, but offer authenticity. In this paper we will define the properties and requirements a service needs, to provide this authenticity for web data and SNS. We then analyse and compare established standards, existing services offered on today's web, and academic proposals. The paper's main contributions are the dissection of the problem, resulting in the list of desired properties, and the analysis of the existing web's landscape and solutions proposed in the literature.

2 Missing authenticity in social networks: Problems and Risks

Comparing the data publication process in social networks with normal web pages we note the following subtle differences: First, the data creator is different from the site owner where data is published. So we can not infer authenticity information from the publishing resource. Secondly, the SNS profile URI's are not controlled by a trusted authority as are domain names. With no regulation anybody can register any name in any SNS. Third, inbound links often have an impact in SNS, but inbound linking has never been controllable. For example: FOAF [com07] only recommends reciprocal links, but Google's Social Graph API [Goo] indicates relationships even if the link is not reciprocal. Finally, a general problem is that data assigned to a single online persona can be spread across several SNSs using different identifiers. Vice versa, equal SNSs identifiers need not represent the same online persona.

If SNS either neglect or only partially cover origin authentication, the missing authentication can be a risk for an online persona's reputation, especially if the data gets aggregated.

3 Properties for Origin Authentication

To establish authenticity an identifier for the origin, named *authorID*, is bound to the authored data (*bond*). To cater for the situation where only fragments of the bound data are present we need to allow for fragmentation. Fragmentation allows for loosely coupled data-driven applications, but can be neglected at first. Desired properties:

- **globally unique**: Collisions shall be hard to compute deliberately.
- **cross-domain**: Allow linkage of data from the same origin across SNSs, for interoperability and transfer of data.
- **pseudonymity**: AuthorID contains no re-identifiable personal information (i.e. email). Unlinkable authorIDs allow to separate personal from professional activities.
- **revertible pseudonymity**: The author can choose to reveal his pseudonym, after bond generation, by publishing re-identifiable data bound to the same authorID.

This list is not exhaustive, but covers all aspects found in identity management systems [ULD04]. From the listed properties other complex properties can be build, i.e. anonymity can be achieved by generating a new pseudonym for each content. Next we turn to the desired properties for the *bond* between authorID and the author's data:

- **data dependent**: Bind to the data itself; independent of the data's location
- **author generated**: Authors generate bonds, also across different domains; possible delegation to third-parties
- **independently verifiable by third parties**: Third-party verifier can automatically verify the bond with as little additional information as possible; verification process is independent from the party publishing the data (i.e. the SNS)
- **off-line verification**: Only to incorporate potential changes in trust relations after the bond generation the verification process requires interaction with a trusted third party; TTP defined by the author to be trusted to support up-to-date verification information
- *Optional* **work on fragmented data**: Bond remains verifiable valid when data bound to one authorID if data is split according to a **policy set forward by the author**; *policy compliant data processing* does not invalidate the bond
- *Optional* **time stamp**: timing information of bond generation by trusted third party
- *Optional* **bond lifetime management**: Authors flag bonds as invalid, stored in a central place; Additionally: state the bond's end-of-lifetime on bond creation

The last three properties hand authors some control over the distributed data. Today data, once published, will be circulating the net forever. There is no way of managing or indicating outdated data. Thus, the value of data is decreased, as there is no way to automatically judge if the author still committed to the data, its accuracy.

4 Analysis of Existing Services for Web Content

Among the analysed are: MicroID.org, ClaimID.com, FindMeOn.com, RegisteredCommons.org (RC), Numly.com, and DulyNoted.co.uk. We also added our own approach ConCert [PÖ8] to the comparison, the details are shown in Table 1 The seven services can be distinguished by several factors: The first three are used for author attribution of URIs only: MicroID and ClaimID are based on reciprocal link, only FindMeOn uses digital signatures. They neglect the data and bind only the data's URIs. The following (RC, Numly, and DulyNoted) store a data backup on their server (different URI) together with the authorID. ConCert directly binds the data independently from their URI using digital signatures.

When it comes to verification reciprocal links work quite well for SNS profiles, but break once data is moved away from the location specified at bond time. Reciprocal links also need manual maintenance. MicroID, FindMeOn and ConCert employ cryptographic primitives, generally allowing third parties to verify the bond without reciprocal links. In the case of MicroID the verifier needs to know the author's URI (i.e. his email). A MicroID is only as trusted as the site that embedded it, as it shall always be generated by the site and stripped from user generated content. So who ever knows your email address is able to verify that you used the same email address with the site that embedded the MicroID. FindMeOn and ConCert digitally sign the bond. They can offer pseudonymity and revertible pseudonymity through the properties inherited from digital signatures. Only ConCert uses only the public key as authorID and is independently verifiable.

Aggregation services (AS) can offer a unique value if they can re-assure the viewer that

	authorID value bound to content	authorID as visible	cross domain linkage	content bound to authorID	content identifier
MicroID	author provided URI	hash*	no	service's URI	hash*
ClaimID	service's profile URI	URI	yes (authorID)	content's URI	URI
FindeMeOn+	service's profile URI	author's public key++	yes (authorID)	content's URI	URL+
Registered Commons (RC)	author provided information	not visible	indirectly (profile page)	stored content (no explicit back-link)	hash (MD5)
Numly	author provided information	not visible	indirectly (profile page)	stored content (explicit back-link)	number (20 digit)
DulyNoted	author provided information	not visible	not possible	stored content	number (>8 digit)
ConCert	author's public key	author's public key++	yes (authorID)	content	hash

	bond generation	third party bond verification	timestamp
MicroID	author or issuer	limited (knowledge of authorID needed)	no
ClaimID	author & issuer**	yes (reziprocal link check)	no
FindeMeOn	author++ or author & issuer**	yes (signature verification)	no
Registered Commons (RC)	issuer	indirectly (search for hash through RC website)	yes
Numly	issuer	indirectly (text-only version at Numly)	yes
DulyNoted	issuer	no, only upon author request	yes
ConCert	author	yes (signature and policy verification)	no

*) MicroID combines two URIs by hashing: hash = $h(h(\text{author's URI}) + h(\text{content's URI}))$
**) Reciprocal link placed on issuer's profile page (by issuer) and data's page (placed by author).
+) Only Web URLs considered here; FindMeOn allows email addresses, screen- or real-names to be bound.
++) Bond is digitally signed. Signature can be generated by user or service. Public key can be used as authorID

Tabelle 1: Comparison of existing web services

all aggregated data belongs to the same authorID. In order to do this, viewers need the ability to verify aggregated, re-published data items. Thus, ASs need a visible authorID: RC, Numly and DulyNoted fail to offer this. Except for ConCert none offers verification of origin only based on the data, nor allows fragments to be verified individually. Finally, let us look at the possibility to manage the bond over its lifetime: The services working with reciprocal links allow to remove those links on the author's anchor site. But as mentioned before, each desired re-publication would require a link, so new fragments will have invalid reciprocal links. This makes it hard to automatically differentiate if a bond was revoked or if it is just a new fragment. FindMeOn's signature inherited some properties of digital signatures including certificate revocation. But the author's public-key used for signing all bonds can be revoked. Thus, revoking all bonds ever generated. ConCert offers to revoke just one bond at a time. Registered Commons offers no bond revocation at all. DulyNoted could be instructed by the author to delete data, but allows no direct third-party verification anyway.

5 Analysis of Standards and Academic Proposals

The obvious standard to look at is HTTPS. But HTTPS tunnels have a different objective: provide a secure tunnel between two endpoints. Though they offer end point authentication (e.g. server authentication), they can not retain the authentication property on data after the

tunnel has been disconnected. Chi and Wu [CW02] presented an extension to the HTTP response header allowing to embed a precomputed digital signature of the content. By using digital signatures without encryption the server's authenticity information can be retained. Their approach focussed on caching of protected content and is tight to the way web servers serve traffic. It does not allow to combine signed data from different authors or sources within one web page, as an aggregator would need.

Secondly, the data could be represented in XML. Standardized methods exist to digitally sign XML [ERS02], and to transport the signature within XML. XML signed data in SNS profiles can solve the problem. It is possible to build an XML signature that is still valid when only certain fragments are kept intact. This involves the use of XPath [W3C07] transforms [BHR03] inside the XML-DSIG. But this results in complicated XML statements and heavily replicates data inside the XPath transform statement [1]. For ConCert [PÖ8] we showed how to include signature values into native (X)HTML as Microformat annotation. Quasthoff et al. [QSM07] took our proposed method [PÖ7] of embedding the content's digital signature and showed how to verify signed XHTML parts embedded in web content using XML-DSIG. They used standard XML-DSIG without XPath transforms and thus only allow complete data to be verified, whilst ConCert is designed to allow also the verification of policy compliant fragmented data.

Work done by Bertino et al. [EBE+04] and by Carminati et al. [CFB05] show how XML data can be protected without trustworthy publishers. Their approach additionally employs confidentiality protection through encryption. They allow, by the use of Merkle hash trees [Mer79], the verification of fragments. Users issue so called "queries" to the publisher, possibly resulting in data fragments to be returned. Their approach lacks the author's ability to control which combination of data fragments the processor can be omitted while retaining a positive verification outcome. Lifetime management is generally discussed by Mayer-Schoenberger [MS07], but not further considered in the above approaches.

6 Conclusion

From our analysis we see an ongoing trend to offer solutions providing authenticity. Reciprocal links generally work for SNS users, but have the burden of management. Automatically verifiable approaches are preferable. Allowing to authenticate by URI is already helpful and works well for complete SNS profile pages. But the moment an aggregator republishes data (fragmented or not), URI based solutions loose their verifiable authenticity. The protection of non fragmented data as offered by some solutions is a good start in the right direction. With data portability starting to gain importance in the area of SNS [Dat07], we but strongly recommend to look into ways to protect the data after fragmentation and re-publication. Verification of deeper citations levels giving assurance for the data's origin adds transparency and value. Limitation and control of data aggregation is the preferred to access control restrictions especially in the area of SNS.

In future offering control and authenticity mechanisms to user's data can be a unique sel-

[1] Example left out for brevity

ling proposition for SNS and data aggregators. We hope to see services preserving this authenticity for their user's data through using secure mechanisms.

Literatur

[BHR03] J. Boyer, M. Hughes und J. Reagle. XML-Sig XPath Filter 2.0. RFC 3653, Dec. 2003.

[CFB05] B. Carminati, E. Ferrari und E. Bertino. Securing XML data in third-party distribution systems. In *Proceedings of 14th ACM CIKM*, Seiten 99–106, 2005.

[com07] FOAF community. FOAF Vocabulary Specification 0.91. `xmlns.com/foaf/spec/`, Nov. 2007.

[CW02] C.-H. Chi und Y. Wu. An XML-Based Data Integrity Service Model for Web Intermediaries. In *Workshop on Web Content Caching and Distribution (WCW)*, 2002.

[Dat07] Dataportability. `dataportability.org`, Nov. 2007.

[EBE+04] E.Bertino, B.Carminati, E.Ferrari, B.Thuraisingham und A.Gupta. Selective and Authentic Third-Party Distribution of XML Documents. *IEEE TKDE*, 16:1263–1278, 2004.

[ERS02] Eastlake, Reagle und Solo. XML-Signature Syntax and Processing. W3C Recommendation. `www.w3.org/TR/xmldsig-core/`, Feb. 2002.

[fac07] facebook. Policy. `www.facebook.com/policy.php`, Dec. 2007.

[fli07] flickr. Phantom Photos – My photos have been replaced with those of another. `flickr.com/help/forum/33657/`, Feb. 2007.

[Goo] Google. Social Graph API Documentation. `code.google.com/apis/socialgraph/docs/api.html`. last accessed: Jan. 2008.

[Jus07] Justia Incorporated. SNYDER v. MILLERSVILLE UNIVERSITY et al. `news.justia.com/cases/featured/pennsylvania/paedce/2:2007cv01660/228127/`, Apr. 2007.

[Mer79] R. Merkle. Secrecy, Authentication, and Public Key Systems. Diss., Stanford, 1979.

[MFSV07] M. Madden, S. Fox, A. Smith und J. Vitak. PEW Internet & American Life Project Report: Digital Footprints. `www.pewinternet.org/pdfs/PIP_Digital_Footprints.pdf`, Dec. 2007.

[MS07] V. Mayer-Schönberger. Das Internet erinnert sich ewig. `http://www.sueddeutsche.de/computer/artikel/189/127981`, Aug. 2007.

[PÖ7] Henrich C. Pöhls. Authenticity and Revocation of Web Content using Signed Microformats and PKI. Bericht B-276-07, University of Hamburg, Department of Informatics, Hamburg, Germany, February 2007.

[PÖ8] H. C. Pöhls. ConCert: Content Revocation using Certificates. In Jörg Siekmann, Hrsg., *Sicherheit 2008*, Jgg. 128 of *GI-Edition Lecture Notes in Informatics (LNI)*, Seiten 149–162, Saarbrücken, Germany, April 2008. GI.

[QSM07] M. Quasthoff, H. Sack und Ch. Meinel. Why HTTPS is Not Enough – A Signature-Based Architecture for Trusted Content on the Social Web. In *IEEE / WIC /ACM Int. Conf. on Web Intelligence*, 2007.

[ULD04] ULD Schleswig-Holstein. Identity Management Systems (IMS): Identification and Comparison Study. `www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf`, June 2004.

[vS08] Sylvan von Stuppe. Social Networking Threat. `sylvanvonstuppe.blogspot.com/2008/01/social-networking-threat-xpfa.html`, Jan. 2008.

[W3C07] W3C. XML Path Language (XPath) v2.0. `www.w3.org/TR/xpath20`, Jan. 2007.