Grouping Verifiable Content for Selective Disclosure

Laurence Bull[1], David McG. Squire[1], Jan Newmarch[2], and Yuliang Zheng[3]

[1] School of Computer Science and Software Engineering,
Monash University, Caulfield East 3145, Australia
{Laurence.Bull, David.Squire}@infotech.monash.edu.au
[2] School of Network Computing,
Monash University, Frankston 3199, Australia
Jan.Newmarch@infotech.monash.edu.au
[3] Department of Software and Information Systems,
University of North Carolina at Charlotte, Charlotte, NC 28223, USA
yzheng@uncc.edu

Abstract. This paper addresses the issue of selective disclosure of verifiable content. It extends previous work relating to Content Extraction Signatures [21] to implement a more complex structure that encodes a richer, more flexible fragment extraction policy, which includes fragment grouping. The new extraction policy enables the signer to specify both optional and mandatory fragment associations (or groupings) for verifying extracted content.

Keywords: Selective content disclosure, content extraction signatures, privacy-enhancing signatures, fragment grouping.

1 Introduction

As the pervasiveness of the Internet grows, so does electronic society. Traditional communication and commerce based on paper documents is being superseded by electronic processes and content.

Documents are merely containers. Traditionally, documents have been viewed and handled as coherent collections of semantically grouped information. More specifically, there are types of documents that represent merely a container of facts, such as a contract, an academic transcript, a non-fiction book, or an encyclopedia. It is with such documents that our main focus lies.

Consider the retrieval and exchange of individual pieces of information contained within a given document, rather than the handling of the whole document. Underlying this activity is the notion that the document itself is not the most important thing to the holder in such cases. The value, rather, lies with the document content, i.e. its constituent pieces of information. Furthermore, this concept is not constrained to small containers of information such as letters, contracts, bank statements or receipts. It is also scalable to very large collections such as books or encyclopedias.

There are everyday situations where, for reasons of relevance or privacy, one wants to disclose only certain parts of a document. Under the current digital signature regime, however, the entire document is signed, thereby forcing the document holder to disclose all of its contents to a third party for the signature to be verifiable.

Stewart Baker, chief counsel for America's National Security Agency (NSA), has warned of the threats to our privacy in an electronic society [1]:

> The biggest threats to our privacy in a digital world come not from what we keep secret but from what we reveal willingly. We lose privacy in a digital world because it becomes cheap and easy to collate and transmit data... Restricting these invasions of privacy is a challenge, but it isn't a job for encryption. Encryption can't protect you from the misuse of data you surrendered willingly.

Blakley claims that digital signatures are quite different from their ink-based predecessors, and suggests that we should "look more closely at every way in which digital signatures differ" so that we may fully realise their worth [5].

We agree with these views. In this paper we propose a means of reducing the erosion of a document holder's privacy in real-world electronic interactions. This is achieved through the use of Content Extraction Signatures (CES) [21], and the further development of a fragment extraction policy that enables the document holder to selectively disclose verifiable content.

1.1 Background

In the physical world commerce is conducted through interactions and transactions. The standard digital signature is well-suited to point-to-point interactions, since party A simply signs the content they wish to send to party B. Not all instances of commerce, however, should be characterised as merely a series of point-to-point interactions. More properly, many instances are multipoint, or multiparty, interactions where information flows from the information signer to the document holder and then to the information consumer(s) as illustrated in Fig. 1. Party A (Alice) produces and signs a document, party B (Bob) receives the document and forwards selected parts thereof to party C (Carol), or party D (Don), who verifies the information.

1.2 Contents of this Paper

After establishing the type of interaction of interest in Section 1, Section 2 introduces two problems relating to electronic multiparty interactions. Section 3 covers related work from a policy and technical perspective. In Section 4, an approach using the current digital signature is discussed to illustrate its limitations and the erosion of the document holder's privacy with its use in these types of interactions. A solution using privacy-enhancing Content Extraction Signatures is then discussed to illustrate their use in multiparty interactions.

Fig. 1. A Multiparty interaction.

2 The Problems

The elegant concept of public-key cryptosystems [12] and their implementation [20] enabled a content-dependent digital signature to be created for electronic documents. Beth, Frisch and Simmons [4] suggest this changed the information security field and its primary focus from secrecy alone to include broader notions of authentication, identification and integrity verification. With the steady rollout of Public Key Infrastructure (PKI), public, corporate and governmental acceptance of, and confidence in, digital signatures has steadily grown.

Whilst digital signatures are becoming widely accepted, there is privacy erosion attendant on their use in some common multiparty interactions. In other multiparty interactions, the coarse granularity of information signing results in higher and unnecessary usage of bandwidth.

2.1 Granularity versus Privacy

This can be illustrated with a commonplace online transaction where Bob wants to purchase online an academic version of software from the Computer Corporation. Computer Corp. requires proof that Bob is a current student. Bob thus sends his electronic student identification document that has been issued and signed by Ace University. Although he need supply only his name and expiry date to establish that he is a current student, he is forced to reveal all of the other information contained in his student identification document which might include date of birth, address, course enrolment, his photograph, etc.

Ace University signs the information that it sends to Bob, thereby requiring Bob to disclose *all* of this information to Computer Corp.: otherwise it will fail verification. This occurs even if only part of the information is required for the interaction and Bob does not want to reveal all of the information.

Ideally, the information holder should be free to disclose only the minimum information required for the interaction. Bob should be able to disclose only his name, student number and expiry date in support of this transaction. However, this must also be in accordance with the signer's expectations of reasonable use of the document's content. Bob's privacy in this transaction is eroded as the document content is signed with a granularity that is too large for this particular transaction. This demonstrates the tension between verifiable information granularity and the information holder's privacy, as illustrated below in Fig. 3(a).

Our goal is to enhance the document holders' privacy in multiparty interactions, moving from coarser content granularity towards finer granularity.

2.2 Granularity versus Bandwidth

The granularity of signed information in multiparty interactions does not only affect privacy; it also causes unnecessary bandwidth usage. Consider Bob, a document holder, who wants to pass a single item of verifiable information to Carol. Instead of being able to pass this single item of information, Bob is forced to furnish the entire document, which could be significantly greater in size than the single item.

Fig. 2. Example of electronic publishing which includes verifiable content.

To illustrate such a scenario, which is not a privacy issue but one of information relevance, consider an electronically published article, in which some aspect of an interview with the Prime Minister (PM) is reported. As depicted in Fig. 2, the PM's office issues a transcript of the interview involving the PM, which has been signed using the standard digital signature.

The publisher would like to quote only the PM's response to a particular question as there are tight constraints on article size and it is neither appropriate, nor possible, to include the entire transcript of the interview. It is desirable for the reader to be able to verify the quoted content in the article from the signed transcript as it would avoid problems of misinterpretation and misquoting.

If the interview transcript is signed using the standard digital signature, this scenario is not possible. The problem is that the standard digital signature requires all of the signed information to be present: otherwise it will fail verification.

This example illustrates the tension that exists between verifiable content granularity and bandwidth, as illustrated in Fig. 3(b). This tension is likely to arise in many other scenarios as the Internet burgeons. A further goal of this work is to reduce the signed content granularity and move towards reduced bandwidth.

(a) With information privacy (b) With bandwidth usage

Fig. 3. Tensions with verifiable content granularity

2.3 Selective Content Disclosure Abuse

The potential for abuse accompanies the ability to disclose verifiable information contained in a document more selectively. For example, using the above scenario, to avoid the PM's responses being quoted out of context, it is desirable that the question and the response be linked so that the response is always preceded by the corresponding question. Hence there is a requirement that the information signer be able to exert some control over what verifiable content can be selectively disclosed by the document holder. Conceivably, the document signer would want to be able to specify which fragments: may be extracted in isolation, be extracted only when accompanied by other specified fragments, and never be extracted (i.e. can only ever be provided with the entire document).

3 Related Work

3.1 Policy Initiatives

The ever-increasing adoption of the Internet by government, business and the community has added to existing concerns over privacy arising from the widespread use of information technology. Governments in countries such as Australia have responded by establishing privacy commissioners to develop and administer privacy laws, privacy policies and standards with which organisations must comply [16]. Privacy rights are often expressed in the form of Privacy Principles. In Australia there are ten, which are based on the Organisation for Economic Cooperation and Development (OECD) guidelines and called the National Privacy Principles (NPP) [15]. Australia also has a Privacy Commissioner [10] who is charged with many functions and responsibilities with respect to the Privacy Act.

Whilst the policies and legal framework initiatives are welcome, they are not a panacea. They simply provide a framework within which organisations under their jurisdiction must operate or face sanctions. What about organisations that operate beyond their jurisdictions? Consider Internet-based gambling. Although it is now illegal in many countries, it has simply moved offshore and out of the respective country's jurisdiction.

These initiatives will not prevent breaches of privacy, as illustrated recently in an incident when customer credit card details were disclosed outside of a company and were subsequently fraudulently used. After an investigation, the Federal Privacy Commissioner stated that "It is important to note that addressing the privacy risks identified would not necessarily prevent a breach such as the one that occurred ..." [17]

Once private information is released, you cannot recall it. In the above example, all the credit cards had to be cancelled and new ones issued. Perhaps not a particularly great inconvenience—what, however, if the privacy breach involved much more sensitive information such as a digital identity, or private key?

Policies alone cannot ensure privacy. There needs to be technical support for privacy and it needs to be put back into the hands of the people to allow them a role in their own privacy.

3.2 The XML Signature

The XML-Signature (XMLsig) specification [2], also from the W3C, defines a scheme for creating digital signatures that can be applied to digital content, or data objects, which may be within the same XML document as the signature, or located externally in other documents on various sites across the web. The XMLsig enables the signer to sign anything that can be referenced by a URI, along with any transforms of the information, so that other users can verify the signature. In essence, the thrust of XMLsig is to enable a signer to efficiently sign multiple objects that may be located on physically different servers and to enable a verifier to verify the available objects even though the entire set of signed objects may not be available.

Whilst the basic XMLsig's functionality is similar to our first CES scheme, *CommitVector* [21, §4.1], it is not designed to provide the CES *privacy* security for blinded content nor does it allow the signer to specify an extraction policy. Nonetheless, it has been shown that the functionality of the XMLsig can be extended to include CES functionality [9], including a richer extraction policy to handle fragment grouping, which is described in this paper. Due to space constraints this could not be included with the work reported in this short version of the paper, however, the interested reader is referred to the full version where it is included [8].

3.3 Other Work

A general concept, proposed by Rivest [19], which has since been referred to as "...signature schemes that admit forgery of signatures derived by some specific operation on previous signatures but resist other forgeries." [3]. Micali and Rivest introduced transitive signature schemes in this area [14], while Bellare and Niven presented schemes that provided performance improvements [3]. Johnson, Molnar, Song and Wagner have investigated a general approach to homomorphic signature schemes for some binary operations such as: addition, subtraction, union, intersection [13].

Brands has performed extensive work on enhancing the privacy of document owners and has proposed "Digital Credentials", which are issued by trusted "Credential Authorities", along with associated protocols that have the capability for selective disclosure of the data fields in the credential [6, 7].

A different approach was taken by Orman [18] who proposes using the XML-sig for an authorisation and validation model for mildly active content in web pages. This enables the content owner's intentions with respect to document modification to be embodied in the document so that any party can validate the document with respect to these intentions. It permits the document owner to delegate modification rights verifiably by signing the URL: a form of "late binding".

Other work has focussed on certain types of path and selection queries over XML documents that can be run on untrusted servers. Devanbu, Gertz, Kwong et al. [11] have proposed a new approach to signing XML documents so that answers to arbitrary queries can be certified.

4 Solutions

4.1 Using Standard Digital Signatures

A simplistic approach to the content granularity problem is for Alice, the signer, to sign the individual document fragments using the standard digital signature and to forward all these signed fragments to Bob, the information holder, for use. If there are n content fragments, then the computational overhead would be n signatures.

Bob does not need to perform any further computation as all that is required is simply to forward the required fragment(s) along with their associated signature(s) to Carol, the information consumer, for verification. For peace of mind, however, it is likely that Bob would first verify each fragment received from the signer, thus requiring n signature verifications.

Carol, upon receipt of the fragment(s) would have to perform m signature verifications where $m < n$ and m is the number of fragments forwarded by Bob.

How could Alice protect against the potential of disclosure abuse? If Alice follows the scheme described above, she *cannot* protect against disclosure abuse. Her alternative is to decide upon allowed subsets of fragments, corresponding to various permissable fragment associations, or groupings. Each of these subsets could be signed and issued as a separate document. There is an upper bound of 2^n possible subsets, which implies a considerable document management challenge for both Alice and Bob.

Using the standard digital signature in this manner departs from the conventional single document/container approach and involves many signed items.

This would require more storage space and complicate the handling required by Bob. Notwithstanding the storage problem, the prospect of searching through the many items to find the desired combination of fragments to disclose would be daunting.

4.2 Using Content Extraction Signatures

Content Extraction Signatures can be verified for a subdocument which has been generated by blinding or removing portions of the original signed document, in accordance with the signer's policy for blinding the document content [21]. The communications and/or computational cost of CES is lower than that of the simple multiple signature solution using the standard digital signature described above.

The same general structure initially proposed for CES will be used. However, in this work we substantially extend the Content Extraction Access Structure (CEAS) encoding to enable the signer to specify a *richer extraction policy* for the document fragments.

Fragment Extraction Policy In [21] we did not specify an encoding scheme for the CEAS. In this paper, we focus on the ability to select and extract particular fragments and their associations, or grouping, with any other fragments. Thus, we have a multidimensional view of the fragment. This presents a challenge: how to achieve this flexibility in the fragment extraction policy whilst constraining the size of the extraction signature. For a document containing n fragments there are 2^n subdocuments possible (although the number of useful subdocuments would be smaller) and 2^{2^n} permutations of the CEAS for the relationships of the n fragments with each other.

The CEAS provides a mechanism for the document signer to avoid the abuse of extracted content by specifying which fragments and groupings (via fragment associations) can be extracted. It is an encoding of the subsets of fragment groupings for which the document holder is 'allowed' to extract valid signatures. All associations are relative to a 'primary target' fragment, asymmetric and non-transitive. Association transitivity has not been included in this work and has been left for further work.

A fragment that is allowed to be extracted in its own right is considered to be a *primary* target. Only primary targets may be directly selected for extraction. If a fragment is not a primary target, then it is called a *secondary* target and may only be extracted through an association with a primary target. If a fragment has a mandatory association with a primary target, this means that the associated fragment *must* accompany the primary target fragment if it is extracted. A fragment which has an optional association with a primary target fragment *may* accompany the primary target fragment if it is extracted. A fragment cannot have a mandatory and optional association with the same fragment.

We will now describe fragment policy options and their use by the document owner. A fragment type and its extraction permissions can be identified as:

- a secondary target with no associations—it can never be extracted;
- a secondary target with mandatory associations—can only be extracted when accompanying a primary target fragment via a mandatory association;
- a secondary target with optional associations—it can only be extracted when accompanying a primary target fragment through an optional association;
- a primary target with no associations—it can be extracted by itself;
- a primary target with mandatory associations—if extracted it must be accompanied by its associated mandatory fragments;
- a primary target with optional associations—if extracted it may be accompanied by its associated optional fragments; or
- a primary target with mandatory associations from *all* other primary targets—a mandatory fragment which must accompany any primary fragment that is extracted.

CEAS Using Byte Lists A simple approach to storing the signer's fragment extraction policy is to use lists for the fragment associations. We implement for each fragment a list for its mandatory associations and a list for its optional associations. A target's type is determined by which list its own number is located in: primary target if in the mandatory list, otherwise secondary target if in the optional list.

With a 32 bit fragment identifier, the size of the CEAS for a document containing 100 fragments with an average of, say, 20 associations per fragment would be 64kbits.

CEAS Using Bit Vectors Bit vectors could be used as an alternative to using lists, where for a document with n fragments, we allocate a vector of n bits for each fragment. This can be seen as a $n \times n$ bit matrix, irrespective of the number of associations. As there are n bits available per fragment, we use:

- *the self-referent bit*—to specify if the fragment is a primary target or a secondary target; and
- *the non self-referent bits (or other bits)*—to specify the mandatory and optional fragment associations.

The type of association specified by the other bits depends on whether the fragment is a primary or secondary target. For primary targets the other bits define the mandatory associations, while for secondary targets they define the optional associations. Also, there are no optional associations between two primary fragments. This would be redundant, as you can simply extract the two primary fragments, or not, as required.

A simple CEAS for a document with six fragments is illustrated in Table 1. This simple example illustrates the encoding of the various fragment types as identified above. However, it is expected that an actual extraction policy would likely involve a good deal more associations. Following is an explanation of the fragment extraction policy for the document.

Table 1. Sample CEAS for a document with 6 fragments

Fragment no.	CEAS
1	0 0 0 0 0 0
2	0 0 0 0 0 0
3	0 0 0 0 1 0
4	0 1 0 1 0 1
5	0 0 0 0 1 1
6	0 0 0 0 0 1

Frag1 is a secondary target and can never be extracted as no other fragments are associated with it, ie. $CEAS_1[1] \vee \ldots \vee CEAS_n[1] = F$

Frag2 is a secondary target and can only be extracted through its mandatory association with frag4. If frag4 is extracted, then frag2 must accompany it.

Frag3 is a secondary target and can only be extracted via its optional association with frag5. If frag5 is extracted, frag3 may optionally accompany it.

Frag4 is a primary target with some mandatory fragment associations that must accompany it should it be extracted. If frag4 is extracted, then frag2 and frag6 must accompany it.

Frag5 is a primary target with mandatory and optional fragment associations. Should frag5 be extracted, then frag6 must accompany it, while frag3 may optionally accompany it.

Frag6 is a primary target with no associations that must accompany it should it be extracted. Frag6 can be extracted by itself.

Frag6 is also a mandatory fragment, which must always be extracted, as every primary target has a mandatory association with it, ie.

$b_1 \wedge b_2 \wedge \ldots b_n = T$

where $b_i = \neg CEAS_i[i] \vee CEAS_i[6]$ and i indexes the fragments.

As the bit matrix hints, the CEAS is in fact a labelled directed graph, the matrix in Table 1 corresponding to the connectivity matrix. The node labels indicate fragment identity, and edges represent associations. Primary targets are represented by nodes that are connected to themselves. Nodes corresponding to primary targets have edges directed to the nodes with which they have mandatory associations. Nodes corresponding to secondary targets have edges directed to nodes with which they have optional associations.

List-based representations are most efficient when the average number of associations (i.e. edges) per fragment (i.e. node) is low. The bit matrix will be the better encoding when the association density is high. Let f be the size of the fragment identifier in bits and $\bar{a}$ be the average number of associations per fragment. The size of the list encoding is $n\bar{a}f$ bits and the matrix encoding is n^2 bits. The matrix encoding will thus be the more efficient when $\bar{a} > n/f$. For the example in Section 4.2, the matrix representation would cost 10kbits.

Signing the Document Signing the document using Content Extraction Signatures involves a two step process: (i) define the fragments, and (ii) specify the fragment extraction policy. The process of defining a fragment includes specifying the content itself as well as whether it is a primary or secondary target. Once the fragments have all been defined, the signer specifies the mandatory and optional fragment associations for each fragment. This information is included as part of the extraction signature. On completion of signing, the document and its extraction signature is forwarded to the document holder.

5 Conclusion

In an electronic society where the use of paper is more the exception than the norm, we have shown that the use of the current digital signature can erode privacy and increase bandwidth usage in multiparty interactions. We have introduced a new, more powerful, approach for encoding the signer's fragment extraction policy. This approach is tailored more for selective fragment grouping rather than selective fragment blinding, as was the emphasis in our earlier paper. This different perspective for the use of CES presents the concept of handling verifiable information selectively for paperless commerce in an online and a mobile environment. Content Extraction Signatures can be used for almost any multiparty interaction involving the selective disclosure of information.

In a digital world, which promises far richer functionality than the paper-based world, we seek more flexible applications of digital signatures. With this work we are striving for additional functionality, beyond that which a simple analogue of the humble and longstanding hand-written signature provides.

References

1. S. Baker. Don't worry be happy. Available online, June 1994. [Last accessed: July 27, 2002].
   URL: http://www.wired.com/wired/archive/2.06/nsa.clipper_pr.html
2. M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon. XML-signature syntax and processing. In D. Eastlake, J. Reagle, and D. Solo, editors, *W3C Recommendation.* Feb. 12 2002. [Last accessed: September 18, 2002].
   URL: http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/
3. M. Bellare and G. Neven. Transitive signatures based on factoring and RSA. In Y. Zheng, editor, *Proceedings of The 8th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2002)*, volume 2501 of *Lecture Notes in Computer Science*, pages 397–414. Springer, December 2003.
4. T. Beth, M. Frisch, and G. Simmons, editors. *Public-Key Cryptography: State of the Art and Future Directions*, volume 578 of *Lecture Notes in Computer Science.* Springer, July 1992. E.I.S.S. Workshop Oberwolfach Final Report.
5. G. Blakley. Twenty years of cryptography in the open literature. In *Proceedings of 1999 IEEE Symposium on Security and Privacy*, pages 106–7. IEEE Computer Society, May 1999.
6. S. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* MIT Press, Cambridge, MA, 2000.

7. S. Brands. A technical overview of digital credentials. Available online, Feb. 20 2002. [Last accessed: February 18, 2003].
URL: `http://www.credentica.com/technology/overview.pdf`
8. L. Bull, D. M. Squire, J. Newmarch, and Y. Zheng. Grouping verifiable content for selective disclosure using XML signatures. Technical Report, School of Computer Science and Software Engineering, Monash University, 900 Dandenong Road, Caulfield East, Victoria 3145 Australia, April 2003.
9. L. Bull, P. Stanski, and D. M. Squire. Content extraction signatures using XML digital signatures and custom transforms on-demand. In *Proceedings of The 12th International World Wide Web Conference (WWW2003)*, Budapest, Hungary, 20–24 May 2003. (to appear).
10. M. Crompton. The privacy act and the Australian federal privacy commissioner's functions. In *Proceedings of the tenth conference on computers, freedom and privacy*, pages 145–8. ACM Press, 2000.
11. P. T. Devanbu, M. Gertz, A. Kwong, C. Martel, G. Nuckolls, and S. G. Stubblebine. Flexible authentication of XML documents. In *ACM Conference on Computer and Communications Security*, pages 136–45, 2001.
12. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–54, 1976.
13. R. Johnson, D. Molnar, D. Song, and D. Wagner. Homomorphic signature schemes. In *Proceedings of the RSA Security Conference Cryptographers Track*, volume 2271 of *Lecture Notes in Computer Science*, pages 244–62. Springer, February 2002.
14. S. Micali and R. L. Rivest. Transitive signature schemes. In B. Preneel, editor, *Proceedings of The Cryptographer's Track at the RSA Conference (CT-RSA 2002)*, volume 2271 of *Lecture Notes in Computer Science*, pages 236–243. Springer, December 2002.
15. Office of the Federal Privacy Commissioner. My privacy my choice - your new privacy rights. Available online. [Last accessed: July 31, 2002].
URL: `http://www.privacy.gov.au/privacy_rights/npr.html`
16. Office of the Federal Privacy Commissioner. Privacy in Australia. Available online, October 2001. [Last accessed: July 12, 2002].
URL: `http://www.privacy.gov.au/publications/pia.html`
17. Office of the Federal Privacy Commissioner. Announcement: Transurban privacy review completed. Available online, May 2002. [Last accessed: July 31, 2002].
URL: `http://www.privacy.gov.au/news/media/02_9.html`
18. H. Orman. Data integrity for mildly active content. In *Proceedings of Third Annual International Workshop on Active Middleware Services*, pages 73–7. IEEE Computer Society, March 2002.
19. R. Rivest. Two signature schemes. Available online, October 2000. Slides from talk given at Cambridge University. [Last accessed: February 19, 2003].
URL: `http://theory.lcs.mit.edu/ rivest/publications.html`
20. R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–8, 1978.
21. R. Steinfeld, L. Bull, and Y. Zheng. Content extraction signatures. In *Proceedings of The 4th International Conference on Information Security and Cryptology (ICISC 2001)*, volume 2288 of *Lecture Notes in Computer Science*, pages 285–304. Springer, December 2001.