XML Security — A Comparative Literature Review

Andreas Ekelhart [*], *Stefan Fenz* [†], *Gernot Goluch* [‡], *Markus Steinkellner* [§], *Edgar Weippl* [¶]

Abstract

Since the turn of the millenium, Working Groups of the W3C have been concentrating on the development of XML based security standards, which are paraphrased as XML Security. XML Security consists of three recommendations: XML (Digital) Signature, XML Encryption and XML Key Management Specification (XKMS), all of them published by the W3C.

By means of a review of the available literature the authors draw several conclusions about the status quo of XML Security. Furthermore the current state and focuses of research as well as the existing challenges are derived. Trends to different application areas - e.g. use of XML Security for Mobile Computing - are also outlined. Based on this information the analyzed results are discussed and a future outlook is predicted.

Keywords: XML Security, XML Encryption, XML Signature, XML Key Management, Web Services, Privacy

1 Introduction

Since the publication of the first two XML Security Recommendations, XML Signature and XML Encryption, several implementations of those standards have provided information about problems during their appliance in real

[*]Secure Business Austria, Vienna, Austria, ekelhart@securityresearch.ac.at

[†]Secure Business Austria, Vienna, Austria, fenz@securityresearch.ac.at

[‡]Secure Business Austria, Vienna, Austria, goluch@securityresearch.ac.at

[§]Information & Software Engineering Group, Vienna University of Technology, Austria, steinkellner@ifs.tuwien.ac.at

[¶]Information & Software Engineering Group, Vienna University of Technology, Austria, weippl@ifs.tuwien.ac.at

world applications. Because of the flexibility of the standards, further research and development was required to adapt them to specific application areas. These areas are widespread due to the fact that XML is the de facto standard for data exchange in information technology not only in the well-known areas, such as E-Commerce, Grid Computing, Agent Systems, etc., but also in a lot of major industry sectors, e.g. the automotive industry, which focus on XML-based description standards for data interchange. Considering the difference between those areas, it becomes obvious that disparate requirements on the digital signature and the encryption of XML are set. For example, Grid Systems require flexibility because of the different architecture and access methods of their resources. On the other side, confidentiality plays the most important role for the exchange of information between two business partners. These different requirements can cause conflicts if they are mutually exclusive. For instance, flexibility, scalability and confidentiality can be provided easily, but only at the expense of performance.

The goal of this literature review is to work out a status quo of XML Security and derive the current state and focuses of research in this area.

2 Methodology

Based on (Ma & Nickerson 2006) we defined our own methods for a sophisticated comparison of current research in the area of XML Security.

In order to find existing literature we focused on the digital libraries of ACM, IEEE, ScienceDirect and Springer, using Boolean search strings, such as "XML (Digital) Signature", "XML Encryption", "XKMS", "XML Key Management Specification" or "Canonicalization". Regarding quality criteria (i.e. the number of references to the specific publication) and contents 50 articles were selected for a full-text review and analysis.

Table 1 shows the classification of the selected articles according to source and publication year.

Source	Sum	2002	2003	2004	2005	2006
ACM	09	3	3	0	2	1
IEEE	14	2	0	4	7	1
ScienceDirect	06	0	1	2	1	1
Springer	21	0	2	7	7	5
Sum	50	5	6	13	17	9

Table 1: Classification according to source and publication year

After the selection process we formulated a priori hypotheses whose veri-

and/or falsification is the dedicated goal of this work.

An objective consideration, regarding the hypotheses, is guaranteed during the review process, due to the predefined focuses. Besides the analysis of our a priori hypotheses, we furthermore describe several observations which were made during the literature review. Table 2 in the Appendix of this work provides the basis for the following hypotheses and observations.

In order to check the relationship between certain standards, we defined values for this correlation:

- No relation = No. of mentions in the article < 3
- Some relation = No. of mentions > 3, but standard is not an elementary component of the article
- Strong relation = Standard is a fundamental part of the article

3 Hypotheses

3.1 H1: In connection to Web Service technology many appliances of XML Security exist

Regarding the appliance of XML Security in connection with Web Services, it turned out that 24 articles bear no, 9 some and 17 strong relation to Web Services. I.e., more than half of all works of the reviewed literature deals with the usage of XML Security in conjunction with Web Services. Considering only articles in connection with the appliance of XML Security standards, this relationship is even more obvious: 19 of 29 articles which are concerned with concrete applications deal with Web Services as well. Remarkably often Grid Systems are also mentioned in this context.

As a result of the literature review, this hypothesis could be validated. Some enterprises, e.g. RSA and Forum Systems, offer XML Security support only within their Web Service Security Suites. Thus, we assume that this trend will continue since XML Security seems to merge more and more with Web Service Security.

3.2 H2: W3C XML Security standards are accepted and their quality is not put into question

It proved true that the Scientific Community plays an important role in the evolution of such technologies. Without any doubt you can gain valuable in-

sight into the (dis)advantages of XML Security by reading scientific literature about this topic.

As a result, some publications included criticism, but some also mentioned potential for improvement and modifications for adapting the standards to special areas. Criticism focused mainly on bad performance and security problems, i.e. the presentation problem. Both issues are discussed in detail in sections 4.1 and 4.2.

In fact, only two articles questioned one or several standards: (Hormann, Wrona & Holtmanns 2006) compares certificate validation mechanisms and states that XKMS is similar to the Online Certificate Status Protocol (OCSP) concerning security, complexity and interoperability, but that it is clearly worse regarding performance and scalability, concluding that OCSP has to be preferred to XKMS. (Bull & Squire 2004) criticizes a part of the XML Signature standard, which states that first references and afterwards the signature is validated. By using custom transforms which are referencing malicious code, this can lead to a security vulnerability. Section 4.2 provides further details about this issue.

Although both articles address serious problems, these will not form an insurmountable obstacle in the evolution of XML Security. Nevertheless the criticism reveals that at some point of this technology further research and development is necessary.

3.3 H3: The XML-based Security Standards (XML Signature, XML Encryption, XKMS, SAML, XACML, XrML) are overlapping

This hypothesis did not validate as clearly as expected, because only a little more than half (26) of the articles discussed two or more standards whereas the number of works with three or more standards is relatively high (18). This can be traced back to the fact that none of the standards was mature at the time of publication. In this respect, scientists preferred to tackle only an aspect of XML Security instead of the integration of several premature standards. This presumption could be verified because more articles, published in the last two years, work on two standards at least.

Regarding XML-based standards which are not assigned to XML Security, some interesting observations could be made: XrML emerges only one time in (Delgado, Gallego & Perramon 2001). Due to their similarity XACML and SAML often occur together, particularly in connection with Web Services. Based on XML Security, a lot of these articles focus on establishing an integrated security system for Web Services, with SAML for Single Sign-On and

XACML for access control (Lee, Upadhyaya, Rao & Sharman 2005, Park, Moon, Sohn & Park 2004, Zhang, Wang & Zhou 2004, Park, Moon, Jang & Sohn 2004*c*, Park, Moon, Jang & Sohn 2004*b*, Park, Kim, Chung, Kim & Won 2005).

At least in scientific literature, it can be stated that XML Security standards are not as overlapping as thought. Indeed they will be used more and more in terms of an integrated security system. Whether these analyzed results can also be noticed in industry implementations was not an object of investigation. However the possible interaction of different standards was a basic goal in the evolution of XML Security.

3.4 H4: Many articles are published by enterprises and/or are published in connection with enterprises, i.e. the IT industry accelerates further evolution

The analysis shows that the Scientific Community is unambigiously in the hands of the universities. Only 8 articles were published by enterprises - 4 by universities in conjunction with enterprises. Mainly companies from North America and Europe published those articles whereas IBM (5 articles) claimed the majority. It seems as if the basic framework and the design goals would have been specified by the industry, while now the universities have to keep on "supervising" this technology up to market maturity. This impression deceives since the enterprises participate in the development but do not publish all of their scientific work in digital libraries. You only have to take a look at the websites of Verisign, Entrust or IBM to be able to ascertain this. The articles of the enterprises tend to deal on the more practical tier as opposed to the other reviewed publications.

Nonetheless this hypothesis cannot be validated. Rather, the universities do a good and valuable job in this respect.

4 Observations

In spite of the diversity of the articles some interesting comparisons can be drawn. For better understanding we divided the 50 articles into two groups. The first group consists of publications about the standard itself or the enhancement of the standard ("Syntax group"). The second one discusses concrete applications ("Application group"). Table 2 in the Appendix shows the assignment of the publications to these groups.

As only 19 articles deal with the standard itself, the predominant part (29 articles) can be counted among the application group. This seems surprising because several articles explicitly stated that the standards are not mature and need more development (Park, Moon & Sohn 2004, Lee, Moon & Sohn 2002, Park, Moon, Jang & Sohn 2004*a*, Park, Moon, Jang, Sohn & Won 2005, Schadow 2005). Another interesting point is the fact that the majority of articles tackle XML Signature although it is the oldest standard (see Appendix—Table 2). Nevertheless, we want to outline the observations from the syntax group first, before the implementations are analyzed.

4.1 Observation 1: Bad performance and memory inefficiency of XML Security

One of the prior design objectives of XML Security was the flexibility and the expressiveness of this new technology. Thereby the performance was disregarded and apparently left to further development. Thus it is not remarkable that frequently mentioned criticism points are the bad performance and memory inefficiency of the standards. Many implementations use DOM-trees since they can be manipulated more easily. But generally, this is at the expense of time and storage. Canonicalization may require a transformation sequence which involves multiple conversions back and forth between DOM and an octet stream which is a serious problem. (Shirasuna, Slominski, Fang & Gannon 2004) tested this in a performance comparison between XML Signature, SSL and Web Service Security. At the used XSUL (Web Service/XML Service Utility Library) implementation with a fast XML Pull Parser it was found, that Canonicalization required 1391 of 1542 msec for signature generation and 1395 of 1445 msec for verification. All other stages such as the calculation of the digest, the en- or deciphering of it and the path validation are minor matters. A similar test for the evaluation of bottlenecks at XML Signature shows slightly better results (Chen, Huang, Hou, Lee, Yang & Cheng 2005). For this purpose a SOAP message was signed and verified 500 times at full CPU speed in a DOM-based implementation with XPath. Then the operating time was assigned to four different components (Canonicalization, XPath, Parser, Other). For the generation of the signature, Canonicalization required 37,6% and XPath 21,2% of the time; for verification Canonicalization 47,7% and XPath 31,5%. Even if these values are smaller than computed before - due to the modified test environment - Canonicalization offers enough scope for faster processing. But not only the signature is affected by this problem, also XML Encryption suffers in the same way from the use of Canonicalization (Imamura, Clark &

Maruyama 2002, Yang, Ng, Lau & Cheng 2006).

(Park, Kim, Chung, Sohn & Won 2006) on the other hand refers the performance problem to the self descriptive structure of XML itself. Due to the inefficient representation of the data, XML based messages are larger and need more operating time than existing protocols as RMI, RMI/IIOP or CORBA/IIOP. (Hormann et al. 2006) confirms this through an evaluation of certificate validation mechanisms, in which short-lived certificates, CRLs, OCSP and XKMS are compared. The sizes of OCSP's requests and responses are much smaller compared to those of XKMS. Also at the criteria scalability XKMS loses against OCSP. On the opposite side, the interoperability with all XML protocols was mentioned positively. Since the client has to interact with the XKMS service continuously, the management overhead was criticized. On the other side the possibility of the users to decide the degree of trust assertion by themselves is one of the major advantages of XKMS.

An example of an e-Diagnostic/Maintenance Framework from the semiconductor industry, which plans to implement XML Security in a Web Service environment, shows how problematic these issues can be (Hung, Chen, Ho & Cheng 2003). By using a system implementation with an integration test the overhead of XML Signature and Encryption was tested. Secured by these two technologies a 100-character string was 600 times slower than unsecured when sending by a Web Service. In this case the bad performance could just still be accepted.

Among criticism various works offered different methods of resolution which provide confident results. The most promising approach is probably the use of stream-based parser since they need no time- and memory consuming DOM-trees and explicit node-sets for data representation. (Imamura et al. 2002) offers an implementation for XML Encryption and (Lu, K.Chiu, A.Slominski & D.Gannon 2005) describes a stream-based parser for signing SOAP messages. The latter describes the architecture and implementation of the GHPX Parser, a fast generic parser developed for usage in connection with Canonicalization. GHPX was implemented in C++ and offers an interface similiar to SAX, but has the advantage that not the whole parsing context is required. However the most important benefit is that Canonicalization is carried out during parsing. Hence the canonical form is a by-product of this process. The memory consumption of GHPX is almost constant compated to the XML Security Library (Wei, Chiu, Slominski & Gannon 2005). For generation of the digital signature GHPX calculates the message digest incrementally, i.e the canonical form is written into a buffer. If this is full, the resultant digest is computed and stored as an intermediate result before the rest keeps on being processed. Besides a Streaming SOAP Signature Validator (SSSV), who acts as an intermediary node between GHPX and

real application, provides fast verification by recognizing and validating the signatures automatically. The developed test implementation was compared with a Libxml2 implementation, both using SAX2 API for parsing. Due to the recursive parsing of GHPX, Libxml2 has advantages in parsing performance. Canonicalization on the other hand could be accomplished 4 to 5 times faster with GHPX; with larger XML files this performance advantage increases even more. Also signature validation was 6 to 7 times faster with GHPX in combination with SSSV. This can be traced back to the explicit node-sets and the use of DOM-trees of Libxml2. With GHPX memory usage remains constantly while this is increasing arithmetically in case of Libxml2. Without any doubt performance and scalability can be improved by using stream-based parsers.

Similiar to GHPX the Quick XML Parser described in (Chen et al. 2005) dispenses with the repeated construction of DOM trees. Instead it generates the required byte array directly. Canonicalization is also carried out at parsing by using tables from the Xerces Native Infrastructure (XNI) as temporary data structure. The performance test shows that validation of SOAP messages can be processed 7 to 21 times faster compared to a DOM-based implementation. If the number of validations increases this advantage is even more recognizable.

Already 2002 IBM developed together with Apache a stream-based parser for XML Encryption (Imamura et al. 2002). Therefore the flexible architecture of Xerces2 was used and adapted to the given requirements. Xerces2 is built up as a pipeline of different parser components. For XML Encryption the basic configuration XML-> Scanner-> Validator-> Parser-> API was expanded to XML-> Scanner-> Validator-> Encryptor-> Parser-> API in case of encryption and XML-> Scanner-> Decryptor-> Validator-> Parser-> API in case of decryption. The stream-based implementation achieved a 0,27-26% reduction of processing time for encryption of XML documents with sizes larger than 2KB and 34-88% for decryption of XML documents of any size. The best performance for the combination of encryption and decryption is achieved if the size of an XML document is in the range from 100KB to 200KB before encryption. Simulations show that particularly time for decryption can be reduced radically by such developments. Also some articles like (Shirasuna et al. 2004) recognized this and defined a stream-based implementation at least as "Future Work".

Apart from this general work on improvement of the performance, other application-specific ideas could be found. (Park, Moon, Kim, Chung & Sohn 2005) and (Park et al. 2006) outline the mergence of XML Signature and Encryption for Location Based Services (LBS) in mobile environment.

Location Based Systems are information services which are accessible over

telecommunication networks via mobile devices and have the ability to determine their location. A well-known example of location-oriented services is GPS (General Positioning System). The primary requirement of this emerging technology is the protection of privacy. While this can be guaranteed by using XML Security, the limited bandwith of mobile devices is an existing problem. In order to bring these technologies together in spite of these issues, an XML "Signcryption" method was defined. Syntactically the structure is similiar to the XML Signature whereas encryption is already integrated. An implementation with JCE (Java Crypto Extension) and SAX supplies better performance compared to the traditional method while integrity and confidentiality are still preserved. It is not surprising that signature generation is distinctly faster than verification since the complexity of the verification suffers from this new approach.

4.2 Observation 2: There are existing security issues

Besides the known presentation problem, some articles uncover further possible security vulnerabilities. These have to be taken seriously even though they are usually only visible at specific applications.

Due to the higher security risk we want to start with the presentation problem for which (Boyer 2003) and (Kubbilun, Gajek, Psarros & Schwenk 2005) offer methods of resolution. Already 2003 (Boyer 2003) focuses on the XML Forms standard ((Boyer, Landwehr, Merrick, Raman, Dubinko & Klotz 2006), published not before March 2006 by the W3C) to detect layout modifications in the XML Signature. This idea is particularly forced by the W3C itself since the integration of XForms and XML Signature enjoys highest priority in the XForms Working Group (Boyer 2006). XML Forms is a representation form that is supposed to fulfill the security maxim "What you see is what you sign" (WYSIWYS). The article shows two alternatives to ward off potential attacks via graphical (dis)appearance of parts of the signature. The first alternative is Overlap Testing in order to detect prohibited superposition. That means, a fast and efficient algorithm divides the document into rectangles and tests with the aid of their x- and y-coordinates whether they overlap. On the other hand the possibility of a Significant Layout Change Test is mentioned. Therewith it is tested if the relative layout of the signed document parts has changed after the document had been divided into sections and the layout had been stored as a hashed value.

(Kubbilun et al. 2005) goes one step further by presenting an implementation of a visualization for multisignatures with the help of XSLT. Different previous approaches, like saving the document as an image or using a given standard like S/MIME, were refused as too impractical and application-

specific. The visualization based on XSL transformations was therefore developed with the objective of usage on standard web browsers and the possibility of flexible adaptation to different display formats, e.g. display of a portable. This can be achieved without any big problems by transforming XML to (X)HTML. In the proof of concept implementation with Java and the XSLT processor Apache Xalan, the signed elements are highlighted graphically. It can be recognized that XSL is indeed very suitable but much work on the appropriate (graphical) representation still has to be done.

Apart from the presentation problem only (McIntosh & Austel 2005) and (Bull & Squire 2004) deal with security vulnerabilities - both related to XML Signature. (McIntosh & Austel 2005) examines attacks on signed SOAP messages and possible countermeasures. Subtle modifications in the references of an XML Signature inside a SOAP message can lead to security problems since this protocol is very sensitive to such changes. Hence (McIntosh & Austel 2005) recommends to use XML Signature together with SOAP only when appropriate security policies are specified and correctly enforced. Since these changes in the references of a signature can usually be tolerated and this is only a problem of specific SOAP messages, it is referred to (McIntosh & Austel 2005) for further details.

(Bull & Squire 2004) detects another vulnerability during development of a transformation in order to integrate available updates of a chosen XML Signature implementation. These updates should be downloaded and executed dynamically from a remote location. An attacker could see this transformation and replace the reference and the valid digest with a different reference linking to malicious code. In the XML Signature Recommendation it was stated that first references and afterwards the signature must be validated. What happens with an application implemented according to the official standard syntax and processing? After dereferencing the references the malicious code will be executed. However, the solution is obvious: Signature validation has to be done before reference validation because in this case the changed message digest would be discovered. The attacker is not able to change the digest over the whole signature without holding the signature key. This would end in an abort of signature validation before the compromised references are processed.

Concerning XKMS there is also a current work from 2006 tackling security considerations. In the article (Hormann et al. 2006), already mentioned in section 4.1, different certificate validation mechanisms were compared. XKMS got a bad report because the client does not have any possibility to check the integrity of the XKMS' Public Key. Furthermore XKMS does not offer any revocation of its key pair if it falls into wrong hands. The Working Group of the XML Trust Assertion Service Specification (XTASS)

is already working on a solution for this problem. Except this, all other security attacks could be warded off. Man-in-the-middle attacks have no success since the whole response is signed. Replay attacks are prevented by the use of <TransactionID> elements binding requests to their corresponding responses. Denial-of-Service (DoS) attacks can be eliminated by implementing a limited-use shared secret with <PassPhraseAuth> or <KeyBindingAuth>. As major advantage the freshness of messages is considered. I.e. XKMS has direct channels in order to communicate with the PKI and supplies current information about the certificates. Due to the lacking trust assertion of the XKMS' Public Key, it has been rated "not satisfactory" and evaluated as the worst certificate validation mechanism in spite of good individual results.

4.3 Observation 3: XML Security for Mobile Computing

XML established itself as the standard for data exchange in distributed networks. At the same time a strong trend toward mobile applications and wireless networks can be observed (Project 2007), manifested by the boom of Wireless LAN and navigational instruments. Nevertheless this field is not exhausted. A lot of new technologies, whose concrete evolution cannot be appreciated now, will join. Not only the application area but also the programming and implementation environment can vary strongly. By means of its flexibility XML is able to cover almost all requirements, especially as the usage in Mobile Computing was an objective of the development of XML. First of all the interoperability and the general agreement on this standard is the biggest advantage of XML in this field while its inefficiency seems to be the only handicap. The latter can have a very bad effect because many mobile devices have problems with bandwith and memory storage. Due to the fast evolution in mobile data transfer (e.g. HSDPA) and micromemory (e.g. micro-SD) this disadvantage will become obsolete in the near future.

Many researchers and developers recognized this trend so that in mobile environment XML enjoys the same influence as in "traditionally wired" networks (Nair, Gopalakrishnan, Mauw & Moll 2005). On basis of these evolutions the application of XML Security is consequentially. The literature review affirms this trend because 6 works deal with the concrete appliance in Mobile Computing. In addition, 4 articles defined the application of XML Security in mobile environment as Future Work (Park, Moon & Sohn 2004), (Lee et al. 2002), (Park, Moon, Jang & Sohn 2004*a*), (Park, Moon, Jang, Sohn & Won 2005). It is presumed that this trend will continue. Remarkably, 3 of these mentioned 4 articles deal with Web Services.

Thus the combination of XML Security, Web Services and Mobile Computing can be very promising in the future. Also much information apart from this literature review indicate that particularly the IT industry shows large interest.

Both of the two very similar articles (Park, Moon, Jang & Sohn 2004*c*) and (Park, Moon, Jang & Sohn 2004*b*) cover the appliance of XKMS in Mobile Grid systems. They tackle the development of a middleware framework for certificate validation with XKMS. For this purpose SAML is used for integrating Single Sign-On and XACML for the definition of a policy. The protocol for secure Mobile Grid applications is based on three main actors: the Mobile Grid application itself, the SAML processor and the XKMS server. Published in 2004, both publications address the already mentioned boom in the fields of Web Service and Mobile Computing. For a detailed description of the frameworks, including sequence and component diagrams, (Park, Moon, Jang & Sohn 2004*b*) is referenced.

(Nair et al. 2005) gives an interesting insight in the appliance of XML Security in multimedia environment. Philips and the Eindhoven University of Technology work on a secure interactive application in connection with the new generation of optical disc formats like Blu-ray, High-Definition DVD (HD) and enhanced DVD. Unfortunately this article does not represent many of the far-reaching multimedia possibilities of XML Security. The opinions of the authors let us hope for further research in this field.

4.3.1 XML Security for LBS

The Korean Information Security Research Division of the Electronic and Telecommunication Research Institute (ETRI) is working on the integration of XML Security with Location Based Systems (LBS). In section 4.1, a short introduction in this technology and the arising performance problems was given.

Despite these problems (Park, Kim, Chung, Kim & Won 2005) develops a key management system based on XKMS and Web Services. Trust is established by a one-time activity per session (Single-Sign On) or by evaluating dynamically on every request. For simulation Single-Sign On was selected and implemented by using SAML. The transaction model consists of the three main actors: LBS application, SAML processor and XKMS Service. Simulation results show that up to a number of 45 clients the system runs stably under the defined conditions. Thereby XML Signature requires 60% of the whole operating time. For this reason (Park et al. 2006) and (Park, Moon, Kim, Chung & Sohn 2005) deal with the development of a method to accelerate this process. Both articles tackle the "Signcryption mecha-

nisms", a combination of XML Signature and Encryption already discussed in chapter 4.1. For this purpose the architecture was taken from (Park, Kim, Chung, Kim & Won 2005). An implementation of this mechanism with JCE (Java Crypto Extension) and SAX supplies better performance compared to the traditional method while integrity and confidentiality are still preserved. This field seems to be a promising application area in the future as well.

5 Discussion

The present analysis provided some interesting results, but also several new questions were raised. Why is performance still felt as the biggest disadvantage of XML Security even though since 2002 ideas and implementations for faster processing of Canonicalization are existing (Imamura et al. 2002)? In fact, stream-based parsers deliver better results than DOM-based and implementations are available for both XML Signature and Encryption. The current state of the art are parsers, published in 2005 by (Chen et al. 2005) and (Lu et al. 2005), who can perform Canonicalization while parsing. Hereby the best results at simulations could be achieved. In the literature no disadvantage of this alternative implementation could be found. At least in performance-critical applications there is no reason for using DOM. It seems that not everyone knows that XML Security represents only a basic framework whose adaptation into different fields is expected. Several articles show that this adaptation is possible in different ways throughout the whole XML field.

It is a fact that XML is very redundant and has large overhead due to its structure. Nevertheless XML evolves into the most important format for data exchange in distributed networks. It would contradict the basic idea of XML to change its design and abandon flexibility by integrating a technology like XML Security. Security has its own price, especially if other requirements also have to be met. The mentioned flexibility can turn out to be very important since no security algorithm offers security forever. With the provided structure it is possible to react to changing conditions.

There is little criticism on the security itself. Only the missing proof of the XKMS Public Key's integrity is an essential issue of XML Security. Published in 2005, the actuality of the standard causes this critique and the XTASS Working Group is already bothered with the solution of this problem. Another big challenge is the presentation problem for which (Boyer 2003) and (Kubbilun et al. 2005) offer promising methods of resolution. For this issue the integration of XForms and XML Signature, announced in (Boyer 2003), has already been realised. The XForms recommendation (Boyer et al.

2006), published by the W3C in March 2006, supports all features of XML Security including transformations. This solves not only the presentation problem, but also an improvement on displaying was achieved. The more it is astonishing that in scientific literature no reference on this work appears since 2003. Nonetheless it remains to be seen if further security problems will arise due to the emerging appliances in big industry systems.

In the application field a trend toward Mobile and Grid solutions is evident. As proved in the hypotheses, the correlation between XML Security and Web Services is recognizably high. While this has been predictable, systems without central management can especially benefit from XML Security. Using the example of Grid Systems you can see that self-organisation is not a trivial requirement in the security area. Nevertheless this can be achieved satisfactorily by using the present standards. Taking these approaches, Multi-agent systems (working autonomously over distributed channels) can also benefit from the addressed advantages of XML Security (Oliveira, Z.Abdelouahab & D.Lopes 2006). However the work on this subject is still just beginning due to the fact that articles exist since the end of 2006. The usage of XML Security can cause further increase to both emerging technologies, Grid and Multi-agents Systems. For Grid Systems, this was already anticipated in (Park, Moon, Jang & Sohn 2004*c*), in case of Multi-agent Systems this prediction is even more evident since they are built upon XML-based RDF-model.

6 Conclusion

A subgoal of XML Security could be achieved undeniably: All XML-based systems can use this security technology with more or less effort. In addition, the existing gap, the absence of a security technology on basis of XML, was filled. Already in recent years, XML Security conduces to the success of the XML Markup Language. We assume that this positive influence will continue with the further maturation of the individual standards of XML Security.

7 Acknowledgment

This work was performed at Secure Business Austria, a competence center that is funded by the Austrian Federal Ministry of Economics and Labor (BMWA) as well as by the provincial government of Vienna.

8 Appendix

Article	WS	Pub	App	Enh	XSig	XEnc	XKMS
(Alvaro, Farrell, Lindberg, Lockhart & Zhang 2005)	0	E	N	N	0	0	2
(Barhoom & Zhang 2004)	0	U	Y	N	2	0	0
(Beznozov, Flinn, Kawamoto & Hartman 2005)	2	E+U	N	N	1	1	0
(Boyer 2003)	0	E	N	N	2	0	0
(Bull, Stanski & Squire 2003)	0	U	N	Y	2	0	0
(Bull & Squire 2004)	0	U	N	Y	2	0	0
(Bull, Squire & Zheng 2004)	0	U	N	Y	2	0	0
(Camenisch, Gross & Sommer 2006)	2	E	Y	N	2	0	0
(Chang & Hwang 2007)	0	U	N	Y	1	2	0
(Chen et al. 2005)	2	U	Y	N	2	0	0
(Cho 2006)	2	U	Y	N	2	0	0
(Delgado et al. 2001)	0	U	Y	N	1	0	0
(Geuer-Pollmann 2002)	0	U	N	Y	0	2	0
(Giereth 2005)	0	U	Y	N	1	2	0
(Hormann et al. 2006)	0	E	N	N	0	0	2
(Hung et al. 2003)	2	U	Y	N	2	2	0
(Hussain & Soh 2004)	0	U	N	Y	2	0	0
(Hwang & Chang 2004)	0	U	N	Y	2	2	0
(Imamura et al. 2002)	0	E	Y	N	0	2	0
(Kim & Moon 2005)	1	U	N	Y	1	1	2
(Kim, Kim, Kim & Shim 2006)	1	U	N	Y	2	0	1
(Kubbilun et al. 2005)	0	E+U	N	Y	2	0	0
(Lee et al. 2002)	0	E	N	Y	2	0	0
(Lee, Kwon, Lee, Oh & Ko 2003)	2	E	Y	N	1	1	1
(Lee et al. 2005)	1	U	Y	Y	2	2	0
(Lee, Choi, Lee, Moon & Lee 2006)	2	U	Y	N	2	0	0
(Lim, Kim, Moon & Baik 2005)	0	U	Y	N	2	0	0
(Lu & Chen 2004)	0	U	N	Y	2	0	0
(Lu et al. 2005)	1	U	Y	N	2	0	0
(McIntosh & Austel 2005)	1	U	Y	N	0	2	0
(Mohammed & Fiaidhi 2005)	1	U	Y	N	1	1	1
(Nair et al. 2005)	0	E+U	Y	N	2	2	1
(Oliveira et al. 2006)	0	U	Y	N	2	2	2
(Park, Moon & Sohn 2003)	0	U	Y	N	1	1	2
(Park, Moon, Jang & Sohn 2004*a*)	2	U	N	Y	1	1	2
(Park, Moon, Jang & Sohn 2004*b*)	2	U	Y	N	1	1	2
(Park, Moon, Jang & Sohn 2004*c*)	2	U	Y	N	1	1	2
(Park, Moon & Sohn 2004)	2	E	N	Y	1	1	2
(Park, Moon, Sohn & Park 2004)	1	U	Y	N	1	1	2
(Park, Kim, Chung, Kim & Won 2005)	2	U	Y	N	1	1	2
(Park, Moon, Jang, Sohn & Won 2005)	2	U	N	Y	1	1	2
(Park, Moon, Kim, Chung & Sohn 2005)	2	Y	Y	Y	2	0	0
(Park et al. 2006)	1	U	Y	Y	2	2	2
(Polivy & Tamassia 2002)	2	E+U	Y	N	2	0	0
(Schadow 2005)	0	Priv.	Y	N	2	2	0
(Shirasuna et al. 2004)	1	U	N	N	2	0	0
(Sun & Li 2005)	0	U	N	Y	2	0	0
(Takase, Uramoto & Baba 2002)	2	U	Y	N	2	0	0
(Yang et al. 2006)	0	U	Y	N	0	2	0
(Zhang et al. 2004)	2	U	Y	N	1	1	2

Table 2: Classification of the articles

Article	WS	Pub	App	Enh	XSig	XEnc	XKMS
SUM	43	8E-37U-4EU	29Y-21N	19Y-31N	72	39	32
%			58%Y-42%N	38%Y-62%N			

Table 3: Summed up classification of the articles

- WS: Relation to Web Services
- Pub: Published By
- App: Application of the XML Security standards
- Enh: Enhancement of the standards
- XSig: Relation to XML Signature
- XEnc: Relation to XML Encryption
- XKMS: Relation to XML Key Management Specification
- 0: No relation
- 1: Some relation but not elementary component of the article
- 2: Strong relation
- E: Enterprise
- U: University
- Y: Yes
- N: No

References

Alvaro, G., Farrell, S., Lindberg, T., Lockhart, R. & Zhang, Y. (2005), Xkms working group interoperability status report, *in* 'Public Key Infrastructure', Vol. 3545/2005, Springer Berlin / Heidelberg, pp. 86–99.

Barhoom, T. & Zhang, S.-S. (2004), Trusted exam marks system at iug using xml-signature, *in* 'Fourth International Conference on Computer and Information Technology. CIT'04', IEEE Computer Society, pp. 288–294.

Beznozov, K., Flinn, D. J., Kawamoto, S. & Hartman, B. (2005), 'Introduction to web services and their security', *Information and Security Technical Report* **10**(1), 2–14.

Boyer, J. (2006), Applying xml signatures to xforms-based documents, *in* 'XML Conference 2006, Boston, USA'. http://2006.xmlconference.org/programme/presentations/100.html.

Boyer, J., Landwehr, D., Merrick, R., Raman, T., Dubinko, M. & Klotz, L. (2006), 'Xforms 1.0 (second edition) w3c recommendation'. http://www.w3.org/TR/2006/REC-xforms-20060314/.

Boyer, J. M. (2003), Bulletproof business process automation: securing xml forms with document subset signatures, *in* 'XMLSEC '03: Proceedings of the 2003 ACM workshop on XML security', ACM Press, pp. 104–111.

Bull, L. & Squire, D. M. (2004), Xml signature extensibility using custom transforms, *in* 'Web Information Systems (WISE 2004)', Vol. 3306/2004, Springer Berlin / Heidelberg, pp. 102–112.

Bull, L., Squire, D. M. & Zheng, Y. (2004), 'A hierarchical extraction policy for content extraction signatures', *International Journal on Digital Libraries* **4**(3), 208–222.

Bull, L., Stanski, P. & Squire, D. M. (2003), Content extraction signatures using xml digital signatures and custom transforms on-demand, *in* 'WWW '03: Proceedings of the 12th international conference on World Wide Web', ACM Press, pp. 170–177.

Camenisch, J., Gross, T. & Sommer, D. (2006), Enhancing privacy of federated identity management protocols: anonymous credentials in ws-security, *in* 'WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society', ACM Press, pp. 67–72.

Chang, T.-K. & Hwang, G.-H. (2007), 'The design and implementation of an application program interface for securing xml documents', *Journal of Systems and Software* **80**(8), 1362–1374.

Chen, K.-Y., Huang, C.-C., Hou, T.-W., Lee, T.-C., Yang, S.-F. & Cheng, P.-W. (2005), A quick xml parser for extracting signatures of secure web services, *in* 'The Fifth International Conference on Computer and Information Technology. CIT 2005', IEEE Computer Society, pp. 1093–1098.

Cho, K. M. (2006), Xml security model for secure information exchange in e-commerce, *in* 'Computational Science and Its Applications - ICCSA 2006', Vol. 3983/2006, Springer Berlin / Heidelberg, pp. 1003–1011.

Delgado, J., Gallego, I. & Perramon, X. (2001), Broker-based secure negotiation of intellectual property rights, *in* 'Information Security', Vol. 2200/2001, Springer Berlin / Heidelberg.

Geuer-Pollmann, C. (2002), Xml pool encryption, *in* 'XMLSEC '02: Proceedings of the 2002 ACM workshop on XML security', ACM Press, pp. 1–9.

Giereth, M. (2005), On partial encryption of rdf-graphs, *in* 'The Semantic Web (ISWC 2005)', Vol. 3729/2005, Springer Berlin / Heidelberg, pp. 308–322.

Hormann, T. P., Wrona, K. & Holtmanns, S. (2006), 'Evaluation of certificate validation mechanisms', *Computer Communications* **29**(3), 291–305.

Hung, M.-H., Chen, K.-Y., Ho, R.-W. & Cheng, F.-T. (2003), 'Development of an e-diagnostics/maintenance framework for semiconductor factories with security considerations', *Advanced Engineering Informatics* **17**(3-4), 165–178.

Hussain, O. & Soh, B. (2004), Maintaining the integrity of xml signatures by using the manifest element, *in* 'Industrial Electronics Society. IECON 2004, 30th Annual Conference of IEEE', IEEE Computer Society, pp. 493–195 Vol.1.

Hwang, G.-H. & Chang, T.-K. (2004), 'An operational model and language support for securing xml documents.', *Computers & Security* **23**(6), 498–529.

Imamura, T., Clark, A. & Maruyama, H. (2002), A stream-based implementation of xml encryption, *in* 'XMLSEC 2002: Proceedings of the 2002 ACM workshop on XML security', ACM Press, pp. 11–17.

Kim, J. & Moon, K. (2005), Design of unified key management model using xkms, *in* '7th International Conference on Advanced Communication Technology, ICACT 2005', Vol. 1, IEEE Computer Society, pp. 77–80.

Kim, Y.-H., Kim, J.-S., Kim, Y.-S. & Shim, J.-S. (2006), A two-phase local server security model based on xml certificate, *in* 'Computational Science and Its Applications — ICCSA 2006', Vol. 3984/2006, Springer Berlin / Heidelberg, pp. 968–978.

Kubbilun, W., Gajek, S., Psarros, M. & Schwenk, J. (2005), Trustworthy verification and visualisation of multiple xml-signatures, *in* 'Communications and Multimedia Security', Vol. 3677/2005, Springer Berlin / Heidelberg, pp. 311–320.

Lee, J. S., Moon, K. Y. & Sohn, S. W. (2002), Eses/signature and its applications for secure data exchange, *in* 'IEEE 5th International Workshop on Networked Appliances', IEEE Computer Society, pp. 45–50.

Lee, J., Upadhyaya, S. J., Rao, H. R. & Sharman, R. (2005), 'Secure knowledge management and the semantic web', *Commun. ACM* **48**(12), 48–54.

Lee, S.-H., Choi, B.-S., Lee, J.-S., Moon, K.-Y. & Lee, J.-K. (2006), Vo authentication framework in grid environment using digital signature, *in* 'Computational Science and Its Applications - ICCSA 2006', Vol. 3981/2006, Springer Berlin / Heidelberg, pp. 945–953.

Lee, S.-M., Kwon, O.-S., Lee, J.-H., Oh, C.-J. & Ko, S.-H. (2003), Ty*securews: An integrated web service security solution based on java, *in* 'E-Commerce and Web Technologies', Vol. 2738/2003, Springer Berlin / Heidelberg, pp. 186–195.

Lim, H.-Y., Kim, Y.-G., Moon, C.-J. & Baik, D.-K. (2005), Bundle authentication and authorization using xml security in the osgi service platform, *in* 'ICIS '05: Proceedings of the Fourth Annual ACIS International Conference on Computer and Information Science (ICIS05)', IEEE Computer Society, pp. 502–507.

Lu, E. J.-L. & Chen, R.-F. (2004), 'An xml multisignature scheme', *Applied Mathematics and Computation* **149**(1), 1–14.

Lu, W., K.Chiu, A.Slominski & D.Gannon (2005), A streaming validation model for soap digital signature, *in* '14th IEEE International Symposium on High Performance Distributed Computing, HPDC-14', IEEE Computer Society, pp. 243–252.

Ma, J. & Nickerson, J. V. (2006), 'Hands-on, simulated, and remote laboratories: A comparative literature review', *ACM Comput. Surv.* **38**(3), 7.

McIntosh, M. & Austel, P. (2005), Xml signature elent wrapping attacks and countermeasures, *in* 'SWS '05: Proceedings of the 2005 workshop on Secure web services', ACM Press, pp. 20–27.

Mohammed, S. M. & Fiaidhi, J. A. (2005), Developing secure transcoding intermediary for svg medical images within peer-to-peer ubiquitous environment, *in* 'CNSR '05: Proceedings of the 3rd Annual Communication Networks and Services Research Conference (CNSR05)', IEEE Computer Society, pp. 151–156.

Nair, G. G., Gopalakrishnan, A., Mauw, S. & Moll, E. (2005), Xml security in the next generation optical disc context, *in* 'Secure Data Management', Vol. 3674/2005, Springer Berlin / Heidelberg, pp. 217–233.

Oliveira, E., Z.Abdelouahab & D.Lopes (2006), Security on mass with xml security specifications, *in* '17th International Conference on Database and Expert Systems Applications, DEXA'06', IEEE Computer Society, pp. 5–9.

Park, N., Kim, H., Chung, K., Kim, S. & Won, D. (2005), Xkms-based key management for open lbs in web services environment, *in* 'Advances in Web Intelligence', Vol. 3528/2005, Springer Berlin / Heidelberg, pp. 367–373.

Park, N., Kim, H., Chung, K., Sohn, S. & Won, D. (2006), Xml-signcryption based lbs security protocol acceleration methods in mobile distributed computing, *in* 'Computational Science and Its Applications — ICCSA 2006', Vol. 3984/2006, Springer Berlin / Heidelberg, pp. 251–259.

Park, N., Moon, K., Jang, J. & Sohn, S. (2004*a*), Development of xkms-based service component for using pki in xml web services environment, *in* 'Computational Science and Its Applications — ICCSA 2004', Vol. 3043/2004, Springer Berlin / Heidelberg, pp. 784–791.

Park, N., Moon, K., Jang, J. & Sohn, S. (2004*b*), Middleware framework for secure grid application in mobile web services environment, *in* 'Grid

and Cooperative Computing — GCC 2004 Workshops', Vol. 3252/2004, Springer Berlin / Heidelberg, pp. 406–413.

Park, N., Moon, K., Jang, J. & Sohn, S. (2004*c*), A xkms-based security framework for mobile grid into the xml web services, *in* 'Computational Science - ICCS 2004', Vol. 3038/2004, Springer Berlin / Heidelberg, pp. 124–132.

Park, N., Moon, K., Jang, J., Sohn, S. & Won, D. (2005), Implementation of streamlining pki system for web services, *in* 'Computational Science and Its Applications — ICCSA 2005', Vol. 3480/2005, Springer Berlin / Heidelberg, pp. 609–618.

Park, N., Moon, K., Kim, H., Chung, K. & Sohn, S. (2005), An effiecient software-based security acceleration methods for open lbs services, *in* 'Geoscience and Remote Sensing Symposium. IGARSS '05', IEEE Computer Society, p. 4pp.

Park, N., Moon, K. & Sohn, S. (2003), Certificate validation service using xkms for computational grid, *in* 'XMLSEC '03: Proceedings of the 2003 ACM workshop on XML security', ACM Press, pp. 112–120.

Park, N., Moon, K. & Sohn, S. (2004), A study on xkms-based key management system for secure global xml web services, *in* 'The 6th International Conference on Advanced Communication Technology', Vol. 1, IEEE Computer Society, pp. 492–495.

Park, N., Moon, K., Sohn, S. & Park, C. (2004), Certificate validation scheme of open grid service usage xkms, *in* 'Grid and Cooperative Computing', Vol. 3032/2004, Springer Berlin / Heidelberg, pp. 849–858.

Polivy, D. J. & Tamassia, R. (2002), Authenticating distributed data using web services and xml signatures, *in* 'XMLSEC '02: Proceedings of the 2002 ACM workshop on XML security', ACM Press, pp. 80–89.

Project, P. I. . A. L. (2007), 'Wireless internet access'. http://www.pewinternet.org/pdfs/PIP_Wireless.Use.pdf.

Schadow, D. (2005), Experience xml security, *in* 'Communications and Multimedia Security', Vol. 3677/2005, Springer Berlin / Heidelberg, pp. 321–329.

Shirasuna, S., Slominski, A., Fang, L. & Gannon, D. (2004), Performance comparison of security mechanisms for grid services, *in* 'Fifth

IEEE/ACM International Workshop on Grid Computing', IEEE Computer Society, pp. 360–364.

Sun, L. & Li, Y. (2005), Xml undeniable signatures, *in* 'International Conference on Computational Intelligence for Modelling, Control and Automation 2005 and International Conference on Intelligent Agents, Web Technologies and Internet Commerce', Vol. 1, IEEE Computer Society, pp. 981–985.

Takase, T., Uramoto, N. & Baba, K. (2002), Xml digital signature system independent of existing applications, *in* 'Symposium on Applications and the Internet (SAINT) Workshops', IEEE Computer Society, pp. 150–157.

Wei, L., Chiu, K., Slominski, A. & Gannon, D. (2005), A streaming validation model for soap digital signature, *in* 'Proceedings. 14th IEEE International Symposium on High Performance Distributed Computing', pp. 243–252.

Yang, Y., Ng, W., Lau, H. L. & Cheng, J. (2006), An efficient approach to support querying secure outsourced xml information, *in* 'Advanced Information Systems Engineering', Vol. 4001/2006, Springer Berlin / Heidelberg, pp. 157–171.

Zhang, S., Wang, B. & Zhou, L. (2004), Constructing secure web service based on XML, *in* 'Grid and Cooperative Computing', Vol. 3032/2004, Springer Berlin / Heidelberg, pp. 1051–1054.