XML A BEZPEČNOST

XML AND SECURITY

Dagmar Brechlerová

Anotace:
Bezpečnostní rysy XML se bouřlivě rozvíjejí. Patří sem vývoj digitálního podpisu XML dokumentů (XML DSIG), který má řadu výhod. Pro utajení je nutno použít XML šifrování, které také prošlo významným vývojem. Dalším bezpečnostním rysem, kterému je v současné době věnována velká pozornost, je řízený přístup do XML dokumentů. Ten umožňuje, aby jednotliví uživatelé po autentizaci měli přístup pouze do určité části tohoto XML dokumentu.

Klíčová slova:
XML, bezpečnost, digitální podpis, autentizace, šifrování

Abstract:
XML is not only static standard for document but now it is a standard for data exchange, too. Security of XML is a very important reason for XML. This paper is about new security attributes of XML (digital signature, encryption and authentication).

Keywords:
XML, security, digital signature, authentisation, encryption

ÚVOD

Bezpečnost hraje při používání výpočetní techniky stále větší roli. Mezi velmi významné bezpečnostní funkce patří digitální podpis, šifrování a autentizace. Následující text podává stručný přehled o nejnovějších trendech v této oblasti ve spojení s technologií XML. XML se stává stále více standardem pro výměnu dokumentů např. obchodního rázu. Rozvoj uvedených bezpečnostních rysů v XML je významným kvalitativním krokem vpřed, neboť spojení těchto technologií s XML umožňuje některé dosud nemožné způsoby užití.

CÍL A METODIKA

Cílem práce je podat přehled nejnovějších trendů v této oblasti a upozornit na stav jejich vývoje a možné použití. Jako metodika byla zvolena zejména studium literatury, zdrojů na Internetu a informací z konferencí.

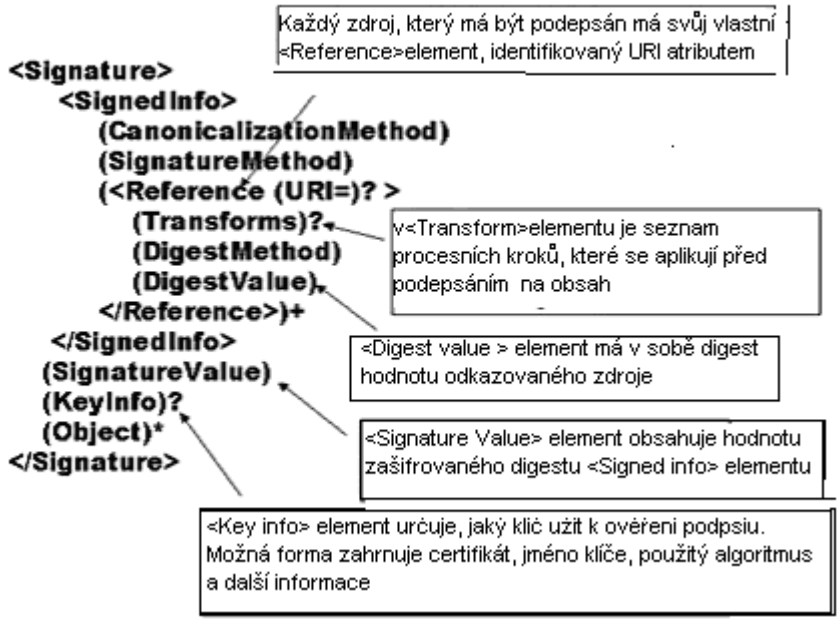
Současná situace

Použití digitálního podpisu prošlo v posledních letech bouřlivým vývojem a to jak z hlediska použitých technologií tak i s tím spojených právních předpisů. Digitální podpis je důležitý z toho hlediska, že poskytuje garanci integrity vzkazu tzv. “end to end” a dále poskytuje autentizační informaci ohledně původce vzkazu. Na rozdíl od SSL, které také poskytuje integritu vzkazu (a navíc soukromí), trvá zde kontrola integrity trvale. U SSL trvá pouze po dobu dopravy vzkazu mezi koncovými body.

DIGITÁLNÍ PODPIS

Mezi nejvýznamnější čin poslední doby patří vývoj digitálního podpisu XML dokumentů tzv. XML DSIG. Pro vývoj syntaxe a procesní specifikace se spojily organizace W3C a IETF. Tyto společné snahy vyústily v doporučení a normalizaci digitálního podpisu XML. XML podpis tedy definuje syntaxi a zapracování podpisu. Ze tří základních bezpečnostních požadavků - autentizace, integrita a důvěrnost – pokrývá digitální podpis první dvě. Pro utajení je nutno použít XML šifrování, které také prošlo významným vývojem. Podrobný popis možno nalézt na stránkách [2] a [6]. Celkem srozumitelné vysvětlení jak XML šifrování tak i XML podpisu je v článku [4].

Digitální podpis XML používá pro podpis běžného postupu, tj. nejdříve se vytváří hash vzkazu, tento hash součet se poté zašifruje privátním klíčem podepisujícího a definovaným způsobem se připojí ke vzkazu. Ovšem podepisování v XML má oproti podepisování např. wordovského dokumentu zcela zásadní výhodu, jednak se dá skutečně přesně definovat, co se podepisuje (což je u wordovských dokumentů vždy problém), jednak se dají podepisovat pouze jednotlivé části dokumentu. Vzhledem k rozsahu příspěvku zde není možné rozebírat dopodrobna schéma podpisu, jedná se o poměrně komplikovanou a rozsáhlou záležitost. Je tedy možné podepsat pouze přesně definovanou část dokumentu pomocí výběru části dokumentu XPath. Je možné, aby jednu část dokumentu podepsalo více lidí. XML DSIG podporuje navíc širokou škálu typů klíčů a klíčové infrastruktury, jako jsou např. X.509 certifikáty. Podrobný popis je možno nalézt na stránkách [3].
Možnost použití v praxi je tedy taková, že různí lidé podepisují různé části dokumentu v různé době, každý podepisuje pouze tu část, která mu náleží. Stejně tak díky vlastnostem digitálního podpisu je zaručena integrita určité části XML dokumentu, zatímco jiné části se mění. XML podpis je možno použít na různé typy zdrojů, je možno podepsat jak HTML data, JPG data, XML data a specifickou část XML souboru. Navíc výběr algoritmů a metod je velmi široký.
Následující obrázek ukazuje, jak vlastně takový digitální podpis XML vzniká. Jsou přidávány další elementy s přesně definovaným obsahem, které podávají jednak informace o vlastních výsledcích a mezivýsledcích podpisu a jednak o použitém klíči, transformačních krocích atd. XML dokument může tedy mít podpis přímo jako jednu ze svých částí.



Praktické použití můžeme demonstrovat např. na užití v universitních systému. Např. pokud by se někdy v budoucnu přešlo k elektronickým výkazům o studentovi (elektronický index), je jasné, že každý pedagog by chtěl podepsat pouze informace, které tam vložil on. Stejně tak by digitální podpis zaručil, že příslušná část indexu nebyla změněna. Nemusí jít přímo o index, ale o celkové informace o studentovi, které jsou o studentovi pořizovány během studia a vlastně s ním putují po celou dobu studia. Ovšem zde nutno upozornit na s tím spojené právní předpisy, které zatím řadu takových věcí znemožňují. Na rozdíl od dříve používaného podepisování např. wordovských dokumentů, není zde problém podepisovat přesně určené části XML dokumnetu. V elektronických vyučovacích materiálech by se stejně tak dalo použít podepisování jednotlivých částí, částí které přibývají nebo jsou měněny apod.

Šifrování v XML

Jde vlastně o použití obdobné technologie jako u podpisu, pouze za opačného použití klíčů. Opět se jedná o standard, jak data zašifrovat a uložit do XML. Stejně jako u podpisu jde šifrovat: libovolná data, XML dokument, XML element, obsah XML elementu. Je opět podporováno několik algoritmů.

Následující ukázka, převzatá ze stránky [5], ukazuje, kterak jsou přidávány další elementy obsahující jednak informace o podepisovaném dokumentu, metodě podepisování atd.

```
<?xml version='1.0'?>
  <PaymentInfo xmlns='http://example.org/paymentv2'>
    <Name>John Smith</Name>
    <CreditCard Limit='5,000' Currency='USD'>
      <Number>
        <EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
         Type='http://www.w3.org/2001/04/xmlenc#Content'>
          <CipherData>
            <CipherValue>A23B45C56</CipherValue>
          </CipherData>
        </EncryptedData>
      </Number>
      <Issuer>Example Bank</Issuer>
      <Expiration>04/02</Expiration>
    </CreditCard>
      </PaymentInfo>
```

Řízený přístup

Dalším bezpečnostním rysem XML, kterému je v současné době věnována velká pozornost, je řízený přístup do XML dokumentů. Řízený přístup do XML dokumentů umožňuje, aby jednotliví uživatelé po autentizaci do daného XML dokumentu měli přístup pouze do určité části tohoto XML dokumentu. Např. se bude jednat o záznam o pacientovi, poté je možné, aby jinou část viděl lékař, jinou sestra, jinou další personál atd. To je samozřejmě velmi zajímavé z hlediska ochrany citlivých a osobních údajů, u kterých je dobré, aby se s nimi do kontaktu dostalo co nejméně osob. XML dokument se tedy posunul od standardu orientovaného na statický dokument ke standardu pro výměnu dat.

Pro použití přístupu do XML dokumentu je nejprve nutno vybudovat model objektů, které přistupují a subjektů, ke kterým je přistupováno. Jedná se o standardní postup z oboru počítačové bezpečnosti. Autorizace se specifikuje buď pro jednotlivé subjekty (což je neúnosně namáhavé) nebo pro skupiny subjektů, případně se zavádí určitá hierarchie subjektů. Můžeme zavést hierarchii např. podle lokalizace subjektu apod. Také objekty musejí být identifikovány, používají se X Path výrazy. Tyto snahy vyústily v poslední době

opět v normalizaci XACML, která byla publikována teprve v tomto roce (únor 2004 - eXtensible Access Control Markup Language).[1]

Rozsah článku opět neumožňuje podrobný popis použitých prostředků, proto se soustředíme na jejich praktický dopad v universitním prostředí. Řekněme, že pro určitého studenta bude veden dokument, ke kterému mají mít přístup pracovnice studijního oddělení, jednotliví pedagogové, samotný student atd. Potom pomocí vhodně vybudovaného modelu je možné, že každý z těchto výše uvedených uživatelů bude vidět něco jiného, je navíc možné vhodným propracováním systému dosáhnou toho, že z různých míst bude možno vidět něco jiného. Tedy např. je možno rozlišit, zda se student připojuje k IS školy z domova nebo z koleje nebo učeben školy.
Význam např. pro e-learning je obrovský, bude možno vytvořit jedny materiály a poté rozlišovat, co uvidí studenti jednotlivých ročníků atd. V budoucnosti lze od této technologie očekávat velké využití.

ZÁVĚR - DISKUSE

Výše uvedený krátký text chtěl pouze upozornit na některé bezpečnostní rysy XML. Řada těchto vlastností je teprve ve fázi vývoje či normalizace. Ale v krátké době se dá očekávat rozvoj využití těchto vlastností a domníváme se, že např. pro digitální podpis teprve těmito možnostmi nastane skutečný rozvoj. Pro některé výše uvedené technologie je již dosažitelný SW, jiné jsou teprve ve stadiu vývoje a normalizace.

Literatura:

[1] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
[2] http://www.w3.org/TR/xmlenc-core/
[3] http://www.w3.org/TR/2001/PR-xmldsig-core-20010820/
[4] http://www-106.ibm.com/developerworks/xml/library/s-xmlsec.html/index.html
[5] http://badame.vse.cz/izi238/slidy/xmisc/frames.html
[6] http://www.w3.org/Signature/#Code

Kontaktní adresa autora:

RNDr. Dagmar Brechlerová, KIT PEF ČZU Praha, Kamýcká ul., 165 21, tel. 22438 2356,
Brechlerova@pef.czu.cz