第 34 卷 第 11 期 计 算 机 工 程 2008 年 6 月
Vol.34 No.11 Computer Engineering June 2008
·安全技术· 文章编号：1000—3428(2008)11—0137—03 文献标识码：A 中图分类号：TP393.08

基于 XACML 的 Web 服务信任协商方案

王尚平，马宏亮，张亚玲，王晓峰
(西安理工大学密码理论与网络安全研究室，西安 710048)

摘 要：针对 Web 服务中首次建立双方信任的问题，提出一种基于 XACML 的 Web 服务信任协商建立方案。利用 XACML 访问控制构建信任模型，给出信任协商策略描述，建立起基于 XACML 的信任协商架构，利用 XML 加密和签名来保证端到端的安全，提高了相互信任和策略的安全性。

关键词：Web 服务；可扩展访问控制标记语言；信任协商；协商策略

Scheme of Trust Negotiation for Web Services Based on XACML

WANG Shang-ping, MA Hong-liang, ZHANG Ya-ling, WANG Xiao-feng
(Lab of Cryptography and Network Security, Xi'an University of Technology, Xi'an 710048)

【Abstract】 Aiming at how to establish firstly among Web services, a new trust negotiation scheme for Web services based on eXtensible Access Control Markup Language (XACML) is proposed. The trust model is constructed by using of XACML, and the description of negotiation strategies is provided, so the trust negotiation scheme based on XACML is fully built. The end-to-end security is protected with XML encryption and signature. The new scheme can be used to improve the security of trust among Web services and negotiation strategies.

【Key words】 Web services; eXtensible Access Control Markup Language(XACML); trust negotiation; negotiation strategies

1 概述

在跨信任域的开放式Web服务环境下，双方在第 1 次交互时，一般互不相信对方，因此，信任协商就显得尤其重要。但在确立双方之间的信任关系期间，敏感的访问控制策略和证书可能包含敏感信息。例如：A 国家制定了一项秘密联合军事演习计划，议定只有B 国家的国防部长才能访问 A 国家的专用资源 R。访问控制策略为 $R \leftarrow Cert_{dod}$，其中，$Cert_{dod}$ 为B 国家的国防部长所持有的证书。如果随意公开 $Cert_{dod}$ 和访问控制策略，那A国家的秘密合作方B国家将被暴露(disclosure)，因此如何保护这些敏感的证书、访问控制策略的私密性已经成为信任协商中的一个重要问题[1]。

近年来比较有影响的信任协商模型有Trust-X, TrustBuilder 2 种[2-3]。其中，Trust-X框架的优点是通过对证书的缓存来提高协商效率，但容易遭受拒绝服务攻击，协商策略语言是X-TNL；TrustBuilder是一个较成熟的用Java语言编写的信任协商中间件，优点是采用TNT协议提高信息传输的安全性，但对于拒绝服务攻击仍无能为力，其协商策略语言为TPL。可以看出，SSL/TLS协议的安全只能到达传输层，在应用层是不安全的，而且协商策略语言的相异导致互操作性的困难。本文旨在利用XACML访问控制模型来构建信任模型，并把XACML作为协商策略语言，通过对XML加密和签名达到应用层级别的安全，适合基于XML的Web服务信任协商建立。

2 相关知识

2.1 XACML 访问控制模型

根据OASIS发布XACML 2.0 规范[4]，XACML访问控制模型中的逻辑组件以及组件间的数据交互如图 1 所示。SunXACML[5]是该模型的一个开源实现，本文将利用此模型来构建访问控制层。

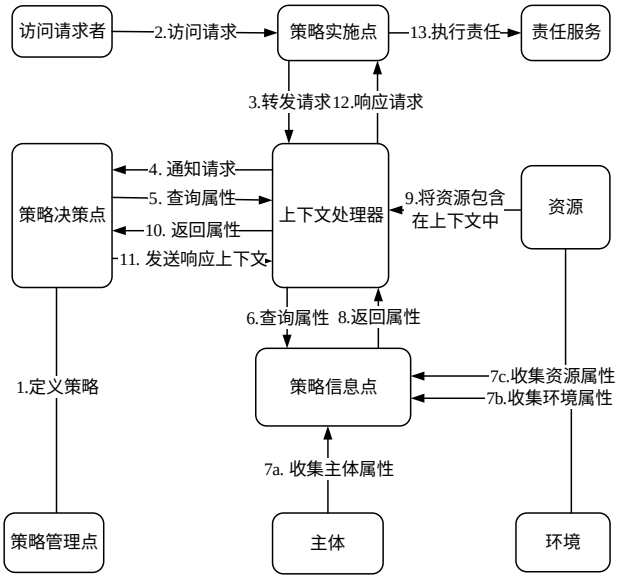

图 1 XACML 访问控制模型的数据流图

2.2 协商策略构造

定义 1[6] 对资源R来说，满足以下的条件：

(1)树的根代表要访问的资源；

(2)除去根，树的每个节点代表一个证书。当上下文清楚后，通过证书的名字来指向将要暴露的节点；

基金项目：国家自然科学基金资助项目(60273089)；陕西省科学研究计划基金资助项目(2006F37)

作者简介：王尚平(1963－)，男，教授、博士，主研方向：密码理论，网络安全；马宏亮，硕士；张亚玲、王晓峰，副教授、在职博士研究生

收稿日期：2007-06-24 **E-mail：**kassymhl999@126.com

(3)任一节点 C 的子树是来自 C 的一个最小解决方案集。则称 T 是一颗暴露树。当 T 的所有叶子是未保护的证书，称 T 为一棵完全暴露树。给定一棵暴露树 T，如果某一证书在从叶子到根的路径中出来 2 次，则 T 是一棵冗余暴露树。

定义 2[6] 给定被保护资源R的暴露序列 $G=(C_1,C_2,\cdots,C_n)$，如果对每个 C_i，在它们暴露的时候是公开的，则称G为一个安全暴露序列。

定理 1[6] 给定一个非冗余的安全暴露序列 $G=(C_1,C_2\cdots,C_n=R)$，必存在一个完全非冗余的暴露树T满足以下 2 个特性：

(1)T 的节点是 $(C_1,C_2\cdots,C_n)$ 的子集；

(2)在 T 中，对满足 C_1' 是 C_2' 祖先的所有的证书对 (C_1',C_2')，则在 G 中，C_2' 先于 C_1' 暴露。

定理 2[6] 如果找到一个安全暴露序列满足 $C_n=R$，则信任协商成功建立。

3 基于 XACML 的 Web 服务信任协商方案

3.1 信任协商建立

3.1.1 符号说明

C：代表服务请求者；

S：代表服务提供者；

R：代表被请求的资源；

T：代表时间戳；

$i.Policy$：代表通信方 i 的策略；

$Request(R)$：代表对 R 的请求；

$Permit(R\leftarrow C,T),\ Sign_S\{Permit(R\leftarrow C,T)\}$：代表 S 授权 C 对 R 的访问；

$Cert_i$：代表通信方 i 的 x509v3 证书；

PK_i：代表包含在通信方 i 的 x509v3 证书中的公钥；

SK_i：代表通信方 i 对应于公钥 PK_i 的私钥；

$Sign_i\{\cdots\}$：代表通信方 i 的签名；

$E_{PK_i}(\cdots)$：代表用通信方 i 的公钥加密的信息；

$D_{SK_i}(\cdots)$：代表用通信方 i 的私钥解密的信息；

$VerifyCert(Cert_i)$：代表对通信方 i 的证书的验证操作；

$VerfiySign(PK_i,Sign_i(\cdots))$：代表用通信方 i 的公钥验证数字签名 $Sign_i\{\cdots\}$ 的操作；

$FindCert(Cert_i)$：代表在 $(C_1,C_2,\cdots,C_n)$ 中查找通信方 i 的证书；

$Evaluate(Cert_C,S.Policy)$：代表用 $S.Policy$ 来评估 $Cert_C$；

$Evaluate(Cert_S,S.Policy,C.Policy)$：代表用 $C.Policy$ 来评估 $Cert_S$ 和 $S.Policy$。

3.1.2 信任协商建立步骤

给定安全暴露序列 $G=(C_1,C_2,\cdots,C_n=R)$，信任协商步骤建立如下：

(1) $C\rightarrow S:\{Request(R),T\},\ Sign_C\{Request(R),T\},Cert_C$

C 首先向 S 发出消息 $Request(R)$，请求必须携带 $Sign_C\{\cdots\}$，同时带有 T 和请求者认为可暴露的 $Cert_C$。

(2) $S:VerifyCert(Cert_C),\ VerfiySign(PK_C,Sign_C(Request(R),T)),\ FindCert(Cert_C),Evaluate(Cert_C,S.Policy)$

S 验证 $Cert_C$，若证书失效，则立即终止会话；否则用 PK_C 验证 $Sign_C\{\cdots\}$，然后与 $(C_1,C_2\cdots,C_n)$ 进行比对，如果不在此序列中，立即结束会话。如果满足 $Cert_C=C_n=R$ 则转向(7)，否则转向(3)。

(3) $S\rightarrow C:\{E_{PK_C}(S.Policy),T\},\ Sign_S\{E_{PK_C}(S.Policy),T\},Cert_S$

S 向 C 发送 $S.Policy$，要求其提供下一个证书，载有敏感暴露策略的消息将被加密 $E_{PK_C}(\cdots)$ 和签名。

(4) $C:VerifyCert(Cert_S),\ VerfiySign\begin{pmatrix}PK_S,\\ Sign_S\{E_{PK_C}(S.Policy),T\}\end{pmatrix},\ D_{SK_C}(E_{PK_C}(S.Policy)),\ Evaluate(Cert_S,S.Policy,C.Policy)$

C 验证 $Cert_S$，若证书失效，则立即终止会话；否则用 PK_S 验证 $Sign_S\{\cdots\}$，然后解密消息，送往信任处理器，信任处理器转换格式后给信任决策点，信任决策点评估 $S.Policy$ 和 $Cert_S$，决定是否把 S 所要请求的证书 $Cert_C'$ 返回给服务端，如果拒绝，则结束会话。否则转向(5)。

(5) $C\rightarrow S:\{E_{PK_S}(Cert_C'),T\},\ Sign_C\{E_{PK_S}(Cert_C'),T\}$

C 向 S 发送 $Cert_C'$，载有敏感 $Cert_C'$ 的消息将被加密并用 $Cert_C$ 作签名。

(6) $S:VerfiySign(PK_C,Sign_C\{E_{PK_S}(Cert_C'),T\}),\ D_{SK_S}(E_{PK_S}(Cert_C')),VerifyCert(Cert_C'),\ FindCert(Cert_C'),\ Evaluate(Cert_C',S.Policy)$

S 验证 $Sign_C\{\cdots\}$，解密消息，进而验证 C 的证书 $Cert_C'$，若证书失效，则立即终止会话；否则与 $(C_1,C_2\cdots,C_n)$ 进行比对。如果不在此序列中，立即结束会话，否则如果评估后满足 $C_n=R$ 则转向(7)，否则转向(3)。

(7) $S\rightarrow C:\{E_{PK_C}(Permit(R\leftarrow C,T))\},\ Sign_S\{E_{PK_C}(Permit(R\leftarrow C,T))\}$

根据定理 2，当满足 $C_n=R$ 时，信任协商建立，C 被授权访问 R。

(8) $C\rightarrow R:Permit(R\leftarrow C,T),\ Sign_S\{Permit(R\leftarrow C,T)\}$

C 提交 $\begin{matrix}Permit(R\leftarrow C,T),\\ Sign_S\{Permit(R\leftarrow C,T)\}\end{matrix}$ 访问 R。

3.1.3 XACML 信任协商架构

基于 XACML 访问控制模型，给出 XACML 信任协商架构如图 2 所示。利用访问控制层的属性查找模块作为与信任协商层的接口，属性查找模块负责查找那些没有包含在起始请求上下文中的属性；处于信任协商层的信任授权服务处理器负责把 XACML 的核心内容与自动信任系统中保护敏感信息的模块进行无缝的整合。在信任授权服务处理器中，协商协议模块处理在建立信任关系过程中的信任协商协议以及消息序列，证书验证模块通过证书链遍历，检查 X.509v3 证书是否被撤消；然后它们被送往信任的策略决策点，信任处理

器用来规范从信任策略决策点中出入请求响应格式，信任决策点通过对接收到的证书和本地策略以及接收到的策略与本地证书进行对比来处理信任访问管理决策，通过遍历本地的策略或证书来与接收到的证书或策略进行比对，进而决定是否进一步地暴露给对方属于自己的证书或策略；处于最底层双方的通信协议为绑定在 HTTP 之上的 SOAP 协议，通过 WS-Security 来对 SOAP 消息进行加密和签名，加密和签名及 X.509v3 证书信息处于 SOAP 消息的<header>元素中。

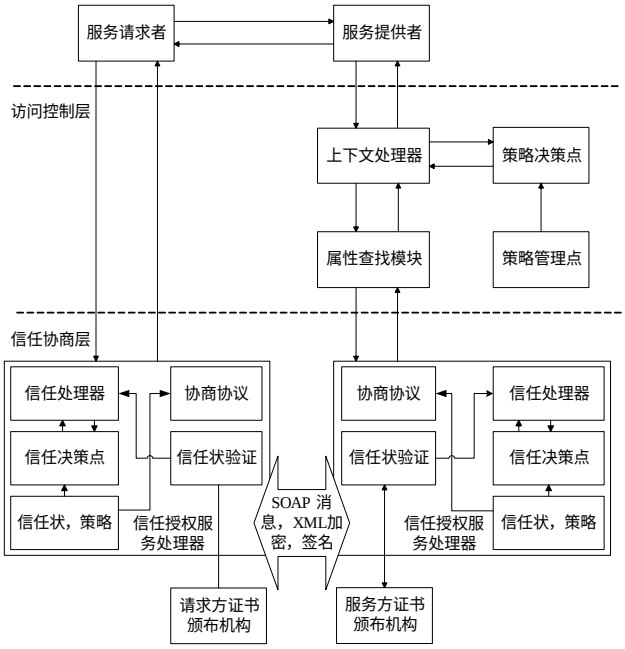

图 2　XACML 信任协商架构

3.2　XACML 协商策略语言

虽然 XACML 本身并不是专门用作协商策略描述的语言，但 XACML 适宜作为一种新的协商策略语言。例如，可用一个策略集代表一棵暴露树，暴露树的根为<Policyset>元素，子元素<Target>作为私密证书和策略暴露的前提条件。策略集中的每个策略<Policy>可以用来表示详细的暴露策略，证书暴露的顺序可以用<Policy>元素的一个属性 PolicyId 规定。例如，有如下的策略文件：

```
<PolicySet>
<Target>
…
</Target>
<PolicyIdReference>
urn:oasis:names:tc:xacml:2.0:server:policyid:3
</PolicyIdReference>
<Policy PolicyId="urn:oasis:names:tc:xacml:2.0:server:policyid:1"
<Target>
…
</Target>
</Policy>
<Policy
PolicyId="urn:oasis:names:tc:xacml:2.0:server:policyid:2">
<Target>
…
</Target>
</Policy>
<Policy
PolicyId="urn:oasis:names:tc:xacml:2.0:server:policyid:3">
<Target>
…
</Target>
</Policy>
</PolicySet>
```

假设有某策略是敏感的，而又不希望该策略暴露给陌生人，则 XACML 提供了良好的层次控制保护策略及证书。具体实例如下：假设 PolicyId 为 urn:oasis:names:tc:xacml:2.0:Server:policyid:3 所描述的策略是“只有 B 国家的国防部长才能访问 A 国家的专用资源 R”。笔者认为这条策略是敏感的，不希望暴露给陌生人，则策略的敏感性可以由 PolicyId 为 urn:oasis:names:tc:xacml:2.0:Server:policyid:2 所控制，即：“只有 B 国家国防部的人员才能访问 A 国家的专用资源 R”，即请求方必须提供国防部的证书 $Cert_{\text{Depofdefence}}$；且这条策略又由 PolicyId 为 urn:oasis:names:tc:xacml:2.0:Server:policyid:1 控制，即“只有 B 国家部级机构才能访问 A 国家的专用资源 R”。请求方必须提供部级机构的证书 $Cert_{\text{DepofCcountry}}$。根据定理 1，有安全暴露序列 $\{Cert_{\text{dod}}, Cert_{\text{Depofdefence}}, Cert_{\text{DepofCcountry}} = R\}$，最后当提交了 B 国家国防部长的证书 $Cert_{\text{dod}}$，满足 $R \leftarrow Cert_{\text{dod}}$，信任成功建立。

4　安全性分析

对信任协商建立的主要安全威胁有探测攻击、分布式拒绝服务功击、中间人攻击等，下面分别针对这 3 种常见攻击进行系统的安全性分析。

(1)探测攻击

敌手通过试探的方法来获取私密的策略。敌手随机提交一个证书，根据服务器所返回的信息来得到有关私密策略的信息。本方案采取的是一种非常谨慎的方式，将保护拥有敏感证书的策略迁移到其他可公开暴露的策略之上，然后以渐增的方式暴露私密策略。因此，最大限度地保护了私密策略。

(2)分布式拒绝服务攻击

信任协商是一个代价较为昂贵的过程，如果敌手以不同的 IP 发送大量的请求，或是发送大量的无关证书，则信任协商的效率会急剧下降。在本文的方案中，访问控制层充当一个代理，请求方发送的证书必须与策略严格对应，否则立即终止协商会话，从而有效地降低了分布式拒绝服务攻击的风险。在原型系统的设计中，实现了这些安全措施，很好地保护了信任协商系统。例如，C 发出一个 SOAP 请求，S 在访问控制层首先进行验证，如果没有通过验证则返回错误消息并终止会话，如下所示。

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope
xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:enc="http://schemas.xmlsoap.org/soap/encoding/">
<env:Body>
<env:Fault>
<faultcode
xmlns:ans1="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss
-wssecurity-secext-1.0.xsd">ans1:InvalidSecurityToken</faultcode>
<faultstring>Certificate validation failed</faultstring>
</env:Fault>
</env:Body>
</env:Envelope>
```

（下转第 142 页）