

Web 服务攻击技术研究

吴明峰^{1,2}, 张永胜^{1,2}, 李园园^{1,2}, 韩艳梅³

- (1. 山东师范大学 信息科学与工程学院, 山东 济南 250038;
2. 山东省分布式计算机软件新技术重点实验室, 山东 济南 250038;
3. 聊城大学 计算机学院, 山东 聊城 252004)

摘要: Web 服务具有平台无关性、动态性、开放性和松散耦合等特征, 这给基于异构平台的应用集成带来极大便利, 使越来越多的企业使用 Web 服务。Web 服务技术在得到快速发展和应用的同时, 它的安全问题越来越重要, 成为黑客或者攻击者选择的目标, Web 服务提供者对于保证 Web 服务安全要面临着严峻的考验。文中分析了 Web 服务攻击技术的特点、原理, 讨论了用于攻击基于 XML 的 Web 服务的各种技术和目前比较流行的防御措施。进一步讨论了 Web 服务攻击将来的研究方向以及面临的挑战。

关键词: Web 服务; 攻击; 安全; 防御

中图分类号: TP309

文献标识码: A

文章编号: 1673-629X(2012)01-0213-04

Research of Web Services Attack Technology

WU Ming-feng^{1,2}, ZHANG Yong-sheng^{1,2}, LI Yuan-yuan^{1,2}, HAN Yan-mei³

- (1. School of Information Science and Engineering, Shandong Normal University, Jinan 250038, China;
2. Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, Jinan 250038, China;
3. School of Computer, Liaocheng University, Liaocheng 252004, China)

Abstract: Web service is characterized by its platform-independence, dynamic, openness and loose coupling. These characteristics greatly facilitate the application-to-application integration based on heterogeneous platform, that an increasing number of enterprise use it. Along with the development of Web services, its safe problem is more and more important. Web service art is attracting attackers and hackers to attack the Web services and the servers on which they run. Organizations are therefore facing the challenge of implementing adequate security for Web services. It detailedly analyzed the characteristics and principle of various attacks on Web service, and pointed out the corresponding detection and prevention countermeasures. On the basis of current research achievements, also presented a discussion on the future research directions and the challenges of Web service defenses against attacks.

Key words: Web service; attacks; security; defence

0 引言

Web 服务是一种基于 XML (eXtensible Markup Language) 的软件系统, 是一种支持机器到机器间互操作新的 Web 应用。其具有自包含、自描述以及模块化应用的特点, 可以发布在 Web 服务、被发现与使用^[1], 即将成为从 B2C (Business to Consumer) 到 B2B (Business to Business) 商业模式转变的关键技术。Web 服务减少了人为干预, 极大的提高了生产效率。然而计算机安全问题成为制约电子商务发展的瓶颈, 例如: 数

据篡改、窃听、未授权访问等。为此采用了安全措施^[2] 比如: 防火墙、访问控制、侵入检测系统、病毒发现、数字证书数据加密。然而这些办法还不能解决 Web 服务面临的很多安全问题。为此微软提出了一系列的安全规范, 如 Ws - Security^[3]、Ws - Trust^[4]、WS - Secure Conversation 等, 这些标准虽然解决了安全问题, 例如: 保证了 SOAP 消息端到端的安全性, 但是所使用的一些支撑技术如 XML, SOAP^[5], WSDL 和 UDDI^[6] 存在安全漏洞, 导致了一些新的 Web 服务攻击。比如 XML 注入攻击、数据过度加密攻击^[7] 等。文中介绍了常见的 Web 服务攻击的形式、攻击原理和防御方法。

1 Web 服务攻击

1.1 基于 XML 拒绝服务攻击 (XDoS)

XDoS^[8] 是通过消耗 Web 服务器主机的资源 (包

收稿日期: 2011-06-10; 修回日期: 2011-09-15

基金项目: 山东省自然科学基金 (ZR2011FM019)

作者简介: 吴明峰 (1985-), 男, 山东枣庄人, 硕士研究生, 研究方向为 Web 服务安全; 张永胜, 教授, 硕士, 研究方向为 Web 服务安全、软件工程环境。

括内存、处理器、网络带宽等)来达到削弱 Web 服务的可用性及其服务质量的目的。有下列几种攻击方式:

1) 重放攻击。

攻击者发送大量重复的 SOAP 消息,超出服务器的处理能力,常会导致机器无法作出响应,甚至会导致系统崩溃。由于 HTTP 请求包 XML 格式良好,IP 地址和网络数据包都是合法的,导致了要发现这种攻击行为是很困难。

2) 递归的有效载荷的攻击^[9]。

XML 语法允许在父元素里嵌子元素,从而可以表达数据之间的复杂关系。为此也留下了攻击漏洞,攻击者可以构造一个嵌套层次较多(一般嵌套层数达 10000)XML 文件,这种攻击可以使目标系统 CPU 使用率达到 100%,大大降低了 Web 服务的可用性。这种攻击可以使用 Schema 验证来处理。

3) 特大型有效载荷^[10]。

Web 服务是基于 XML 的,然而解析 XML 文件是一个很耗时间和内存资源的过程,这也给攻击者留下了一个漏洞。攻击者可以构造一个足够大的请求报文发送给服务器,XML 解析器处理 SOAP 消息、Ws-Security 规范里 XML 签名、XML 加密要消耗大量的内存资源,甚至导致内存溢出以达到攻击的目的。目前的 XML 解析器大都是基于 DOM(Document Order Model)的,这种模型解析器首先把 XML 文件读入内容,然后数据以树状结构的形式被加载到内存中,在内存中构造这样的树涉及大量时间开销和空间开销。实验表明一个 1M 的 XML 文件经 XML 解析器编译后达到内存 12M。

下面是一个包含大量元素的 SOAP 文件。

```
Envelope>
<Body>
<getArrayLength>
<item>data</item>
<item>data</item>
<item>data</item>
...
</getArrayLength>
</Body>
</Envelope>
```

4) 分布式拒绝服务攻击(DXDoS)。

攻击者操纵大量的主机使用 XDos 对受害主机进行攻击,这种类型攻击对 Web 服务安全造成很大威胁。主要是由于攻击者即便有很窄的网络带宽也会收到很好的攻击效果,即便此时网络管理发现攻击行为,也没有一个有效的方案来立即停止攻击行为。文献[11]实验表明停止该攻击行为最少也要 1 小时。另

外还有外部实体攻击、Schema 中毒攻击^[9]、路由劫持攻击。

5) SOAP 消息过度加密攻击。

XML 加密机制为 Web 服务安全提供了保证,然而也没 Web 服务安全留下隐患。下面是用 n 个密钥对 SOAP 消息中的 Body 进行 n 次加密。图 1 所示为一个对 SOAP 消息的 n 次加密过程。

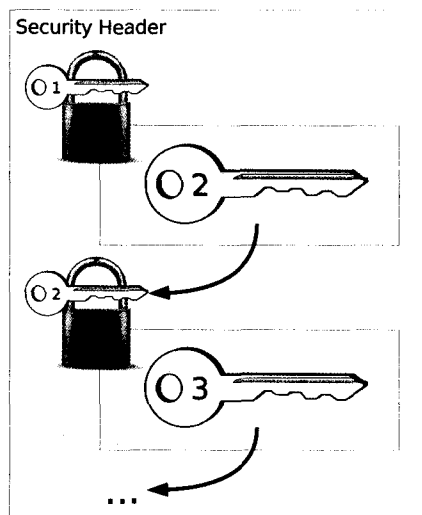


图 1 SOAP 消息加密

先用锁 1 对 SOAP 消息进行加密,形成密文 1;接着再用锁 2 对密文 1 进行加密从而形成密文 2;以此类推,用锁 n 对密文 $n-1$ 加密最后形成密文 n 。由此实现了对 SOAP 消息的 n 次加密。

要取得 SOAP 消息的数据,首先 Web 服务器收到一个 SOAP 消息后,然后对多次加密的 SOAP 消息进行一个反向解密。然而解密的大致流程是先得到第 n 次加密锁对 Body 进行一次解密操作,得到 Body ($n-1$);然后在用第 ($n-1$) 次加密锁对 Body ($n-1$) 进行解密,得到 Body ($n-2$);依次用解密锁进行解密操作,直到完全解密后的 Body 元素。在整个过程中,其中解密公共密钥的对于非对称算法,解密花费的时间大约是对称密钥算法的 1000 倍^[12],因此解密此密文会耗费大量的 CPU 资源。同时在整个过程中必须使用缓存区缓存每一对密钥,同时会占用大量的 Memory 资源。当 SOAP 消息加密加密的次数太多时,黑客会使用此漏洞进行加密攻击。

1.2 探测攻击

1) WSDL 扫描。

WSDL 是一个用来描述 Web 服务和说明如何与 Web 服务通信的 XML 语言,在 Web 服务描述中定义了一组接口供 Web Quest 调用。其中描述的主要内容有要传递的数据(Message)、消息参数(Part)、特定端口类型的具体协议和数据格式规范(Binding)、绑定和网络地址的组合(Port/Endpoint)等。然而这些信息

很轻松在 UDDI 或 UBR 获取。一般而言,把 Web 服务请求者分为内部访问者和外部访问者。内部访问者仅能访问本地网络,外部访问者仅能访问外部网络。把 Web 服务及扣分为外部接口和内部接口。现在的开发工具如. Net 还是 J2EE 都会自动生成全部的方法调用的 WSDL 文件,这些信息可以被 hacker 用来寻找攻击漏洞;同时,攻击者可以使用掌握的有用信息去推测未公开的接口信息并调用。

2) WSDL 参数篡改。

为了调用 Web 服务服务请求者需要传递一些必要参数给服务器。WSDL 文件中描述了参数的具体使用^[13],恶意用户通过修改 WSDL 文件中的参数来达到访问未授权的信息。

1.3 注入攻击

1) XML 注入攻击。

XML 注入攻击是在 SOAP 消息中加入未经验证的 XML 元素,从而更改 SOAP 消息的 XML 的结构。修改后的 SOAP 消息是符合 XML 语法规则的,但是可能会包含不安全内容,如图 2 所示。

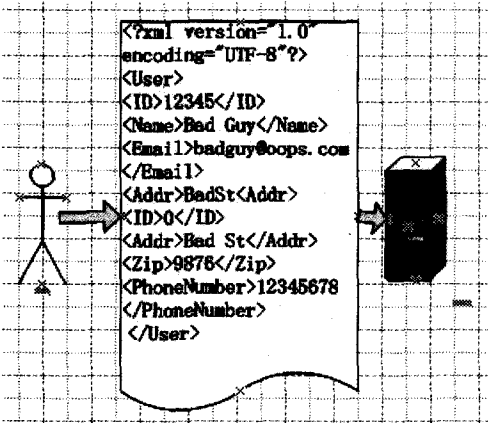


图 2 XML 注入攻击

刚开始用户经解析为 12345,攻击者在后面加入伪造的 ID 节点后,最总的解析结果 ID 为 0,主要是因为 SAX 解析器允许现有节点的值覆盖先前的节点值。然而 DOM 解析器比较复杂且智能化,他可以很好的抵御 XML 注入攻击。Xpath 攻击和 XML 注入攻击相似,这里不再累赘。

2) SQL 注入攻击。

许多 Web 服务的基本应用是向外界提供信息或者将数据提交服务器端,这些都要与数据库进行交互。如果 Web 应用程序没有对客户端提交的对数据库操作相关信息进行安全性检验,有可能通过注入恶意 SQL 命令,从而达到非法的目的。造成的后果是非常严重的,比如^[14]攻击者未经授权可以访问一些敏感信息、对数据库执行 insert, delete 操作。图 3 给出了 SQL 注入攻击的一个实例。本例子利用 “--” 使原有的部

分查询条件失效 “OR 1=1” 构造出永远为真的查询语句。如果有用户名为 admin,不需要密码可以轻松的获取管理员的权限,删除数据表,达到攻击目的,如图 3 所示。

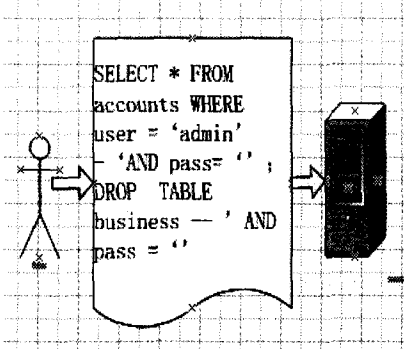


图 3 SQL 注入攻击

2 防御措施

SOAP 协议主要致力于简单传输,没有考虑太多的安全因素,W3C 和 IETF、OASIS 等组织提出了 XML 加密、XML 签名、SAML 等规范,该规范为 Web 服务提供一个不同粒度级别的内容加密。数字签名与安全访问控制,保证数据传递的不可否认性。这些 Web 服务安全协议保证 SOAP 消息端到端的安全传输,但是协议本身太过复杂,并没有考虑太多语义 Web 服务安全,也带来了新的 Web 服务安全威胁。文献[8]提出了基于服务的追踪架构(SOTA)然后引进了一个过滤防御系统(XDetector),把 SOTA 和 XDetector 联合起来可以有有效的防御 XDoS 攻击和 DXDoS 攻击。Jenson et al^[12]和 Padmanabhuni et alD^[15]讨论了 XDoS 攻击带来的影响以及抵御对策。在文献[16],提出了基于 Honey-pot 的简单而且有效的入侵检测系统,但是该系统仍然没有广泛应用。文献[14]指出使用正在表达式过滤像 like 和%等关键字,来预防 SQL 注入攻击。通过检查 SOAP 消息行为,可以预防一些攻击行为。文献[17]提出通过检测 SOAP 消息的请求速率来检查 SOAP 洪范攻击。

3 结束语

Oracle 的 J2EE 平台和微软的. NET 平台在 Web 服务上的互操作性,为集成提供很大的便利。成为从 B2C (Business to Consumer) 到 B2B (Business to Business) 商业模式转变的关键技术。然而,Web 服务面临的安全问题阻碍了 Web 服务的大规模应用,Web 服务的安全逐渐引起人们的重视。

文中对 Web 服务安全攻击进行了研究,主要包括既分析理论也结合现实应用,为 Web 服务安全各关键技术指明了研究方向。

参考文献:

- [1] 任艳娜, 闻素红, 刘 斌, 等. NET 与 Web 服务解析[J]. 计算机技术与发展, 2006, 16(1): 196-197.
 - [2] 李程程, 张永胜, 李 静, 等. 一种简单的 Web 服务安全通信模型研究[J]. 计算机技术与发展, 2010, 20(9): 158-160.
 - [3] OASIS. Web Services Security: SOAP Message Security1. 1 [S/OL]. 2006-02-01 [2010-05-10]. <http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>.
 - [4] OASIA. WS-Trust1. 4 [S/OL]. 2009-02-02 [2011-05-11]. <http://docs.oasis-open.org/wss/v1.1/was-v1.1-spec-os-SOAPMessageSecurity.pdf>.
 - [5] 张俊妍, 陈启买. SOAP 协议性能与安全的研究进展[J]. 计算机技术与发展, 2009, 19(6): 163-167.
 - [6] 胡佳辉. 基于 UDDI 的 Web 服务平台研究[J]. 计算机技术与发展, 2006, 16(11): 7-12.
 - [7] 高文婕, 赵逢禹. 基于 SOAP 消息的过度加密攻击检测算法[J]. 计算机工程, 2011, 36(22): 129-131.
 - [8] Chonka A, Zhou Wanlei. Defending grid web services from XDoS attacks by SOTA [C]//Proc of the Seventh Annual IEEE International Conference on Pervasive Computing and Communications. [s. l.]: [s. n.], 2009.
 - [9] Lindstrom P. Attacking and Defending Web Services[R]. [s. l.]: [s. n.], 2004.
 - [10] Vorobiev A, Han Jun. Security Attack Ontology for Web Services [C]//Proceedings of the IEEE Second International Conference on Semantics, Knowledge and Grid. [s. l.]: [s. n.], 2006.
 - [11] Jensen M, Gruschka N, Herkenhoener R. A survey of attacks on web services [C]//Computer Science - Research and Development (CSR D). [s. l.]: [s. n.], 2009: 185-197.
 - [12] 高文婕, 赵逢禹. 基于 SOAP 消息的过度加密攻击检测算法[J]. 计算机工程, 2010, 36(22): 128-131.
 - [13] Jensen M, Gruschka N, Herkenhoner R, et al. SOA and Web Services: New Technologies, New Standards - New Attacks [C]// Proceedings of the Fifth European Conference on Web Services. [s. l.]: [s. n.], 2007.
 - [14] 王伟平, 李 昌, 段桂华. 基于正则表示的 SQL 注入过滤模块设计[J]. 计算机工程, 2010, 37(5): 158-160.
 - [15] Padmanabhuni S, Singh V, Kumar K M S, et al. Preventing Service Oriented Denial of Service (PreSODoS): A Proposed Approach [C]//ICWSapos 06 International Conference on Web Services. [s. l.]: [s. n.], 2006: 577 - 584.
 - [16] Sidharth N, Liu Jigang. IAPF: a framework for enhancing Web services security [C] //Proc of the 31st Annual International Computer Software and Applications Conference. [s. l.]: [s. n.], 2007.
 - [17] Xu Jun, Lee W Y. Sustaining availability of Web services under distributed denial of service attacks [J]. IEEE Trans on Computers, 2003, 52(2): 195-208.
- +++++
- (上接第 212 页)
- eling of web services security [C]//Proceedings of the IEEE International Conference on Web Services (ICWS 2007). [s. l.]: [s. n.], 2007: 431-438.
 - [2] 汪红波, 袁利永, 汪红刚. 基于用户令牌实现 Web 服务身份验证[J]. 计算机与数学工程, 2006, 34(10): 79-82.
 - [3] 续亚锋, 陈志国, 李 涵. 用 WSE 构建安全可靠的 Web Services [J]. 计算机技术与发展, 2008, 18(8): 155-158.
 - [4] 董国栋. Web Service 消息级安全研究[D]. 青岛: 中国海洋大学, 2008.
 - [5] 赵会洋, 王 爽, 魏士伟. 网络安全模型中认证策略的研究 [J]. 计算机技术与发展, 2010, 20(4): 171-174.
 - [6] Brown K. WSE 3. 0 中的安全性功能 [EB/OL]. 2005. <http://www.microsoft.com/china/MSDN/library/WebServices/WebServices/WSESecurity.aspx?mfr=true>.
 - [7] 孟 伟, 张 瑕, 李军怀, 等. Web 服务安全模型研究与实现[J]. 计算机工程与应用, 2006(26): 134-136.
 - [8] 李程程, 张永胜, 刘广钰. 一种安全的语义 Web 服务模型研究[J]. 计算机技术与发展, 2010, 20(2): 171-174.
 - [9] 柳翠寅, 刘 霞. XML 签名技术的研究与应用[J]. 计算机应用与软件, 2007, 24(4): 36-38.
 - [10] OASIS Standard Specification. OASIS Web Services Security 3 X. 509 Certificate Token Profile 1. 1 [EB/OL]. 2006. <http://www.doc88.com/p-14385135283.html>.
 - [11] Hollunder B. Domain-Specific Processing of Policies or: WS-Policy Intersection Revisited [C]//2009 IEEE International Conference on Web Services. Los Angeles, USA: [s. n.], 2009: 6-10.
 - [12] Web Services Enhancements (WSE) 3. 0 的新功能 [EB/OL]. 2005. <http://blog.csdn.net/hiyaolee/archive/2005/11/13/528496.aspx>.
 - [13] 李 婧, 赵逢禹. 基于策略断言的 SOAP 消息的部分签名和加密[J]. 计算机工程与设计, 2009, 30(8): 1914-1917.
 - [14] 魏文红, 吴清江. WSE 加密在 Web 服务中的应用[J]. 计算机与现代化, 2005(12): 56-58.
 - [15] 胡晓红, 付永军, 张志平. 基于策略的 Web 服务安全解决方案研究[J]. 微计算机信息, 2008, 24(15): 93-94.
 - [16] Xiong Pengcheng, Fan Yushun, Zhou Mengchu. Web Service Configuration Under Multiple Quality-of-Service Attributes [J]. Automation Science and Engineering, 2009, 6(2): 311-321.