SOAP的安全性影响和WEBSERVICE接口云计算系统

计算机工程系主任，西得乐工程技术大学道路，卡拉奇，信德75300，巴基斯坦HASSANZAKI ,计算机工程系主任，西得乐工程技术大学 道路，卡拉奇，信德75300，巴基斯坦

摘要：

云计算系统在IT行业发布了一个演进，从用户的PC中删除了应用程序。它

可以在Webservice技术中实现，其界面不过是一个Web浏览器。

因此，Webservice的固有漏洞也可以使云计算系统成为可能

同样的风险。在本报告中，我将讨论云计算系统的安全问题

由webservice引起。本文由四部分组成：第一部分和第二部分用于介绍一些

关于云计算和Webservice。安全问题将在第三和第四讨论

部分。第三部分安排了Saas层的安全漏洞，由webservice引起。最后一部分解释

Iaas层中的漏洞是什么。

关键词 - 安全问题，Web服务，云计算，安全漏洞，漏洞，Saas层。

介绍

如今，用户PC中安装的传统应用程序面临着许多问题。例如，它的

副本权可以被反转引擎覆盖，PC可能无法达到最低要求

应用。被认为是互联网的未来的云计算为这些问题提供了一个解决方案。

云计算是一个新概念，其目的是使其客户摆脱安装任何应用程序

在他们的电脑。用户只需要使用他们的网络浏览器即可在线访问应用程序，并可能收取费用

即付即用模式。它不仅可以提供巨大的计算大量数据的能力，而且可以让它们

产品避免破裂。到目前为止，还没有关于如何实施Cloud的明确定义

计算系统。然而，在web 2.0广泛部署在IT行业之后，大多数人喜欢设计

云计算系统通过组合Ajax和Webservice。 Webservice是一个基于Internet的应用程序

它也有很多安全问题。本文的目的是解释云计算系统的方式

受到Webservice的漏洞的影响。

1.1。背景

什么是云计算？

云计算被IT从业者视为未来的技术。但是，目前还是一个

IT行业新兴概念。其目的是使用基于Internet的服务来代替安装的应用程序

在用户的电脑中。因此，用户将不再需要在其计算机中安装应用程序，并可以对其进行充电

每次使用它时。 “云”这个词是与客户提供的服务的类比。现在，

不同的组织仍然使用自己的原则来建立自己的系统，而且似乎都没有

克服别人成为一个标准。然而，云计算的架构仍然可以总结

通过使用Xaas（Every thing as a service）[1]。

ISSN：0975-5462

Vol。 3 2011年4月4日

3472

软件即服务（Saas）

平台即服务（Paas）

基础设施即服务（Iaas）

硬件即服务（Haas）

图。 1云计算系统架构

上图中的图1云计算系统可分为4层。第一层代表

用于为客户提供服务的应用程序或软件。第二层是平台

应用程序由其设计人员实现。第三层由广泛分布的基础设施组成

用于为两个上层提供数据。底层由硬件构建，整个地方

系统正在运行。目前，市面上已经有很多云计算产品

Google App和Amazon EC2。虽然他们的系统架构符合4层架构，

他们仍然在不同层面提供云服务。 Google App是云计算的一个很好的例子

他们的服务在Saas层上运行。它使用户可以在线使用Word应用程序并将其保存在服务器上

以及。相反，Amazon EC2在Iaas层提供了他们的云服务，允许用户上传

他们自己的应用程序并在线运行。

B.云计算Web服务

Webservice实际上是一种在线应用，被认为是非常适合的技术

实施云计算系统。 Webservice的结构设计在Client-服务器格式也。服务器将提供一个称为WSDL的XML文件，供用户设计其界面。 WSDL对用于开发接口的技术没有任何限制，因此可以通过多种方式进行设计。一般来说，Webserivce可以安排在Saas，Paas和Iaas层。[2] •••Saas：在这一层，Webservice将作为应用程序运行，用户可以通过浏览器直接访问该应用程序。 Paas：Webservice可以与其他技术相结合，为Saas层中的应用程序提供一个环境。 Iaas：Webserive扮演上层应用程序的海量数据中心的角色。 2. SAAS层的安全问题在SaaS层面，Webservice可以用于为用户提供云服务。在云计算系统中，浏览器应该是用户与服务器进行通信的唯一接口。因此，Webservice非常适合通过与Web2.0结合来实现Saas层。因此，Webservice的安全问题也使得云计算易受影响。 A. SOAP消息的问题SOAP是Webservice在客户端和服务器端之间传输消息的协议。该消息实际上是以XML格式设计的，其内容不仅仅是纯文本。在这种情况下，云计算系统极易受到数据篡改，嗅探和拦截的威胁。这些问题可以通过在SOAP消息中添加一个头文件[3]来解决。标题包含可用于加密XML文件内容的标签。在标题中，标签<xenc：ReferenceList>定义SOAP消息的哪个部分将被加密。加密部分称为<xenc：EncryptedData>，其加密密钥存储其名为<ds：KeyInfo>的子元素。图2是标题的示例。 ISSN：0975-5462Vol。 3 No. 4 April 20113473 Danish Jamil et al。 /国际工程科学与技术学报（IJEST）图2 SOAP消息的加密B.浏览器的问题如上所述，SOAP消息可以通过使用加密来保护。然而，目前市面上的所有浏览器都不能生成用于加密SOAP消息的XML头。有两个解决方案来解决这个问题。 SSL是可以用来替换XML头文件的第一种方法。它可以使用公钥和私钥加密消息，以保证只有收件人能够理解它。但是，SSL也容易受到网路钓鱼攻击。 [2] [4]黑客可以使用Phising攻击向用户发送欺骗性网页，而不是从真实服务器发送的网页。如果用户没有注意到网页被篡改，所有的输入数据将被攻击者接收。与第一种方法相比，第二种方法更为安全。它通过将SSL与Microsoft的护照相结合来实现。 [2] Microsoft Passport是第三方代理，可用于将重定向存储到请求的服务器。用户成功登录护照服务器后，代理可以通过利用用户的凭据生成Kerberos令牌。 （例如用户名和密码）令牌可用于生成XML头，并通过预先存储的重定向传送到预期的接收者。因此，可以通过与Microsoft Passport结合来添加SOAP消息。然而，它也使SOAP消息受到高度的攻击风险，因为只有Microsoft Passport才能保护具有相同原始策略（SOP）的Kerberos令牌。幸运的是，这个问题仍然可以通过多种方式调用SSL来解决。[2]例如，使用SOP比较每个客户端收到的公钥，而不是其DNS信息。 C.旁路认证由于Web浏览器和服务器之间的通信应严格遵循WSDL的定义，黑客也可以利用它来绕过认证。当用户向服务器发送消息时，根据WSDL，他们必须指定要执行的输入和操作的类型。在这种情况下，如果入侵者可以拦截传输的数据，系统将极其脆弱。 OWASP提供了一个解释如何利用此漏洞的教程。黑客可以通过篡改行动名称获得更多权利。图3是上述攻击的例子。攻击者拦截了该请求，并通过更改操作的名称成功地执行了未经授权的操作。 ISSN：0975-5462Vol。 3 No. 4 April 20113474 Danish Jamil et al。 /国际工程科学技术学报（IJEST）图3 DataTamperD截取的请求动作。 SQL注入此攻击被认为是对数据库的严重威胁，似乎与Webservice无关。然而，云计算需要webservice必须使用浏览器作为接口，并通过HTTP协议发送数据。在这种情况下，黑客在传统网站上执行SQL注入的技术对云计算系统也是有效的。这个问题的对策sh可以和传统的一样。 E.拒绝服务拒绝服务攻击可以分为两类：输入海量数据和洪泛攻击。这两种类型的攻击可以通过向服务器输入或淹没海量数据来实现。它们可能导致服务器必须安排更多的内存来处理这些请求，并最终使系统崩溃。当攻击者想要通过输入大量数据来实现它时，通常不会只输入数百个简单的字符。而不是这些字符，它们将输入许多在WSDL中定义的XML元素。因此，服务器将继续忙于处理这些标签，直到它折叠。下图是通过输入大量元素的Dos攻击的例子。图4通过输入多个元素进行DOS攻击洪泛攻击中的数据与定期请求相同。然而，这种攻击是由许多计算机完成的。这些电脑可能是由黑客通过木马控制的僵尸电脑。因此，如果攻击者在同一时间启动100个请求，目标将被停止。 3. IAAS和PAAS层中的安全问题A. XML包装攻击在IAAS和PAAS层中，云计算服务提供商通常希望为供应商提供WSDL文件来设计应用程序。在这种情况下，如果攻击者成功获取了WSDL文件，那么它们可能是ISSN：0975-5462Vol。 3 No. 4 April 20113475 Danish Jamil et al。 /国际工程科学与技术杂志（IJEST）利用XML包绕来绕过认证。[5] [6]。 XML包装与SQL注入的方式大致相同。由于用户发送的消息是XML格式的，所有的输入数据都将被包装成XML标签，称为元素。因此，如果用户输入一些元素，SOAP消息也将它们视为其固有元素。在这种情况下，黑客可以通过注入相关元素修改未经授权的数据。下面的图4是XML包装攻击的示例。黑客注入两个元素以便更改用户102的数据。对于这个弱点的对策也可以被引用为SQL注入的对策。供应商可以通过为用户输入过滤器来删除关键字或指定预期输入的长度来防止此攻击。图5 XML Wrapping AttackB。 WSDL枚举WSDL通常设计有XML模式。在表面上，它不只是一个纯XML文件。因此，如果XML文件被攻击者窃取或成功猜测，则整个云计算系统可能被其接管。这些是从webservice系统转储WSDL文件的许多方法。第一种方法，也是最简单的方法，是谷歌黑客。谷歌目前已经为用户提供了许多特殊操作来缩小搜索范围。例如，关键字“url：”表示查找目标网址中的预期信息。因此，攻击者使用一些关键字来表示包含WSDL的预期结果，Google机器人可能会发现WSDL。以下关键字是可以通过Google搜索WSDL的一些示例[7]。 a）feltype：wsdl b）indexof“/ wsdl”c）inurl：wsdl d）inurl：asmx有时，webservice设计者希望将WSDL文件安排在具有网页界面的同一目录下。因此，攻击者可以通过将所有字符串（url中的问号后面）与WSDL相关联来收集WSDL文件。例如：target / webservice？WSDL。 4.结论如上所述，作为实施云计算系统的核心技术，网络服务对其安全问题起着非常重要的作用。 Saas，Iaas和Paas层广泛部署了安全问题。在Saas中，Web服务被用作云计算系统的实质，为客户提供云服务，Webservice面临来自SOAP消息，Web浏览器，SQL ISSN：0975-5462Vol的问题。 3 No. 4 April 20113476 Danish Jamil et al。 /国际工程科学技术学报（IJEST）注射和DoS攻击。 SOAP消息通常以纯文本形式写入，Web浏览器将不会提供特定的加密功能。在这种情况下，可以预期用于加密XML消息的新功能。在Paas和Iaas层中，Web服务被用作工作环境或数据中心来支持整个系统。在这种情况下，许多Web服务提供商将向Clouding Computing System开发人员提供WSDL文件。但是，WSDL文件也可以被攻击者使用。在这种情况下，它使云计算系统非常容易受到WSDL包装攻击和WSDL枚举的影响。在这种情况下，供应商应该仔细思考如何正确地保护其WSDL。 5.致谢我向斯奈德工程技术大学计算机工程系主任Syed Faisal Ahmed Bukhari博士致以诚挚的谢意，为本文提供了领导和便利。我扩大我的t对穆罕默德·努曼·阿里汗先生的合作表示衷心的感谢。我也衷心感谢Syed工程技术大学的所有其他教授和我的朋友们的支持和鼓励。参考文献[1] [2] B.P.R。 Enumi Choi和Ian Lumb，“云计算系统分类与调查”，第五届国际联合会议，IMS和IDC，第44-45页，2009年.Jensen和N.Gruschka，“云计算技术安全问题”，2009年IEEE国际云计算会议，第109-116页，2009年。[3] [4]（2002）微软网站，[在线]，可用：http://msdn.microsoft.com/en-us/library/ms951257。 aspx＃wssecuritytoc6120253C.L。 Abad和R.I.Banilla，“Analysis of the Schemes for Detecting and Preveting ARP Cache Poisoning Attack”，IEEE.org，Pages1-8,2007。[5] N。 Gruschka and LL Iacono，Vulnerable cloud，2009 IEEE International Conference on Clouding Computing pages，Pages 625-631,2009。[6] [7]（2010）Webgoat Tutorial，[online]，Available http://yehg.net/lab /pr0js/training/webgoat.php#Authentication\_FlawsN。 Bhalla和S. Kazerooni。 Web服务漏洞，安全，安全指南针，2007年2月15日，第6页。ISSN：0975-5462Vol。 3 No. 4 April 20113477