文章编号:1005-1228(2015)06-0036-02

基于客户端特征增强 Web 会话安全技术研究

阳瑞发

(中国工程物理研究院计算机应用研究所,四川 绵阳　621900)

摘　要:基于 HTTP 通信协议的 Web 应用中,使用 Session 和 Cookie 的会话是应用认证的主要方式。分析了 Web 会话的实现原理和安全威胁,提出了一种基于客户端特征的 Web 会话安全增强的方案,用于增强 Web 会话以及应用认证的安全性。

关键词: Web 会话;安全;Cookie

中图分类号:TP31　　**文献标识码:**A

Research on the Web Session Security Enhancement Technology Based on Client Features

YANG Rui-fa

(Institute of Computer Application, China Academy of Engineering Physics, Mianyang 621900, China)

Abstract: It's the main method of authentication for web applications that are based on HTTP communication protocol by using session and cookie. The principle and security threats of Web session are analyzed, and an approach that is used to enhance not only the security of web session, but also the security of web application authentication based on client features is proposed.

Key words: web session; security; cookie

HTTP 是一种无状态的通信协议,Web 服务器会将接收到得每个 HTTP 请求视为相互独立、互不干扰的访问请求。在服务器每次完成一次请求后,即自动关闭与客户端的连接,因而不能判断一个请求序列是否来自相同的客户端,也不能区分一个请求序列是否来自同一用户,无法记录用户操作等。而在 Web 应用中,通常需要记录和跟踪用户的会话状态,用于对用户进行身份认证、访问控制等[1]。

为解决会话保持与跟踪问题,引入了 Session 和 Cookie 两种技术[2]。Session 是一种服务端的会话保持技术,由 Web 容器管理,Web 容器会为每个用户创建一个具有唯一标识 Session ID 的 Session 对象用于记录用户的会话状态,并将 Session ID 作为一段 Cookie 返回到客户端的浏览器中,由浏览器进行管理。当同一用户通过浏览器再次提交 HTTP 请求时,浏览器将自动提取 Cookie 中的 Session ID 一并提交到服务端,服务端的 Web 容器则通过 Session ID 查找对应的 Session 对象,获得用户的会话信息。由于 Session ID 的唯一性,从而实现了用户与 Session 对象的一一对应,解决了 HTTP 协议无状态的问题。

1　安全威胁分析

在 HTTP 通信中,会话的认证、保持与跟踪由 Session 和 Cookie 共同完成,其核心是 Web 服务器和客户端之间传递的 Session ID 值,客户端提交请求时需要同时提交 Session ID 值,服务器则根据 Session ID 值查找对应的会话,Session ID 值是会话认证的关键信息。由于在 HTTP 通信中,请求数据均以明文方式提交,在数据传输过程中,Session ID 值容易被恶意攻击者获取,攻击者一旦获取 Session ID 值,将会发起针对会话的攻击,绕过 Web 应用本身的认证机制,从而获得与合法用户等同的操作权限、数据权限,给 Web 应用带来安全威胁[3]。

常见的针对会话的攻击有:会话劫持、会话固定、会话重放、CSRF 攻击等,这些攻击方式的共同特点是获取合法用户的 Session ID,欺骗 Web 服务器,冒充合

收稿日期:2015-08-07
基金项目:中国工程物理研究院科学技术发展基金资助项目(项目编号:2013B0403076)
作者简介:阳瑞发(1984-),男,硕士,主要研究方向:Java EE 系统开发、系统集成。

法用户对 Web 应用进行非授权访问。

2　安全增强实现

在当前的会话认证中,Session ID 值由 Web 服务器生成,与客户端无关,换言之,只要 Session ID 值相同即被认定为是同一客户端的同一访问用户，而不管发出请求的是合法用户还是非法攻击者，这种会话认证的方式在一定程度上为会话攻击提供了便利。

因此,提出了一种基于客户端特征的 Web 会话认证方案,用于增强会话的安全性。客户端特征是指具有标识性或唯一性的客户端属性，包括客户端 IP 地址、访问时间、User-Agent 属性、Schema 等。该方案中 Session ID 的生成流程如图 1 所示。

图 1　基于客户端特征的 Session ID 生成流程

首先仍使用传统的方式生成 Session ID,并创建会话。之后由 Web 服务器提取客户端特征,并将这些特征进行组合,组合方式可以是字符串组合,也可以是对特征值进行位移计算等。最后对组合结果计算 HASH 值,所得结果称之为 Session SID(会话安全 ID),并将 Session SID 保存到已创建的会话中。同时将 Session ID 返回到客户端,此时,客户端和服务器之间传递的仍是 Session ID,Session SID 则保存到服务器端的 Session 对象中,不返回到客户端,不进行网络传输。

创建会话后,在后续的 HTTP 请求中,需要对会话进行认证,认证流程如图 2 所示。

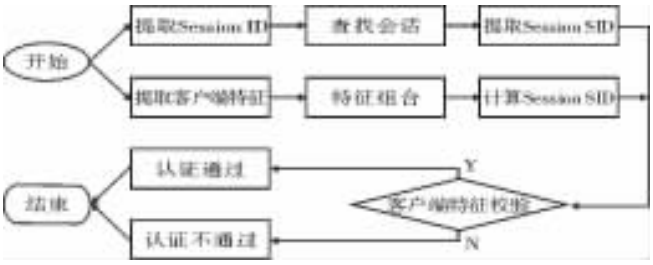

图 2　基于客户端特征的会话认证流程

在会话认证流程中，首先根据客户端和服务器之间传递的 Session ID 查找对应的会话，并从会话中提取已保存的 Session SID。与此同时,由 Web 服务器提取客户端特征,并将这些特征进行组合,组合方式需要与 Session ID 的生成过程保持一致，最后对组合结果计算 HASH 值,重新生成 Session SID。之后将会话中保存的 Session SID 与重新计算生成的 Session SID 进行比较,如比较结果相同,则表示当前请求来自同一客户端的合法用户,会话认证通过,否则,表示当前请求来自非法用户或攻击者,会话认证不通过。

与传统的会话认证只需要 Session ID 相比，这里的认证过程在此基础上添加了对客户端特征的校验,一旦客户端发生变化,会话认证将不通过。因此,即便 Session ID 被攻击者截获后冒充合法用户发起 HTTP 请求,由于攻击者与合法用户的客户端特征不尽相同,根据客户端特征计算产生的 Session SID 值也将不同,所以会话认证将不会通过。这有助于增强会话认证和 Web 应用的安全性。

3　结束语

通过使用客户端特征计算会话安全 ID(Session SID),在会话认证时,除了使用传统的方式通过 Session ID 进行认证外,还需要对客户端特征进行认证,有效的增强了会话认证的安全性。此外,在生成 Session SID 后,Session SID 只保存在服务器端的 Session 对象中,不返回到客户端,不进行网络传输,避免了被攻击者截获的风险,这进一步增强了会话认证的安全性。

参考文献:

[1] 张道银. Web 会话安全研究[J]. 中国科技信息,2010(3):142-144.

[2] 李景峰,祝跃飞,张栋. 用户控制下 Cookies 安全研究与实现[J]. 计算机工程,2005,31(14):150-152.

[3] 徐兵,谢仕义. Web 应用程序会话安全模块的设计[J]. 计算机工程,2008,34(19):176-178.