

防火墙与入侵检测系统的联动

冯庆煜

(西华师范大学 计算中心, 四川 南充 637002)

(fgy_work@163.com)

摘 要:从网络安全整体性和动态性的需求考虑,采用分布式开放平台安全互联的方法,实现防火墙与入侵检测系统的联动。提出联动系统对突发网络攻击进行主动防御的思想,对相应关键技术进行了探讨,目的在于增强入侵检测系统的阻断功能。

关键词:个人防火墙;入侵检测系统;联动;主动防御

中图分类号: TP393.08 **文献标识码:** A

Interaction technology with firewalls and intusion detection system

FENG Qing-yu

(Computing Center, West China Normal University, Nanchong sichuan 637002, China)

Abstract: Considering the demand of obtaining integrity and dynamics in network security, an interaction model with firewalls and IDSs (Intrusion Detection System) was implemented based on the ideal of distributed open platform of security. To strengthen the stop function of intrusion detection, the idea which interaction system making initiative recovery to paroxysmal network attack was presented, and the key technology of implementation was introduced.

Key words: personal firewall; Intrusion Detection System(IDS); interaction; initiative recovery

0 引言

针对网络攻击、入侵等安全问题,产生了个人防火墙、入侵检测系统(IDS)等多种网络安全技术。然而,不同的安全技术主要解决某一个安全问题,它们各自为战,不能互相进行信息交流。个人防火墙是一种访问控制安全技术,主要是根据网络安全策略控制进出主机的网络流量,阻断非法连接及访问。它的规则都事先设置,对于实时的攻击无法实时调整策略,基于性能考虑,一般不检查数据包内容,对一些协议细节不作详细解析,所以只要是经过合法通道的网络攻击,防火墙就无能为力了。入侵检测系统可以弥补防火墙内容检查和协议解析的缺点,从中发现违反安全策略的行为和攻击迹象,但对攻击的抵抗力较弱^[1]。

通过联动机制把各种安全技术有机联系起来,实现网络的全面安全保障。个人防火墙和入侵检测系统之间的联动,使防护体系达到由静态到动态,由平面到立体的转变,提升了防火墙的机动性和实时反应能力,增强了入侵检测系统的阻断功能。

1 使个人防火墙与入侵检测系统联动

联动是指通过一种组合的方式,把不同的安全技术整合

在一起,由其他安全技术弥补某一安全技术自身功能和性能的缺陷,以适应网络安全整体化、立体化的要求^[2]。个人防火墙作为主机安全的最后一道防线,检测系统作为主动发现入侵行为的设备,它们之间的协同工作,能够进一步强化各自的作用,从而提高桌面计算机抵抗入侵的能力。

图1给出了个人防火墙和IDS的联动系统模型。该系统主要由三个部分组成:(1)基于ACE和SSL的可移植安全通信平台。ACE(Adaptive Communication Environment)是一个开源的面向对象网络通信中间件,具有高可移植性、增强的软件质量、高效率与可预见性等优点。SSL(Secure Socket Layer)是在Internet基础上提供了一种保证私密性的安全协议,它能使客户/服务器应用之间的通信不被攻击者窃听。基于ACE和SSL构建的通信平台不仅保证了通信的安全性,还具有高效率 and 可移植性强的特点。(2)联动控制模块是联动系统的核心,主要有分析决策、策略应用和日志模块。分析决策模块对收集的入侵报告进行分析、过滤,将策略提交给策略应用模块;策略应用模块负责将策略应用到相应的防火墙,收集应用反馈,并记录日志;日志查询模块提供日志信息的访问接口。其中策略库由报警事件与基本响应事件相关联组成^[3]。(3)联动代理在启动和关闭时分别向联动控制模块进行注册和注销,负责联动信息的交换,并对所代理的安全产品实施策略设置。

收稿日期:2005-06-20;修订日期:2005-08-25

作者简介:冯庆煜(1950-),男,四川中江人,副教授,主要研究方向:计算机网络安全、程序设计语言。

参考文献:

- [1] AGRAWAL R, KIERNAN J. Watermarking Relational Databases [A]. Proceedings of the 28th International Conference on Very Large Databases(VLDB)[C]. Hong Kong, China: 28 VLDB, 2002.
- [2] AGRAWAL R, KIERNAN J. Watermarking Relational Data: Framework, Algorithm and Analysis[J]. The VLDB Journal The International Journal on Very Large Data Bases, 2003, 12(2): 157-169.
- [3] SION R, ATALLAH M, PRABHAKAR S. Rights Protection for Relational Data[A]. Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data[C]. San Diego, California: ACM SIGMOD, 2003. 98-109.
- [4] GROSS-AMBLARD D. Query-preserving Watermarking of Relational Databases and XML Documents[A]. Proceedings of the Twenty-second ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems[C]. San Diego, California: ACM Press, 2003. 191-201.

联动系统的基本原理是:在防火墙和 IDS 所构筑的安全体系中,当 IDS 检测到入侵行为时,迅速启动联动机制,产生入侵报告(包括入侵类型,协议类型,攻击源的地址和端口,攻击目标的地址和端口,时间等),经过联动代理封装和加密发送给联动控制模块。分析决策模块对入侵报告处理后得出相应的响应策略,并通过策略应用模块通知所有已知防火墙的联动代理。联动代理从中解析响应策略,为各自防火墙新建访问控制规则,从而达到抵御入侵的目的。由于当一次入侵发生时,局域网中的所有防火墙都做出相应策略的动态修改,从而实现了这种突发网络攻击的主动防御。

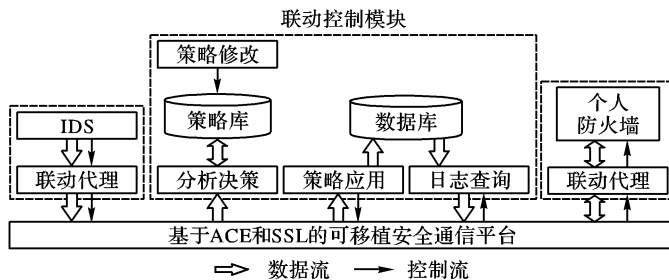


图1 个人防火墙和IDS的联动系统模型

2 关键技术分析

2.1 基于ACE和SSL的网络通信平台

ACE是可以自由使用、开放源码的面向对象框架,它提供了一组丰富的可复用C++包装外观和框架组件,可跨越多种平台完成通用的通信软件任务^[4]。由于ACE具有高可移植性和更强的软件质量的优点,使得基于它开发的通信平台和联动代理等网络模块能方便地在常用系统进行移植,并保持良好的效率。

SSL安全协议为网络应用层通信提供了认证、数据保密和数据完整性的服务,较好地解决了Internet上数据传输的安全问题^[5]。联动系统中SSL的实现是利用了OpenSSL提供的开发库。其通信过程和HTTP协议类似,在客户端和服务端建立TCP连接(connect和accept)成功之后,SSL开始运行。首先进行安全握手连接即SSL_connect和SSL_accept,以确定协议版本、密码算法、密钥和压缩方式等密码学参数并进行交互身份认证;握手成功之后,SSL_write对应用层数据进行加密并将密文向TCP层发送,SSL_read对由TCP层传上来的数据进行解密然后将明文向上层发送。

在联动系统中联动控制模块作为服务器运行,并开放事先约定的通信端口,当个人防火墙和IDS启动时,其联动代理作为客户端向服务器发送连接。只有通过服务器认证,连接才能建立。SSL会话建立后,联动系统就可以安全稳定地进行通信了。

2.2 基于XML的数据封装

XML是一种数据交换格式,允许在不同的系统或应用程序之间交换数据。XML为数据交换提供了一种新的信息传输和信息表达方法,其特点在于它的简单性、灵活性和可扩展性^[6]。联动系统中使用XML对入侵报告和响应策略进行数据封装,因此具有更好的扩展能力。下面以阻断SYN Flood攻击为例说明联动系统对数据的封装:

(1) 入侵报告

```
< intrusion >
< name > SYN_Flood < /name >
```

```
< protocol > TCP < /protocol >
< sip > 202. 202. 43. 124 < /sip > //源 IP 地址
< sport > 1734 < /sport > //源端口
< dip > 202. 202. 45. 223 < /dip > //目的 IP 地址
< dport > 80 < /dport > //目的端口
< datetime > 2005 - 1 - 19 20: 49: 28 < /datetime >
```

```
< /intrusion >
```

(2) 响应措施

```
< response >
< action > block < /action >
< protocol > TCP < /protocol >
< rip > 202. 202. 43. 124 < /rip > //远程地址
< rport > any < /rport > //任意端口
< lport > 80 < /lport > //本地端口
< during > 5 < /during > //规则有效时间(分钟)
< /response >
```

3 联动系统的主动防御

网络入侵者在入侵主机之前,总是对一个网段的计算机进行端口扫描,寻找入侵目标。这使网络入侵具有局部性。联动系统在检测到网络入侵时,对入侵目标主机和邻近的计算机都进行策略更新,对可能随之而来的入侵进行抵御,从而达到对突发网络入侵的主动防御。

为实现联动系统的主动防御,必须注意以下几点:

(1) 局域网内所有个人防火墙的联动代理在启动时,必须向指定的联动控制模块进行注册登记,这样,联动控制模块才可以在第一时间通知在线的代理模块进行策略更新。在防火墙关闭时,其联动代理也必须进行注销。

(2) 联动策略只针对拒绝服务和其它高风险的攻击。否则可能会被黑客利用成为新的攻击方法,致使IDS联动防火墙产生大量无用的规则,导致防火墙性能下降甚至拒绝服务。

(3) 联动控制所产生的规则与防火墙原有的静态规则不同,表现在以下三个特点:优先性、动态性和阻断性。优先性是指生成的规则将首先被用于访问控制,优于防火墙原有的规则;动态性是指生成的规则有一定的生存时间,不是一直存在的,攻击行为阻断或消失后规则自动超时删除;阻断性是指生成的规则的动作永远都是拒绝的,不可能生成一条允许通过的规则。这三个特点充分保证了联动和主动防御的安全性和可用性。

4 结语

联动体现了网络安全整体性和动态性。我们实现了局域网中个人防火墙与IDS的联动系统,使防护体系由静态到动态,由平面到立体,提升了防火墙的机动性,增强了局域网的整体防护能力。同时提出对突发网络入侵进行主动防御的思想,可有效保障个人计算机提前对入侵实施防卫。由于该联动系统具有很好的可扩展性,将来可以加入防病毒、安全扫描等安全产品共同参与联动,实现网络的深度防御,为局域网的网络安全提供更全面的保障。

参考文献:

- [1] 杨阔朝, 蒋凡. 模拟攻击测试方式的漏洞检测系统的设计与实现[J]. 计算机应用, 2005, 25(7): 1562 - 1564.
- [2] 姚兰, 王新梅. 防火墙与入侵检测系统的联动分析[J]. 信息安全与通信保密, 2002, (6): 29 - 31.
- [3] 方杰, 许峰, 黄皓. 一种优化入侵检测系统的方法[J]. 计算机应用, 2005, 25(1), 147 - 149.