Design of Security Inspection in Network

ZHAO Yong-chi
Computer center Mianyang Normal University, Mianyang, China
zhao0426@yahoo.com.cn

Abstract: In order to make up the existing network existence the shortage of security, this paper analysis network security question regarding the business and user's daily urgency, and has simultaneously designed the network security new defensive system structure, and proposed the independent examination new algorithm design, the comprehensive utilization many kinds of network security aspect technology, in which has designed based on the cryptology (t, n) threshold plan in the invasion examination system application, at the same time strengthened the network invasion examination, the independent defense, self-perfection network defense ability from many aspects, also strengthened the guard virus or the harmful procedure invasion, thus enhanced the system network security; Finally has carried on the safety performance test, analyzed in the network to appear the viral examination integer, to error number of times, reports to the effective the number of times, in the foresight virus integer, the actual effective viral number advantageous and the disadvantageous question, thus it can be seen, this design proposal applied during the actual network guard has certain result.

Keywords: Threshold scheme; self-detection ; Integration system; Central control

网络中安全检测的设计

赵永驰
绵阳师范学院，绵阳，中国，621000
zhao0426@yahoo.com.cn

【摘要】为了弥补现有网络存在的安全缺陷，该论文分析网络安全问题对于商家和用户的日益的迫切性，同时设计了网络安全的新型防御体系结构，提出了自主检测新型算法的设计，综合利用多种网络安全方面的技术，其中设计了基于密码学（t，n）门限方案在入侵检测系统中的应用，与此同时从多个方面加强了网络的入侵检测、自主防御、自我完善网络防御的能力，也加强了防范病毒或者有害程序的入侵，从而提高了系统的网络安全性；最后进行了安全性能测试，分析了网络中出现病毒检测个数、误警次数、有效报警次数、预见病毒个数、实际有效病毒数之中的有利与不利的问题，由此可见，该设计方案应用于实际的网络防范之中有一定的成效。

【关键词】门限方案；自我检测；集成系统；集中管理

1 引言

自从因特网诞生以来，特别是商家依靠网络来生存，各种各样的安全问题也随之层出不穷，并随着网络技术的不断发展而日益凸显网络安全的重要性。对于现今对网络已无比依赖的广大商家以及用户而言，网络安全问题始终是特别头疼而又不得不面临解决的问题。如何为商家以及用户创造一个安全网络体系，并且构建高效、可用、智能的安全网络，为商家以及用户提供无后顾之忧的安全的万全之策，是网络安全发展的最终的方向之一。同时随着网络的广泛使用、人们对网络的深入了解、越来越多的研究，使人们对网络安全方面的攻击与防范有了较深入的了解，与此同时网络上有很多网络攻防的程序源代码，均在一定程度上增加了网络安全防范的难度。总体而言，可以从几方面说明需要加强防范的理由。首先，人们可能很快发现网络安全系统的存在漏洞以及安全隐患；其次，人们可以查看程序源代码，深入明白网络的安全漏洞所在，改善自身网络体系结构，提高了网络的安全能力，第三人们很容易对病毒源代码进行修改，可以生产出新的病毒程序，也很快带来了网络病毒和破坏性程序的流行。因此需要进行多方面

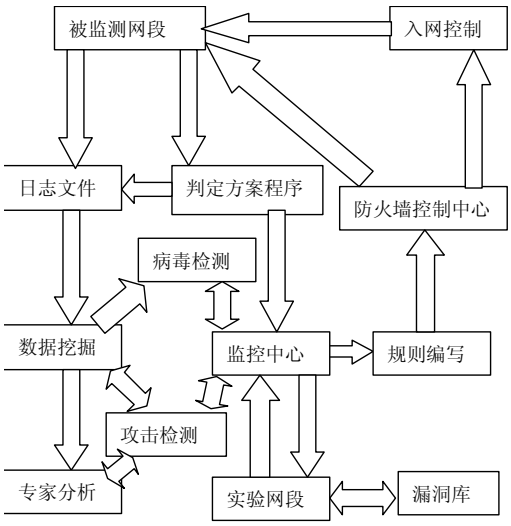
978-1-935068-09-9

网络安全防范的探讨，如何防范新型的病毒和破坏性程序，动态提高网络的防范能力，该议程随着网络的发展而逐渐迫切，该论文从网络安全等多个方面提出了一个系统体系结构，从而利用网络安全技术的数字签名和门限方案、防火墙、入侵检测等三方面的安全因素构造一个网络防御系统，极大改善了网络的防御能力，提高了系统的网络自我检测与自我调整，从而自动优化系统的安全性能。

2 防御体系设计

2.1 系统体系设计

该系统需要更改以往的网络系统设计模式，利用主动的入侵检测技术与被动的防火墙技术相互结合的办法来保护网络的安全性，现在要求对网络中出现的新型网络问题进行及时自动的处理与响应，能够通过长期的使用使整个网络的安全性能日益不断自我改善。关键是利用监控中心从各个不同的单机的获取检测信息或者报告曾经的网络疑似病毒信息，在根据信息的分门别类分析与数据挖掘分析来发现问题。然后联系整个网络中的安全问题进行了深入数据分析，得出了可能存在的网络安全隐患，把该隐患及时通知整个网络而及时自我调整的思路方法。设计见下图 1：



网络体系图

Figure 1. Network security systems design

图 1. 网络安全体系设计

2.2 网络设计方案

网络纵深防御设计包括了被监测网段、判定方案程序、监控中心、实验网段、防火墙控制中心、数据挖掘、专家分析、攻击检测等功能，从检测网络的运行程序状态来进行分析程序的正常与否，来加强网络的安全运行管理以及自检管理的能力。

被监测网段就是被管理的局域网或者几个局域网，每个主机上安装有异常报告软件：它关注网络运行期间各个主机上程序运行情况，看程序是否运行正常，同时可以查看是否有扫描其端口的行为以及对网络的攻击异常行为，以及并非本网段主机的远程登陆的行为等，如果出现如此行为，就发送给判定方案程序或者直接发送给监控中心；与此同时还要把每个主机的日志文件发送给远程的日志主机，以供分析破坏性的程序或者病毒行为，为及早发现被检测网段内出现的异常程序，并且给予及时地清除。

判定方案程序是一个基于椭圆曲线(t，n)门限方案的判定方案程序，当从监测网段发送过来具有加密与签名的功能的密文时，分类其相同行为方式，如果同类情况出现 t 次，那么就认为是出现非正常情况，需要发送到监控中心去判断，另外还需要把判定方案程序的结果发送给日志主机以供分析，有利于全方位对被监测网段的全面安全管理。当超越 t 个计算机向检测中心报告某个程序有异常行为或者破坏行为，那么就有该 t 个计算机的签名和子密钥，从而可以构造出密钥，检测中心再等待一段时间以确认该程序是病毒或带破坏性程序，那么可以发送到控制中心，控制中心在发送到各个计算机的单机防火墙以拦截该程序或者把该程序删除，如此可以提高整个系统的安全控制，可以自动提高系统防御入侵和病毒攻击的控制能力，从而提高了系统的安全性。

监控中心分析其各类行为，判断处理方式，如果属于病毒类型，可以发送到病毒处理模块以供处理；如果不能确定的行为，把该异常行为方式争取在实验网段再次显现，由实验网段来分析行为。同时监控中心还把认为存在的威胁发送到规则编写模块中改写防御规则，以便应对出现的危险。

实验网段根据监控中心发送来的消息，恢复监测网段的现场，跟踪程序的运行机制，判断程序是否是可靠运行或者存在的问题，便于明白存在的问题原因。如果存在问题，返回问题到监控中心；如果存在不能决断的问题，可以通知管理员参与或者加入专家分析系统。

漏洞库是提供了一个漏洞的发现库，以提供给实验网段进行检测，提前判断出可能出现的攻击行为，加强网络的防范能力。

规则编写是根据监控中心发送的信息，来生成防火墙新的规则，并且发送给防火墙控制中心。

防火墙控制中心根据产生的规则，判定处理运行的程序，是否先让监测网段的各个主机查看是否具有该危害的程序，如果有就首先删除程序，然后监测网段上各个主机的防火墙接受规则。

入网控制是网络的信息出入口，组成可以是有路由器、防火墙等组成的网络信息拦截防御体系，控制曾经已经判断为病毒的数据而进行实施拦截。

日志文件主要收集被监测网段内日志或者网络出现的异常行为，与此同时还记录判定方案程序的事件。

数据挖掘的功能是分析日志文件中可能出现的网络安全不易察觉的威胁或者对判定方案程序的分析，检测查看是否判定方案程序分析的合理性，以利于将来对判定方案程序的修改与完善。

病毒检测的主要功能是分析数据挖掘的结果是否属于病毒，如果是病毒就发送给监控中心。同时分析有监控中心发送过来的数据，以便及时发现存在的安全隐患性问题。

攻击检测是分析数据挖掘的结果，查看是否有出现的攻击，以提前发现攻击的出现；同时提供系统分析结果给专家分析模块，以便它们提供更加正确的判定信息；同时分析监控中心发生来的信息。

专家分析对数据挖掘的结果进行专家的判断，查看是否出现攻击行为。同时把发现的结果发送到监控中心进行处理，以加强网络防范行为。

3 检测算法的设计

需要一种既利用 t 子密钥恢复一个密钥又能够进行数字签名的密钥方案，选择方式可以利用 ELGamal 密码体制，或者利用椭圆曲线密码体制。论文选择了基于椭圆曲线的加密体制。与 Shamir 门限方案类似，t 个点唯一地确定 t-1 次多项式 h(x)，所以秘密密钥 K 可以从 t 个共享中重构出，但从少于 t 个点无法确定 h(x)或者密钥 K。给定 t 个点唯一地确定 h(x)。其为 $h(\forall x)=y_{i_s}\prod_{\substack{j=1\\ j\neq s}}^{t}\frac{\forall x-x_{i_j}}{x_{i_s}-x_{i_j}}$，对 $\forall x$ 随机选取，其值 $\forall x$、$h(\forall x)$、可疑线程编号用数字签名以及加密传送。

$\forall x$、$h(\forall x)$ 用随机选取的对称密钥 k 加密，密钥 k 用椭圆曲线加密传送 CA 中心，解密可以得到 $\forall x$、$h(\forall x)$、随机对称密钥 k、可疑线程编号。

算法流程如下：

①选择随机数对称密钥 k。（AES 加密或者自己构造一个加密体制加密）

②对 $\forall x$、$h(\forall x)$、可疑线程编号使用对称密钥 k 加密。

③ $\forall x$、$h(\forall x)$、可疑线程编号、密钥 k、密钥 k 用椭圆曲线加密等进行数字签名

④解密用椭圆曲线加密密钥 k 。

⑤解密 $\forall x$、$h(\forall x)$、可疑线程编号。

⑥进行数字签名验证。

⑦若验证通过，认可一次危害出现或者出现攻击。

⑧等待其他线程报告，超过 t 次可以认为是可能具有危害性的危险线程。

⑨发送到测试网络等待判决，判决认为是事实危险线程。

⑩发送到各个主机对该程序进行删除或者清理；同时发送到防火墙，填加防火墙规则进行阻止。

4 安全性测试分析

针对网络的病毒检测个数、误警次数、有效报警次数、预见病毒个数、实际有效病毒等数据进行了统计分析。可以表 1 看出，从预见病毒个数到实际有效病毒的个数看，系统还是具有一定的成效，能够有效的防止了病毒的入侵；不过系统误警次数还是比较高的，花费的代价还是比较可观的，与系统的安全性能相比，还是值得的。

Table 1. System resulting data of standard expriment
表 1. 网络检测统计表

检测次数	病毒检测个数	误警次数	有效报警次数	预见病毒个数	实际有效病毒数
一	67	837	38	13	4
二	56	659	46	23	6
三	68	789	59	21	5
四	62	850	74	34	6

经过一段时间的试用与测试，证明了网络有一定的预警能力，对有些未出现的攻击有一定的抵抗能力，对网络的安全性能有明显的提高与改善，同时对于网络的管理要求不高，不需要网络管理人员有较好的网络安全意识与网络安全危害的敏锐性，可以较好地保护好自己组建的网络方案，该方案加强了网络的防范攻击，可以改变被动攻击的局面，侧重了网络的自我防卫，集防火墙功能与入侵检测功能为一体，加之主动的防范攻击策略，有效地抑制了网络中出现的破坏性行为，有效地保护了网络的安全性。

不足之处是需要大量的数据才能够察觉有害的新型攻击类型，同时对网络已经存在的危害行为仅仅能够抑制，但不能对已经瘫痪的计算机实行自我调整，

978-1-935068-09-9 © 2010 SciRes.

同时对网络存储空间要求较大，才可能实现数据分析与挖掘，从而发现可能存在的更深层次的攻击。

5 结束语

该论文构造出了网络的纵深防御体系结构，给出了网络自我防御能力加强的关键就是判断与识别网络的威胁和存在的破坏程序，给出了关键的分析设计，加强了网络的安全防范能力与自我侦察能力，有效地保护了网络的安全性，改变了网络仅仅依靠防火墙对网络防御被动的防御问题，入侵行为的检测功能得到加强应用，很好地起到保护内部网络的效果。

References (参考文献)

[1] Raman Kumar，Harsh Kumar Verma. An Advanced Secure (t, n) Threshold Proxy Signature Scheme Based on RSA Cryptosystem for Known Signers. 2010 IEEE 2nd International Advance Computing Conference.

[2] Zhang Fangguo and so on. Based on elliptic curve digital signa-ture and blind signature[J].Transactions of Communica-tions, 2001,(8), P22-28.
张方国等.基于椭圆曲线的数字签名与盲签名[J].通信学报，2001,(8), P22-28.

[3] Zhang Zhaozhi, modern cryptology foundation[M],Beijing Uni-versity of Posts and Telecommunications Publishing house，2005.P236-240
章照止,现代密码学基础[M]，北京:北京邮电大学出版社，2005.P236-240

[4] Yang Yixian, Sun Wei, Niu Xinxin. Modern cipher new theory [M]. Beijing: Science publication,2002:P113-119.
杨义先，孙 伟，钮心忻.现代密码新理论[M].北京:科学出版社,2002:P113-119.