

一种基于门限签名的可靠蠕虫特征产生系统

向 继 高 能 荆继武

(信息安全国家重点实验室(中国科学院研究生院) 北京 100049)

摘 要 蠕虫特征产生系统是一种利用大量的、分布式部署在 Internet 的监控器共同协作,从而产生和发布有效的蠕虫特征的新型安全系统.该系统产生的蠕虫特征可以配置到防火墙或者路由器中以遏制蠕虫的传播.虽然它是一项比较有效的对抗蠕虫的安全技术,但是其自身存在一些严重的安全问题,特别是当一个或者少数几个系统节点被黑客控制后,它们可能被利用来阻碍系统产生蠕虫特征,篡改系统发布的特征甚至误导系统发布虚假的特征,这些都会严重影响系统产生特征的可靠性.针对现有系统存在的问题,作者提出了一种基于门限签名的可靠蠕虫特征产生系统,它通过数字签名技术保证系统产生的蠕虫特征是可验证的,同时,为了避免单点失效和提供高可靠性,作者利用一种改进的双层门限签名机制来产生签名.可靠性分析表明,新系统能够抵抗攻击者对部分系统节点的各种形式的攻击,在可靠性上优于现有的主流蠕虫特征产生系统.

关键词 蠕虫特征产生系统;单点失效;数字签名;门限签名

中图法分类号 TP309

DOI号: 10.3724/SP.J.1016.2009.00930

A Dependable Worm Signature Generation System Based on Threshold Signature

XIANG Ji GAO Neng JING Ji-Wu

(State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100049)

Abstract Worm Signature Generation System (WSGS) is a new sort of security systems that generate and disseminate worm signatures by deploying many monitors at different sites of the Internet. The signatures can be used by firewalls or content filters to contain the spread of worms. While it is a promising technology to combat with Internet worms, WSGS has some serious security problems. When one or a few system components are compromised and controlled by attackers, they may conceal, modify or forge worm signatures, thus make the signatures generated by WSGS undependable. Motivated by the security challenges of existing systems, this paper presents a dependable WSGS based on threshold signature technology, which generates verifiable worm signatures through digital signature, so that any parties receive the signatures can verify their correctness. Furthermore, to avoid single point of failure and provide highly attack resilient, it applied an improved two-tier threshold signature scheme to generate digital signatures. Security analysis shows that the system can tolerant various attacks to a few components.

Keywords worm signature generation system; single point of failure; digital signature; threshold signature

收稿日期:2007-05-09;最终修改稿收到日期:2008-12-29. 本课题得到国家自然科学基金(60573015)、国家“八六三”课题“跨域认证授权关键技术与系统”(2006AA01Z454)资助. 向 继,男,1976年生,博士,主要从事恶意代码防范、安全协议等方面的研究工作. E-mail: jixiang@lois.cn. 高 能,女,1976年生,博士,讲师,主要从事蠕虫攻击、数据挖掘技术等方面的研究. 荆继武,男,1964年生,博士,教授,博士生导师,主要从事信息与网络安全方面的研究与开发工作.

1 引 言

网络蠕虫是一种恶意的计算机程序,能够不断进行自我复制,并且通过网络进行传播,对网络和计算机造成严重破坏.随着 2001 年红色代码和尼姆达蠕虫的相继爆发,新的、危害程度更高的网络蠕虫不断出现,日益成为因特网的头号安全威胁.

最近,研究者们提出了一种分布式的蠕虫特征产生系统方案来对抗网络蠕虫,它的基本原理是在 Internet 中散布很多个监控器,这些监控器能够检测到蠕虫传播行为,并能够识别蠕虫特征,例如传播蠕虫的计算机的 IP 地址、蠕虫传播载荷的特征串等等,然后该系统利用汇集器收集来自于这些监控器的蠕虫特征,进而产生可用于遏制蠕虫传播的特征,例如 IP 地址黑名单、蠕虫特征串等等.这些特征可以发布到防火墙或者路由器中,从而阻断蠕虫在 Internet 中的传播.目前主流的蠕虫特征产生系统主要包括 EarlyBird^[1]、Domino^[2]、WormSheild^[3]等,实验表明这些系统对于抑制蠕虫的传播具有较好的效果.

但是上述这些系统在设计时主要考虑蠕虫抑制的有效性和系统可扩展性,而较少关注系统自身的安全性.有的系统虽然引入了一些安全方案,例如 WormShield 中提出利用 DHT 技术来组织系统节点,从而使系统能够容忍部分节点失效;Domino 中提出利用 PKI/CA 技术来实现节点之间的认证,从而避免假冒节点攻击.但是这些安全方案无法防御更加高明的攻击,例如黑客攻占并控制部分系统节点,进而阻挠系统产生蠕虫特征,甚至误导系统产生虚假的特征.如果这种攻击一旦得逞,将会对系统产生的蠕虫特征的可靠性造成严重损害.考虑到蠕虫特征的系统节点分布在 Internet 的各处,而且一般由不同的机构维护,所以安全性问题十分突出.

针对这一问题,本文首先对现有的蠕虫特征产生系统方案进行统一化建模,并以该模型为基础来分析系统所面临的主要安全威胁,进而提出保障系统在 Internet 环境下安全运转所必需的两个核心安全需求:避免系统节点单点失效和产生可验证的蠕虫特征.

为了满足上述两个安全需求,本文提出了一种基于门限签名的可靠蠕虫特征产生系统模型,它利用数字签名技术和门限签名技术来保证蠕虫特征收集、汇

总和发布等各个环节的安全.与现有的系统相比,该系统能够容忍部分节点被黑客攻占甚至完全控制,从而能容忍高明的黑客攻击,在可靠性上大大增强.

传统的门限签名技术因其主要应用在 CA 系统等对扩展性要求较低的系统中,所以对扩展性支持不强,随着系统节点的增加,系统管理的密钥数量迅速膨胀.而本文提出的系统对扩展性要求很高,系统节点数量可以达到数千甚至上万,系统维护的密钥数量将达到几百万个,极大地降低了系统的可用性.所以本文提出了一种改进的双层门限签名技术,在不降低系统安全性的情况下,保证系统维护的密钥数量只以线性方式增加,提高了系统的可扩展性.

本文采用分析方法,通过定量分析以及与现有系统的可靠性特征比较表明,该系统在可靠性上明显优于现有系统,更加适合在 Internet 等复杂和恶劣网络环境下布置.

本文第 2 节提出了一般化的蠕虫特征产生系统模型,并结合该模型分析系统的安全威胁和安全需求;第 3 节给出了可靠蠕虫特征产生系统的设计;第 4 节描述了改进的两层门限签名的设计;第 5 节对该系统的可靠性进行分析,并与现有系统进行安全特征比较;第 6 节是结论部分.

2 蠕虫特征产生系统模型及安全需求

2.1 蠕虫特征产生系统一般模型

目前主流的蠕虫特征产生系统主要包括 Early-Bird, Domino, WormSheild 等,虽然这些系统在节点组织和结构上都有所不同,但大体上我们可以都将其一般化为如图 1 所示的模型.

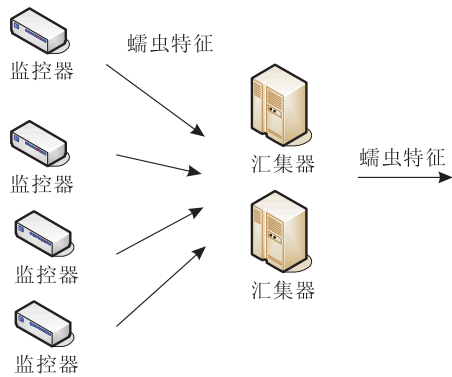


图 1 蠕虫特征产生系统一般模型

蠕虫特征产生系统一般由许多监控器和若干汇集器组成:

(1) 监控器. 一般布置在网络的边界处, 它的作用是检测蠕虫的传播行为, 并试图发现蠕虫的传播特征, 根据所使用的检测算法的不同, 监控器可以检测到各异的蠕虫传播特征. 检测到蠕虫传播后, 监控器将发现的蠕虫特征以及该特征出现的频率等参数提交给汇集器.

(2) 汇集器. 汇总来自所有监控器的蠕虫特征, 如果发现某一特征出现频率超过某一阈值, 就认为该特征表征了一种正在传播的网络蠕虫, 可以作为过滤规则发布到防火墙或者路由器中, 以遏制蠕虫的传播.

在这个一般化模型框架下, 具体的不同系统有着各自的特点, 这些特点会影响系统的安全性和可扩展性:

(1) EarlyBird. 只有一个汇集器汇总来自所有监控器的特征.

(2) Domino. 不同汇集器管理不同的监控器组. 汇集器之间利用广播共享信息.

(3) WormSheild. 监控器自身同时也是汇集器. 监控器采用 DHT 技术进行组织.

2.2 安全威胁和安全需求

蠕虫特征产生系统自身会面临来自各个方面的攻击的威胁, 一般黑客可能从下面几个方面攻击此类系统.

(1) 攻击监控器. 黑客可能设法使监控器失效, 假冒成一个监控器或者控制合法监控器向汇集器发送虚假的信息.

(2) 攻击通信信道. 篡改监控器发送给汇集器的蠕虫特征.

(3) 攻击汇集器. 设法使汇集器失效, 假冒成一个汇集器或者控制合法的汇集器篡改监控器发送来的特征, 甚至私自发布虚假的蠕虫特征.

(4) 攻击特征发布. 在蠕虫特征发布后篡改特征.

这些攻击一旦成功, 可能导致两种后果: 阻碍系统及时的发布蠕虫特征, 或者控制系统发布错误甚至虚假的蠕虫特征. 相对而言, 第二种后果更为严重, 因为该系统产生的特征一般会被 Internet 中数以千计的防火墙或者路由器所采用, 虚假的特征势必会极大地影响该系统的可靠性.

虽然在现有的系统中引入安全认证机制可以一定程度上提高系统的安全性、遏制节点假冒等攻击行为, 但是由于在设计之初较少考虑安全性, 所以现

有系统对下面两类攻击还是比较脆弱:

(1) 篡改特征. 现有系统产生的蠕虫特征没有采用任何保护机制, 所以容易在产生、存储或者发布时被篡改.

(2) 节点被黑客控制. 现有系统对节点完全信任, 这样只要有一个节点(监控器或汇集器)被黑客攻占并控制, 它就可以利用该节点使系统发布错误甚至虚假的蠕虫特征.

针对这一问题, 我们认为对于蠕虫特征产生系统, 一个更加完善的安全解决方案除了实现一些基本的安全功能之外, 还必须满足如下两个核心的安全需求:

(1) 避免系统单点失效.

冗余是解决单点失效问题的一个最直接的途径, 它能够实现当某一个系统节点失去作用后, 系统中会有备份节点取代它的作用. 但是简单的冗余并不能够解决节点被控制的单点失效问题, 因为此时节点看似工作“正常”, 但是它提供的信息都是虚假或者错误的.

为了解决这一问题, 要求系统在进行决策(产生蠕虫特征)时不能仅仅依赖一个或者少数几个节点提供的信息, 因为它们有可能被黑客控制而提供虚假的信息.

同时, 避免单点失效还要求从总体上考虑系统的安全性, 不能只重视一部分系统的安全而忽视另一部分. 例如, 重视保护监控器和汇集器, 但是忽视了对特征发布的保护, 这样黑客就可能攻击特征发布环节, 从而同样可以达到攻击整个系统的目的.

(2) 系统产生的蠕虫特征可验证.

考虑到蠕虫特征产生系统所产生的特征可能会被 Internet 中数以千计的防火墙和路由器所采用, 如果特征自身不可验证, 那么它很容易在产生和发布环节被恶意篡改.

实现蠕虫特征可验证的最直接的途径是利用数字签名, 即对系统产生的所有蠕虫特征进行数字签名. 但是简单的数字签名不能完全解决问题, 必须谨慎的设计和解决若干关键问题, 例如由谁签名? 如何签名? 如何避免单点失效? 如果进行数字签名的那台服务器失效, 系统的安全性同样会丧失, 所以必须将蠕虫特征可验证和避免单点失效问题一起考虑和解决.

在 Costa 等人提出的 Vigilance 系统^[4]中也认识到特征可验证的重要性, 但是该系统是一个基于

主机的解决方案,蠕虫特征只能够在有漏洞的主机上才能够验证,而作为蠕虫特征产生系统产生的特征更多的是被防火墙和路由器所使用,所以不能够采用 Vigilance 系统中所采用的方法.

3 基于门限签名的可靠蠕虫特征产生系统

3.1 系统架构和工作原理

基于上一节中对现有蠕虫特征产生系统安全威胁和安全需求的分析,我们设计并实现了一种基于门限签名的可靠蠕虫特征产生系统,它利用数字签名技术和门限签名技术来保证蠕虫特征收集、汇总和产生发布等各个环节的安全.

该系统的架构如图 2 所示.

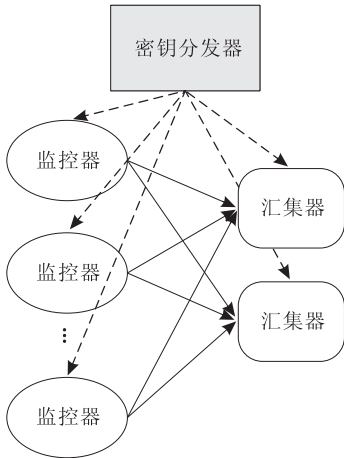


图 2 基于门限签名的可靠蠕虫特征产生系统结构

系统中有一个离线的密钥分发器,在系统初始化时,它会产生一对公-私钥对,利用公钥向可信的认证机构 CA 申请一个数字证书,然后将数字证书发布给防火墙和路由器.接下来密钥分发器利用门限签名技术将私钥进行拆分,然后分别分发给监控器和汇集器,这样只有一定数量的监控器和汇集器共同合作才能够产生合法的数字签名.

监控器检测到蠕虫的传播特征后,利用自己拥有的部分私钥对特征进行部分签名后提交给汇集器,当汇集器收集到超过一定门限的监控器对于同一蠕虫特征的部分签名后,合成拥有完整签名的蠕虫特征,并发布出去.防火墙和路由器接收到蠕虫特征后,可以利用系统的数字证书验证系统产生的特征的正确性.

由于使用了门限签名技术,该系统拥有如下的一些安全特性.

(1) 系统产生的蠕虫特征是经过签名的,任何人或者设备都可以验证它的正确性,这样就有效地杜绝了特征在发布时被恶意篡改.

(2) 少量监控器或者汇集器被控制,无法诱骗系统产生虚假的蠕虫特征,因为少量的被控制的监控器无法产生足够数量的合法部分签名,也就无法合成拥有完整签名的特征.同样汇集器也无法私自产生蠕虫特征.

(3) 少量监控器或者汇集器被黑客控制无法阻碍系统产生准确的蠕虫特征,由于有签名保护,监控器和汇集器都无法篡改别人产生的蠕虫特征.

下面结合一个具体的例子说明该系统的工作过程,该例子中假定系统检测的蠕虫传播特征为传播蠕虫的计算机的 IP 地址.同时假定系统的门限值为 3,即至少有 3 个监控器合作才能够合成合法的数字签名.

图 3 显示了系统的工作过程,首先密钥分发器将私钥拆分后分别发布给监控器和汇集器(具体的私钥拆分方法和签名合成方法将在第 4 节中介绍).当一个蠕虫传播时,监控器 1 检测到 IP 地址 203.12.34.2 为可疑的传播蠕虫的计算机,于是它利用自己拥有的部分私钥对该 IP 地址进行签名,然后将 IP 地址和部分签名结果发送给汇集器.同时监控器 2 发现了可疑的 IP 地址 203.12.34.2 和 187.78.65.1,监控器 4 发现了可疑的 IP 地址 203.12.34.2,它们都利用自己的部分私钥签名后发送给汇集器.汇集器接收到来自这些监控器的汇报后,发现对 IP 地址 203.12.34.2 汇报的数量超过门限值 3,所以它就利用门限签名方法对部分签名进行合成,产生系统对该 IP 地址的完整的签名,这样这个 IP 地址与其签名一起可以作为 IP 地址黑名单的一部分发布给防火墙和路由器进行蠕虫阻断.

如果检测到的蠕虫传播特征是蠕虫载荷的特征串,上述方法同样适用,这时,监控器汇报给汇集器的是检测到的蠕虫载荷特征串以及对特征串的部分签名,当接收到的对同一特征串的不同部分签名的数量超过门限值,汇集器就可以合成最后完整的签名.

由于在本系统中,只有对同一个传播特征的部分签名才能够合成完整的签名,这样就对传播特征的产生提出了一定的要求,即要求如果一个蠕虫在网络中传播,多个不同的监控器会同时检测到,并且产生同一个蠕虫传播特征.通过对蠕虫传播特性的分析,这一要求是不难达到的.蠕虫一般采用随机扫描的方式进行传播,这样一台感染蠕虫的计算机就

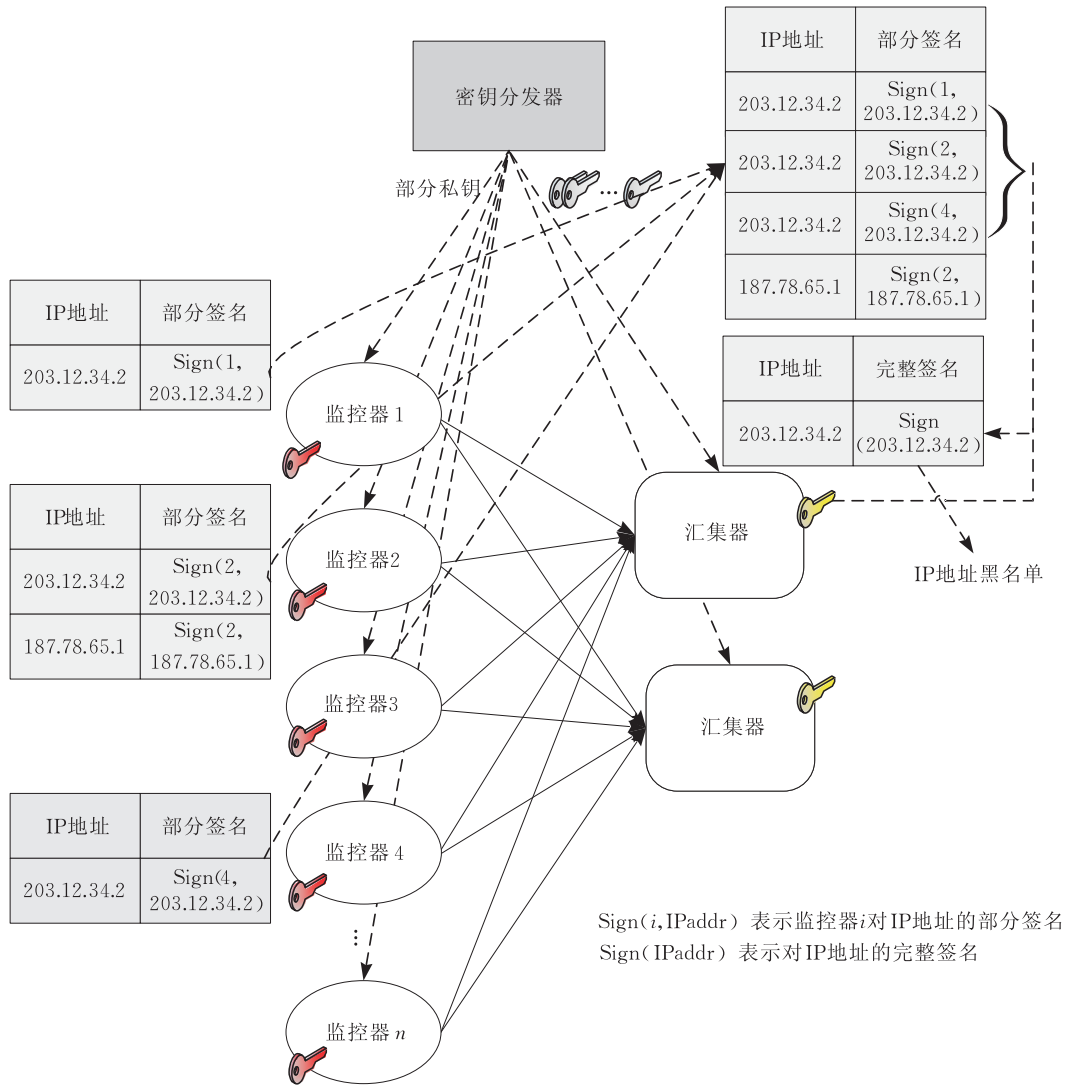


图 3 系统工作原理示意图

会试图访问 Internet 的多个不同网络,只要监控器的数量足够多,会被多个不同的监控器检测到.同时蠕虫一般采用自我复制的方式传播,这样不同监控器分析出来的特征串也是一致的.一个例外是变形(polymorphic)蠕虫^[6],它在复制时会改变载荷的内容,这样就可能会导致不同的监控器产生不同的特征串.所以对于变形蠕虫,可疑 IP 地址检测方法更为有效.

3.2 汇集器的组织

采用了门限签名机制后,少数被黑客控制的监控器和汇集器都无法产生错误或者虚假的蠕虫特征,但是门限签名技术本身不能够解决攻击者试图阻止蠕虫特征产生的问题,这一问题的解决主要依赖于汇集器节点的组织,原因如下:

(1)少量的监控器被黑客控制并不能够有效地阻止系统产生蠕虫特征,因为它至多能做到不将自

己发现的特征发送给汇集器,但不能阻止别的监控器发送特征或者篡改别的监控器的特征.考虑到监控器数量很多,少数几个监控器不提交特征并不能够阻止系统及时地产生有效的蠕虫特征.

(2)如果汇集器组织不当,黑客则有可能通过控制少量的汇集器来达到阻止系统产生部分甚至全部蠕虫特征的目的.例如系统中只有一个汇集器(EarlyBird 系统采用的方法),或者系统只有少数几个汇集器,分别管理不同的监控器组(Domino 系统采用的方法),如果有一个汇集器被黑客控制,就可能会有相当一部分甚至全部的监控器汇报的特征被丢弃,这样就会有有很多有效的特征无法产生和发布.

解决这一问题的一个最直接的途径是使监控器将其发现的特征发送给每一个汇集器,这样除非黑客控制所有的汇集器,否则他不能够阻止系统产生有效的蠕虫特征.但是这种方法的缺点是网络通信

量大, 汇集器的处理负荷大。

为了降低汇集器的处理负荷, 我们将汇集器用 Chord 方式进行组织。其组织方式如下: 为每个蠕虫特征和汇集器节点都分配一个标识符 ID, 这个 ID 分别通过对节点 IP 地址和蠕虫特征 Hash 计算以后获得。然后系统按照如下的方式来存放蠕虫特征, 将一个蠕虫特征 K 放在一个节点当且仅当这个节点的标识符是大于等于蠕虫特征 K 标识符的第一个节点。Chord 方案的优点是能够容忍节点失效, 如果一个节点失效, 那个标识符仅次于它的节点就会自动替代它。

但是基本的 Chord 方案也存在一个缺点, 那就是一个蠕虫特征只存放在一个汇集器节点上, 对于这一个蠕虫特征来说存在单点失效问题, 因为如果存放该特征的汇集器节点被黑客控制, 这个蠕虫特征就无法发布。为了解决这一问题, 我们对 Chord 进行扩展, 使得一个蠕虫特征能够存放在两个甚至更多的汇集器节点上。

扩展的具体方法是:

- (1) 首先对接收到的蠕虫特征进行 Hash 计算, 获得该特征的标识符 ID, 从而可以确定该特征应当存放的第一个节点。
- (2) 接下来对特征的标识符 ID 再进行一次 Hash 计算, 获得一个新的标识符 ID, 通过这个 ID 可以获得另一个存放该特征的节点。
- (3) 依此类推, 获得所有存放该特征的节点。将蠕虫特征发送给这些节点保存。

改进的基于 Chord 的节点组织机制如图 4 所示, 图 4 中显示了节点 3 接收到一个蠕虫特征 K , 通过计算后分别提交给节点 1 和节点 4 保存。

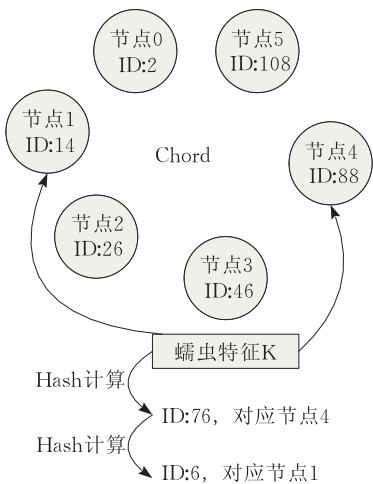


图 4 汇集器节点组织示意图

通过使用 Chord 机制进行组织以后, 能够将系统收集的蠕虫特征平均地分配到不同的汇集器中, 同时监控器也不需要发现发现的蠕虫特征提交给所有汇集器, 而只需要提交给两个或者少数几个即可。这样就减轻了每个汇集器处理的负荷, 同时也减少了网络通信。

4 改进的双层门限签名方案

我们提出的可靠的蠕虫特征产生系统, 需要门限签名技术的支持。目前主流的门限签名技术的一个缺陷是可扩展性差, 随着系统节点的增加, 系统维护的密钥数量迅速膨胀。目前门限签名主要应用在 CA 等系统中, 这些系统往往只拥有几十个节点, 所以扩展性问题不太突出, 而本文提出的系统对扩展性有很高的要求, 监控器的数量要求达到几千甚至上万个, 在这种情况下, 传统的门限签名技术难以满足实用化要求。

以文献[6]中经典的 ITTC 门限签名方案为例, 每个监控器需要维护的密钥数量为 C_{k-1}^{t-1} , 其中 t 为门限值, k 为监控器的数量。如果设 $k=1000, t=3$, 则可以计算出每个监控器需要管理约 50 万个密钥, 如果设 $k=2000$, 这一数字将增长到 200 万个。

为了满足我们设计的系统的实用化需求, 需要提高门限签名方法的扩展性, 为此我们采用了一种两层结构的门限签名技术^[7], 除了监控器拥有部分私钥外, 汇集器也拥有部分私钥。使用两层结构后, 监控器只需要管理少数几个部分私钥。

但是在原方案中, 随着监控器数量的增多, 汇集器需要管理的密钥数量仍然十分庞大。所以我们对原来的密钥拆分方案进行了改进, 在不降低安全性的情况下大大降低了汇集器维护的密钥的数量, 使其适合于在我们设计的蠕虫特征产生系统中部署。

我们采用的双层门限签名方案基于 RSA 算法, 我们将私钥表示为 d , 公钥表示为 e 和 N 。假定系统中有 k 个监控器和若干汇集器。设定系统门限值为 t , 即至少有 t 个监控器和 1 个汇集器共同合作才能够合成签名。

4.1 原有私钥拆分方案

原方法的私钥拆分方法如下:

首先, 密钥分发器随机选择 k 个随机数 d_1, d_2, \dots, d_k , 然后将它们分别分发给 k 个监控器。

下面对于每一个 t 元组 (一个由任意 t 个监控

器构成的组合), 密钥分发器计算一个特定的合成部分私钥, 记为

$$c_j = d - (d_{i_1} + d_{i_2} + d_{i_3} + \cdots + d_{i_t}),$$

其中 i_1, i_2, \dots, i_t 表示属于这个 t 元组的 t 个监控器的序号. 这样对于 k 个监控器, 就会有 C_k^t 个 t 元组和 c_j , 密钥分发器将所有 c_j 分发给汇集器.

在原方法中, 虽然监控器只需要维护一个密钥, 但是汇集器需要维护 C_k^t 个, 如果 k 数量很大, 密钥数量是不可接受的, 例如设 $k = 1000, t = 3$, 则有 $C_k^t \approx 1.7$ 亿个.

4.2 改进的私钥拆分方案

我们对原方法进行了改进, 通过在每个监控器中存放多个部分私钥, 从而极大减少汇集器中管理密钥的数量. 假设有 k 个监控器, 每个存放 m 个部分私钥 ($m < t$).

开始时, 密钥分发器同样随机选择 n 个随机数 d_1, d_2, \dots, d_n , 有 $C_n^m \geq k$, 然后按照如下的方式将它们分别分发给 k 个监控器.

1. 密钥分发器随机选择 m 个在 1 到 n 之间的数, i_1, i_2, \dots, i_m , 然后将 $d_{i_1}, d_{i_2}, \dots, d_{i_m}$ 分发给某一个监控器 h .
2. 按照上述步 1 为每一个监控器分发 m 个部分私钥.
3. 分发时保证没有两个监控器拥有完全一样的一组部分私钥.
4. 监控器都互相不知道各自拥有的部分私钥的序号.

接下来, 密钥分发器计算 C_n^t 个 c_j , 然后分发给汇集器.

改进后, 同样设置 $k = 1000, t = 3, m = 2$, 这样我们有 $n = 46, C_n^t = 15180$ 个, 即使 k 增加到 2000, 有 $m = 64, C_n^t = 41664$, 增长幅度不大, 而且与原有的双

层门限方法相比, 汇集器需要管理的密钥的数量大为减少.

4.3 签名合成方案

合成签名的过程如下:

1. 监控器发现蠕虫传播特征 M 后, 利用其拥有的部分私钥, 计算部分签名 $y_i = M^{d_i} = (\text{HASH}(M))^{d_i}$, 然后将 M 和部分签名发送给汇集器.
2. 当收集到超过门限数量的监控器发来的对同一传播特征的部分签名后, 汇集器分别选择这些监控器发来的部分签名中的一个, 构成一个 t 元组, 然后从本地存储的部分私钥中查找与该 t 元组相对应的 c_j , 并计算

$$R = (\text{HASH}(M))^{c_j} \times \prod_{i=1}^t y_i.$$

很容易验证

$$R = (\text{HASH}(M))^{c_j + d_{i_1} + d_{i_2} + \dots + d_{i_t}} = (\text{HASH}(M))^d,$$

R 即为对 M 的完整签名结果.

采用了改进的密钥拆分方法后, 上述合成方法存在一个安全隐患, 那就是如果一个监控器知道其他监控器拥有的部分私钥的序号, 那么它就有可能假冒别的监控器. 我们可以通过在汇集器中进行完备计算防止这一攻击, 汇集器接收到所有 $t \times m$ 个部分签名后, 将它组成 m 个组, 对每一个组中包含来自于 t 个不同监控器的一个部分签名. 汇集器对每一组查找对应的 c_j , 并计算最后的签名结果, 如果有一组产生错误的签名, 则整个签名构造过程失败. 采用完备计算后, 门限签名的安全性不会有所降低.

图 5 所示的两幅图总结了改进方案与传统的 ITTC 方案相比在扩展性方面的优势. 其中假定门限 $t = 3, m = 2$.

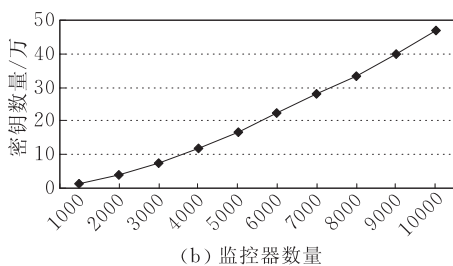
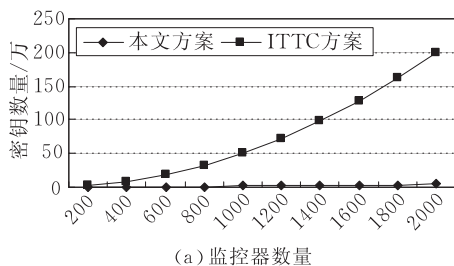


图 5 改进方案扩展性优势

图 5(a) 显示了不同方案在监控器数量从 200 到 2000 变化时, 系统需要维护的密钥的数量的变化情况. 从图 5 中可以看出, 本文的改进方案与 ITTC 方案相比, 密钥数量随监控器数量增长的幅度变化非常小.

图 5(b) 显示了本文方案在监控器数量从 1000 到 10000, 系统密钥数量的变化情况, 可以看出, 密

钥数量的增长基本上呈一个线性方式.

5 系统可靠性分析

5.1 可靠性分析

第 2 节中提出了 3 种黑客攻击方法: 攻击监控器、汇集器、信道和已发布的特征. 在本文提出的系

统中,已发布的特征是经过数字签名保护的,所以黑客无法攻击已发布的特征.同时监控器发送给汇集器的特征也包含部分签名,黑客虽然可以通过攻击信道篡改或者私自发送虚假的特征,但是由于在汇集器处无法合成完整的签名,虚假的特征不会被发布.黑客也有可能利用攻击信道发起重放攻击,但是这种攻击很容易在特征中包含时间等信息来防止.所以本系统能够有效地阻止黑客对信道和已发布特征的攻击.

下面主要分析本系统对监控器和汇集器节点遭受攻击的容忍能力.我们首先对黑客攻击方式按照其目的、强度和对象的不同进行划分,然后分别分析本系统对每种攻击方式的容忍能力.为了定量地分析,我们将容忍能力定义为“在某种攻击方式下,实现攻击目标所必需攻击的最少节点的数量”.

对于本系统,黑客攻击监控器或者汇集器有如下 3 个目的:

(1) 诱骗系统发布虚假特征,使监控器向汇集器发送虚假的特征,或者使汇集器直接发布虚假特征.

(2) 阻止系统发布合法特征,通过使监控器或者汇集器失效实现.

(3) 窃取节点存储的部分私钥,进而获得完整的系统私钥,这样就可以随意产生虚假特征.

黑客攻击节点有两种强度:

(1) 一种是完全控制节点攻击,即通过入侵手段占领节点,并可以控制节点进行任何操作.

(2) 另一种是非完全控制攻击,这时黑客无法完全控制节点,只是通过假冒节点、从外部向节点发起拒绝服务攻击等方式进行攻击.

实现完全控制攻击更加困难,但是攻击成功的可能性更大,例如同样使汇集器失效,非完全控制攻击常通过远程拒绝服务攻击来实现,这时汇集器网络通信往往中断,容易被监控器察觉到.一旦发现该汇集器无法访问,监控器可以选择使用其他的汇集器,这样攻击就无法得逞.而对于完全控制攻击,黑客可以控制汇集器按正常方式接收监控器发送来的特征,但是不进行任何签名合并操作,也不进行特征发布,这样监控器不容易察觉攻击行为,也就使得攻击更容易成功.

只有在完全控制情况下,才有可能窃取节点存储的部分私钥,而且一般窃取私钥要更加困难一些,因为节点可以采用硬件设备如加密卡或者 USBKey 来存储私钥,使黑客很难窃取.

- 黑客可能的攻击对象也包括下面 3 类:
- (1) 只攻击监控器;
 - (2) 只攻击汇集器;
 - (3) 同时攻击部分监控器和汇集器.

表 1 分析了黑客在不同的攻击目的、强度和对象情况下,系统对其攻击的容忍能力.表中“—”表示此种攻击方式对本系统无效.我们假定两层门限密码方案中门限为 t ,每个监控器保存 m 个部分私钥,同时在汇集器组织中,每个特征同时发布给 p 个汇集器.我们还假定系统中监控器和汇集器的数量都比较多,攻击者只能攻击其中少数的节点,不可能攻击所有的节点.

表 1 本文系统容忍能力			
攻击方式	只攻击 监控器	只攻击 汇集器	同时攻击监控器和 汇集器
发布虚假特征 (非完全控制)	—	—	—
发布虚假特征 (完全控制)	t	—	t 个监控器
阻止特征发布 (非完全控制)	—	—	—
阻止特征发布 (完全控制)	—	p	p 个汇集器
窃取私钥	—	—	$t-m+1$ 个监控器和 1 个汇集器

首先,非完全控制攻击对本系统无效,在非完全控制的情况下,黑客无法产生包含合法部分签名的特征,也就无法诱骗系统产生包含合法签名的特征.同时由于组织汇集器所使用的 Chord 协议能够容忍部分节点失效,当某个汇集器失效并被发现后,会自动用另一个汇集器来代替它,这样使少数汇集器失效并不能阻碍系统产生特征.

其次,对于完全控制攻击,想要发布虚假特征只有对监控器进行攻击才会效果,因为汇集器如果没有监控器的协助无法产生拥有合法签名的特征,而且由于门限签名的限制,只有黑客同时控制 t 个以上的监控器才有可能产生完整的签名.另一方面,如果黑客想要阻止系统发布特定特征,只有攻击汇集器才有效果,而且由于采用了改进的 Chord 协议,所以黑客必须同时控制至少 p 个汇集器.

最后,单独窃取监控器和汇集器的私钥都没有效果,只有同时窃取 $t-m+1$ 个监控器和至少一个汇集器的部分私钥,黑客才有可能获得完整的私钥.

通过上面的分析可以看出,我们的系统能够抵抗攻击者对部分系统节点的各种形式的攻击,即使在少数系统节点被黑客完全控制的情况下,系统仍

然能够产生正确的蠕虫特征,同时也不会被误导而产生虚假的特征.

5.2 与现有系统的可靠性对比

本节将我们的系统与现有主流的蠕虫特征产生系统 EarlyBird, Domino, WormShield 的可靠性进行对比. 其中重点比较不同系统对节点攻击的容忍能力.

表 2 分析了针对不同的系统,黑客在不同的攻

击目的、强度和对象情况下,为了实现攻击系统的目标所必须攻击的最少节点的数量. 表 2 中“—”表示此种攻击方式对该系统无效.

与前一节相比,表 2 中没有分析窃取私钥攻击方式和同时攻击监控器和汇集器的情况,因为这些攻击主要针对本文中的系统,而且对于其他系统根本没有必要采取如此复杂的攻击方式就可以达到攻击目标.

表 2 不同系统容忍能力比较

攻击方式	节点数量							
	本文系统		EarlyBird		Domino		WormShield	
	攻击监控器	攻击汇集器	攻击监控器	攻击汇集器	攻击监控器	攻击汇集器	攻击监控器	攻击汇集器
发布虚假特征(非完全控制)	—	—	1	1	—	—	1	1
发布虚假特征(完全控制)	t	—	1	1	1	1	1	1
阻止特征发布(非完全控制)	—	—	—	1	—	1	—	—
阻止特征发布(完全控制)	—	p	—	1	—	1	—	1

由表 2 中可以看出 EarlyBird 系统的可靠性最低,除了攻击少量监控器无法阻止系统发布特征外,以其他任何方式攻击系统中的任何一个节点都会导致黑客攻击目标的实现. EarlyBird 系统最大的安全问题在于只有一个汇集器,如果这个汇集器被攻击的话,整个系统的可靠性就会丧失.

Domino 系统由于引入了 PKI 认证机制,加强了节点之间的通信认证,这样就可以防止在非完全控制下,利用攻击系统节点诱骗系统发布虚假特征,但是一旦黑客完全控制某个节点后,认证机制就起不到任何作用,所以黑客的攻击目标仍然可以实现. 另一方面,Domino 系统采用多汇集器配置,提高了汇集器对攻击的容忍能力,但是由于采取不同汇集器分管不同监控器组的组织方式,如果某个汇集器失效,还是会有相当一部分监控器失去作用.

WormShield 与前两个系统相比优势在于利用 DHT 方式来组织节点,提高了对节点失效的容忍能力,如果一个节点失效后,可以自动由另一个节点来代替它的作用. 但是这仅限于容忍非完全控制方式的攻击,在完全控制方式下,节点失效很难被察觉,也就不会有另一个节点来代替它.

通过对现有系统的分析可以看出,通过引入 PKI 认证,DHT 组织等安全机制,系统可以较有效地容忍非完全控制方式的攻击,但是对于完全控制方式的攻击,现有系统都存在单点失效问题,而且没有很直接的解决办法. 而本文中提出的系统除了能够容忍非完全控制方式攻击外,还能够一定程度上容忍完全控制攻击,避免了单点失效.

本文中系统与现有系统相比在可靠性上的另一

个优势在于,本系统发布的特征是经过数字签名的,任何人都可以很方便地验证特征的正确性,而现有系统没有对发布的特征进行任何保护,导致特征很容易被篡改或者替换.

6 结 论

本文针对现有的蠕虫特征产生系统存在单点失效和产生的特征不可验证的问题,提出了利用数字签名技术和门限签名技术设计的一种可靠蠕虫特征产生和发布的系统化方法.

传统的门限签名的一般用途是将待签名的信息同时提交给多个实体进行部分签名,最后合成对该信息的完整签名. 而在我们的系统中,签名的信息是各个监控器自己发现的蠕虫特征,这些特征都汇总到一起,最后对同一个蠕虫特征的部分签名进行合成,从而产生对该蠕虫特征的完整签名. 根据我们的调研,目前还未见其他研究者采用类似的门限签名的用法.

另一方面,传统的门限签名应用中参与计算的实体比较少,所以每个实体管理的密钥数量不多. 但是在我们提出的系统中,监控器的数量可能达到一千个甚至更多,这样每个监控器管理的密钥数量会达到几十万甚至几百万之多. 为了提高门限签名方案的扩展性,我们没有采用主流的单层门限签名方案,而是采用了一种改进的双层门限签名方案,使得每个监控器只需要管理两个密钥,而汇集器也只需要管理几个.

除此之外,我们还利用改进的 Chord 协议来组

织汇集器节点,进一步提高了系统的鲁棒性. 根据可靠性分析,我们设计的系统能够容忍部分节点被黑客控制,并利用它来发起各种攻击,而系统的可靠性不会受到损害.

参 考 文 献

- [1] Singh S et al. Automated worm fingerprinting//Proceedings of the Usenix Symposium on Operating System Design and Implementation, Usenix Assoc., 2004; 45-60
- [2] Yegneswaran V, Barford P, Jha S. Global intrusion detection in the domino overlay system//Proceedings of the Network and Distributed System Security (NDSS 04). Internet Soc., 2004; 79-95
- [3] Cai Min, Hwang Kai, Kwok Yu-Kwong, Song Shanshan, Chen Yu. Collaborative Internet worm containment. IEEE Security and Privacy, 2005, 3(3): 25-33
- [4] Costa M, Crowcroft J, Castro M, Rowstron A, Zhou L, Barham P. Vigilante: End-to-end containment of Internet worms//Proceedings of the ACM Symposium on Operating System Principles (SOSP). 2005
- [5] Newsome J, Karp B, Song D. Polygraph: Automatically generating signatures for polymorphic worms//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, California, USA, 2005; 226-241
- [6] Wu T, Malkin M, Boneh D. Building intrusion tolerant applications//Proceedings of the USENIX Security Symposium. Washington, DC, USA, 1999; 74-87
- [7] Jing Ji-Wu, Liu Peng, Feng Deng-Guo, Xiang Ji, Gao Neng, Lin Jing-Qiang. ARECA: A highly attack resilient certifica-

tion authority//Proceedings of the ACM Workshop on Survivable and Self-Regenerative Systems. Washington, DC, USA, 2003; 53-63

- [8] Locasto Michael E, Parekh Janak J, Keromytis Angelos D, Stolfo Salvatore J. Towards collaborative security and P2P intrusion detection//Proceedings of the IEEE Workshop on Information Assurance and Security. 2005; 30-36
- [9] Provos N. Honeyd — A virtual honeypot daemon//Proceedings of the 10th DFN-CERT Workshop. 2003
- [10] Kim H A, Karp B. Autograph: Toward automated distributed worm signature detection//Proceedings of the Usenix Security Symposium, Usenix Assoc., 2004; 271-286
- [11] Wang Ke, Gabriela Cretu, Stolfo Salvatore J. Anomalous payload-based worm detection and signature generation//Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection (RAID 2005). Seattle, Washington, USA, 2005; 227-246
- [12] Perdisci Roberto, Dagon David, Lee Wenke, Fogla Prahlad, Sharif Monirul. Misleading worm signature generators using deliberate noise injection//Proceedings of the 2006 IEEE Symposium on Security and Privacy. Oakland, California, USA, 2006; 15-31
- [13] Chen Wei-Dong, Feng Deng-Guo. Some applications of sign-cryption schemes to distributed protocols. Chinese Journal of Computers, 2005, 28(9): 1421-1430(in Chinese)
(陈伟东, 冯登国. 签密方案在分布式协议中的应用. 计算机学报, 2005, 28(9): 1421-1430)
- [14] Chen Wei-Dong, Feng Deng-Guo. A group of threshold group-signature schemes with privilege subsets. Journal of Software, 2005, 16(7): 1289-1295(in Chinese)
(陈伟东, 冯登国. 一类存在特权集的门限群签名方案. 软件学报, 2005, 16(7): 1289-1295)



XIANG Ji, born in 1976, Ph. D. His research interests include malicious code prevention, security protocol, etc.

GAO Neng, born in 1976, Ph. D., lecturer. Her mainly engaged in the researches of worm attack data mining techniques, etc.

JING Ji-Wu, born in 1964, Ph. D., professor, Ph. D. supervisor. His mainly engaged in the research of information and network security.

Background

This paper is based on the research results of two projects, “Cross-Domain Authentication and Authorization Technology and System”, which is supported by the National High Technology Research and Development Program (863 Program) of China; and “Large Scale Worm Simulation Platform”, which is supported by National Natural Science Foundation of China.

After systematically researches on worm detection and prevention technologies, the authors found that worm signature generation technology and system is a active area, and

there are some mature algorithms and architectures for worm signature generation and distribution. And they also found that existing systems have the same problem: single point of failure. The problem means that If one or a few nodes of the system are controlled by hackers, the system may generated fake or non-dependable worm signature. To solve the problem, the authors modify the architectures and protocols of existing systems based on threshold signature, and design/implement a dependable worm signature generation system more suitable for Internet deployment.