第33卷 第19期 计 算 机 工 程 2007年10月
Vol.33 No.19 Computer Engineering October 2007
·安全技术· 文章编号：1000—3428(2007)19—0161—03 文献标识码：A 中图分类号：TP393

基于入侵容忍的网络取证系统设计

张有东[1]，江 波[1]，王建东[2]
(1. 淮阴工学院计算机工程系，淮安 223003；2. 南京航空航天大学信息科学与技术学院，南京 210016)

摘 要：现有的网络取证系统假设当发生入侵行为时系统仍然处于可靠的工作状态，未考虑系统状态变化对取证的影响。该文提出一个具有入侵容忍能力的网络取证系统INFS，分析了该原型系统的入侵容忍机制、基于SMP的取证控制机制和安全传输机制，以及取证agent、攻击回溯agent的工作机理，讨论了对应于不同系统状态的取证分析方法，提出了协同取证技术。

关键词：网络取证；入侵容忍；半马尔可夫过程；agent；协同取证

Design of Network Forensic System Based on Intrusion Tolerance

ZHANG You-dong[1], JIANG Bo[1], WANG Jian-dong[2]
(1. Department of Computer Engineering, Huaiyin Institute of Technology, Huaian 223003;
2. Institute of Information Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016)

【Abstract】 All the present network forensic systems assume that the system is still working on reliable state when intrusion occurs, and the effect of system state changes is not considered. This paper proposes a network forensic system with intrusion tolerance ability, INFS. Mechanisms and modules of this prototype system are presented, such as intrusion tolerance, forensic control based on SMP, security transition, forensic agent, attack trace agent and so on. This paper discusses different forensic analysis methods corresponding to different states, and brings forward the concept of cooperating forensic.

【Key words】 network forensic; intrusion tolerance; semi-Markov process(SMP); agent; cooperating forensic

在计算机网络犯罪手段不断升级的形势下，单靠网络安全技术将入侵者完全拒之门外是很困难的，人们已认识到，必须依靠法律制裁的威慑和技术上的防范来共同遏制网络犯罪，网络取证技术正是在这种形势下产生和发展的，它是一种动态的、实时的取证。

1 网络取证系统研究现状

目前，对于网络取证系统的原理和实现还处于研究阶段。最早应用于网络取证的是IDS技术。1999 年，Yuill等人详细阐述了具有证据分析能力的入侵检测系统的使用。2004 年，Payer提出了第 1 个实时入侵取证原型系统[1]。但是，目前所做的将二者结合的工作还很有限，IDS还没有设计出适应法律需要的证据链获取系统。基于agent技术，文献[2]提出了一种分布式网络取证系统框架，但该系统同时收集主机和网络数据的机制还不完善，也没有与访问控制、认证、加密以及其他安全机制建立有效的联系。

分析现有的网络取证原型系统可以发现，它们都基于一个共同的假设，即当发生入侵行为时，系统仍然处于可靠的工作状态，忽视了入侵发生时系统状态变化对取证的影响。事实上，在系统遭受攻击时，其网络通信已经处于不稳定、不安全状态，显然，在此状态下进行取证的可信度无法衡量，取证的可靠性甚至能否正常进行取证都无法保证。为解决这一问题，本文提出了一种基于入侵容忍(intrusion tolerance)的网络取证系统(INFS)。

2 INFS 系统结构

结合入侵容忍系统SITAR[3]和agent技术，INFS的结构如图 1 所示。其中，EA为证据分析服务器；ES为证据存储服务器。系统根据错误容忍技术，通过负载平衡、系统错误检测以及冗余资源等方法，保证了系统的可用性；通过使用虚拟公用IP地址池、隐藏内部配置细节、检测非授权访问和接受性测试等机制，保证了系统的机密性；通过服务器信息的可接受性测试和投票算法，保证了系统的完整性。同时，系统还具有在威胁性环境下的动态安全转换、可执行和自组织能力。

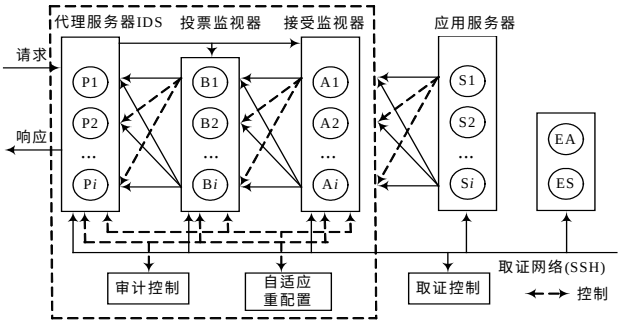

图 1 INFS 的体系结构

3 INFS 工作机制及主要模块分析

3.1 入侵容忍机制

入侵容忍系统具有及时自我诊断、自我恢复和自我重构的能力，使得系统在遭到入侵后，提供服务的应用服务器不

基金项目：江苏省高校自然科学基金资助项目(06KJD520019)
作者简介：张有东(1967－)，男，副教授、博士，主研方向：数据挖掘，入侵检测；江 波，讲师、硕士；王建东，教授、博士生导师
收稿日期：2006-12-26 **E-mail：**z.yd@163.com

仅能够在一定程度上抵抗攻击和发现入侵行为，更能在受到攻击或已经被入侵的情况下，仍然能提供既定的服务，必要时提供降级服务，并保持一定的安全底限。INFS的入侵容忍机制由虚框内的部件来实现，客户端的每个服务请求提交给某个代理服务器，这些服务器可以通过外部机制进行负载平衡，并且增加了第三方的IDS(Snort)。初始确认测试后，代理服务器发送请求到应用服务器，并通知相关的投票监视器和接受监视器。相应地，应用服务器返回的响应被发送到接受监视器，接受监视器再把响应发送到投票监视器集合，以决定最终的响应，最终的响应被向前传递到代理服务器再转交到远程客户端[3]。审计控制模块(ACM)通过审计活动监控系统中所有参与组件的操作，自适应重配置模块(ARM)从所有其他模块中接收入侵触发器信息、评估入侵威胁、预测和量化入侵容忍系统的机密性、完整性和可用性安全行为，并产生新的系统配置。

INFS 的入侵容忍机制使得系统能够在部分被入侵、性能下降等情况下维持最小等级服务，即系统在受到攻击时，不是完全崩溃，而是维持有限的原系统功能，从而满足对入侵行为进行动态取证的基本需要。

3.2 取证控制机制

取证控制机制通过取证控制模块(FCM)来实现，它是INFS 的核心。

3.2.1 FCM 的原理

FCM 取证控制的实现基于一个模型化的取证状态转移图机制(如图 2)，共有 5 个状态：正常状态(G)，易受攻击状态(V)，攻击状态(A)，功能退化降级状态(D)和失效保护状态(F)。如果攻击前的探测(probe)被检测到，系统将停留在 G 状态；在攻击的渗透阶段系统进入 V 状态，此时 FCM 可能触发取证机制，触发取证 agent 进行证据收集与传输。

当系统进入 A 状态时，FCM 将启动动态取证分析机制。此时，系统使用恢复策略进行系统修复，如果有足够的冗余，系统能够通过屏蔽攻击影响将系统带回 G 状态，取消取证触发，否则，系统会尝试限制危险的扩展，同时维持原系统功能，继续进行动态取证分析。

如果所有策略失败，系统进入 F 状态，并发出告警信号，提醒进入事后取证分析。图 2 中虚线表示在攻击发生后，通过手工干涉恢复所有的服务，实线为系统自动恢复。

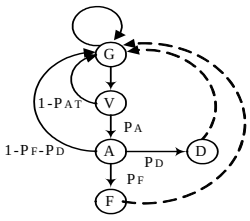

图 2 取证状态的转移

3.2.2 取证状态转移过程

FCM 通过 ARM 评估、检测系统的不同运行状态，根据系统状态的转换，控制系统取证机制，实现取证状态转换。

取证状态转移图可以根据半马尔可夫过程(semi-Markov process, SMP)建立量化的随机模型：用状态{G, V, A, D, F}模型化取证控制，设各状态的转移概率为P_i，t为攻击者所需花费的时间(精力)，则系统在V状态时，启动取证机制的概率为

$$FC_V(t) = 1-(\pi_G) \quad (1)$$

启动取证分析的概率为

$$FC_A(t) = 1-(\pi_G-\pi_V) \quad (2)$$

其中，π_i(i=G, V, A, D, F)表示SMP在状态i的平稳状态概率，转移概率P_i为经验值，它与入侵的类别有关。显然，在A状态时，$FC_V(t)=1$, $FC_A(t)=1$。

例如对于DoS攻击，根据ARM工作机制可得[4]：

$$\pi_G = \frac{h_G}{h_G + h_V + p_a[h_A + p_u h_{GD} + (1-p_u)h_{TR} + p_G(1-p_u)h_{UC} + (1-p_u)(1-p_g)h_F]}$$

$$\pi_V = h_V \frac{\pi_G}{h_G}$$

根据式(1)、式(2)可得，当发生 DoS 攻击时，系统启动取证机制与取证分析机制的概率。系统将根据设定的经验阈值，启动取证机制进行证据收集、传输与保存，然后启动取证分析功能进行证据的分析，并形成证据链。

3.3 证据安全传输机制

证据传输采取基于 PKI 的 CA 体系。当 FCM 评估系统进入 V 状态时，将触发取证机制，同时系统根据当前密码规范中定义的加密算法和 MAC 算法进行证据加密和完整性认证保护，通过取证网络传输到 ES。ES 收到后对所有证据进行处理，采用 MD5 进行数字签名并加盖时间戳，防止证据信息被删节、篡改和伪造，并能向第三方证明证据信息的完整性，从而完成原始证据到 ES 的移交过程。

证据的法律效力要求上述证据信息的传输也是安全的，为此，系统使用 SSH 协议实现认证加密传输。SSH 协议是一个嵌入在 TCP 和应用层协议之间的安全协议，它在应用层协议通信前完成加密算法、通信密钥的协商以及服务器认证工作，从而预防窃听及篡改通信中的数据，有效地保护证据移交过程中的证据机密性、完整性以及不可否认性。

3.4 主要功能模块分析

ACM 模块、ARM 模块在文献[4]中已阐述，本文主要分析 IDS 模块、取证 agent 和攻击回溯 agent 的功能和机制，其中，agent 机制的实现基于现有的研究工作。

3.4.1 IDS 模块

IDS 运行于代理服务器，通过对网络数据包的捕捉和分析，检测网络的运行情况。当发现网络出现异常行为时，IDS 判断异常情况的威胁等级。INFS 采用基于规则的 Snort 系统，并按系统要求进行了配置和改造。根据系统要求，对入侵检测日志记录进行配置，要求每条日志记录包括应用层在内的完整数据，并打上时间标记；将规则库中的规则分为 G 和 V 这 2 个等级。探测扫描、连接企图，缓冲区溢出企图等规则定为 G 级。这表明系统已被入侵的响应规则定为 V 级。对于 G 级，系统不进行取证，但可由系统管理员通过监视与控制模块强制进行网络取证。对于 V 级，系统通过 FCM 决定是否启动动态取证、分析机制。

3.4.2 取证 agent

取证 agent 置于被保护系统中，实时采集各种可能的证据信息，获取入侵攻击的特征、类别、被入侵主机地址等信息。INFS 收集的电子证据来源于系统、网络和主机 3 个方面。系统证据包括 IDS、应用服务器(Si)、ACM、ARM 和 FCM 的状态日志，该类信息连续动态存储备份到 ES。网络证据来源于 Snort 捕获的网络数据流，在 V 状态下由 FCM 触发进行存储备份。主机数据信息包括用户连接、进程状态、文件系统、交换分区、内外存等信息，其中，连接信息是跟踪用户当前会话、用户登录与退出的信息。所有证据由各种取证 agent 通过 SSH 协议实时地发送到 ES 上保存起来，并用 MD5 进行数字签名。

3.4.3 攻击回溯 agent

攻击回溯agent主要实现攻击源的回溯及记录，攻击源回溯采用包采样标记技术，它可以满足执法机构的取证需 要[5]。包采样使用任意的值作为标记概率p对包进行边缘采样，当路由器标记一个包时，它将自己的地址写入开始域，并将0 写入距离域，否则，如果距离域已经是 0，表明该包已经被前面的路由器所标记，在这种情况下，路由器将自己的地址写入结束域。如果路由器没有标记该包时，它总是增加距离域，这样，当包达到受害者时，由于它所包含的边缘被采样，它的距离域代表hop的数目。任何攻击者写的包必然有一个大于或等于实际攻击路径的距离，据此可以重构攻击者的攻击路径，找到真正的攻击者。攻击回溯agent可以在攻击发生或攻击完成后进行，其具体实现利用了IPv4 头几乎不使用的标识域。

4 INFS 的取证分析原理

证据的分析和处理是取证系统设计的核心，现有的一些网络取证分析技术主要是对攻击特征的分析，或是对单一证据源的分析。INFS 是动态取证与事后取证相结合的过程，在系统失效状态需要事后取证。系统利用数据挖掘技术进行攻击特征分析、攻击趋势分析、攻击时间序列分析和协同分析，不同的取证分析策略选择取决于取证时系统的状态，而此时的系统状态也是确定证据法律效率的首要因素。

对于复杂的网络入侵，其攻击行为往往是分步、多变或综合的，对其入侵行为的认定需要从时间、空间、协议等多方面进行关联分析。事实上，对于复杂的案件，法律上更注重证据之间的关联性，成功起诉复杂入侵的关键也在于发现有因果关系的、相互确证的多个独立的证据，而且攻击证据之间的关联也有利于重建攻击过程。

INFS采用贝叶斯网络(BN)进行协同分析，与IDS研究热点之一的入侵事件关联技术[6]不同的是，协同分析是对不同证据的因果关联分析，以找出证据之间的因果关系，形成证据链，有力地支持法庭举证。INFS协同分析的证据源包括Snort、应用服务器(S*i*)、ACM、ARM和FCM的状态日志。算法基本步骤为：对不同证据源的日志记录聚类形成元事件；所有元事件经过预处理转换为统一的标准报警数据格式(intrusion detection message exchange format, IDMEF)，形成标准元事件；用BN对标准元事件进行因果分析；标记因果 事件。

5 结束语

INFS 将入侵检测、入侵容忍技术与取证技术相结合，构建了一个容忍入侵的取证系统，可以根据系统的不同状态进行取证，从而大大减少了证据的存储量，而且系统的不同状态反映了系统被侵害的程度，这对于法庭取证是很重要的。

目前，网络取证研究无论在理论还是在实现方面都还有许多工作要做，今后将在取证状态转移图与取证过程的证据链关联、网络取证的协同分析等方面作进一步深入的研究。

参考文献

1 Payer U. Realtime Intrusion-forensics, A First Prototype Implementation[C]//Proc. of TERENA Networking Conference. 2004.

2 Ren Wei, Jin Hai. A Framework of Distributed Agent-based Active and Realtime Network Forensics System[C]//Proc. of the 19th International Conference on Advanced Information Networking and Applications. 2004.

3 Wang F, Gong F, Sargor C, et al. SITAR: A Scalable Intrusion Tolerance Architecture for Distributed Server[C]//Proc. of the 2nd IEEE SMC Information Assurance Workshop. 2001.

4 Goševa-Popstojanova K, Wang F, Wang R. Characterizing Intrusion Tolerant Systems Using a State Transition Model[C]//Proceedings of the DARPA Information Survivability Conference and Exposition. 2001.

5 Savage S, Wetherall D, Karilin A, et al. Practical Network Support for IP Tracebak[C]//Proceedings of the 2000 ACM SIGCOMM Conference, Stockholm. 2000.

6 穆成坡, 黄厚宽, 田盛丰. 入侵检测系统报警信息聚合与关联技术研究综述[J]. 计算机研究与发展, 2006, 43(1): 1-8.

（上接第 154 页）

前文已定义每棵子组身份树的最大高度为 h，则每个成员最多需要在本地保存($h-1$)条相关节点私钥信息。子组成员协商密钥时，每个成员最多需要做($h-1$)次 pairing 运算。

一个子组从建立到最终协商出生成密钥 K_1^1，KGCs 最多需要进行 2^{h-1} 次单播。当某个成员需要与 t 个子组进行通信时，其需要将欲发送的消息分别用各子组的公钥进行加密后连接起来广播出去，消息总长度大约为 $2tn$。

5 结束语

设计动态高效的分布式组密钥管理协议是安全组播中需要重点考虑的问题。本文在文献[4]的基础上，提出了一个新的基于身份的安全组播密钥协商方案，实现了任意多个子组之间的直接保密通信，而无需KGCs的转发，降低了延迟，灵活性较高。子组成员以及子组之间，在协商密钥或通信时相互独立，充分体现了分布式的特点。使用一组并行工作的KGCs，也大大降低了单个KGC的工作负担，避免了单点故障的产生，提高了组播系统的健壮性。密钥托管(key escrow)是基于身份的密码系统所固有的缺点，本文方案同样存在这个问题，即KGCs可计算出所有子组的公、私钥。近年来提出的无证书密码系统[6]在传统的基于证书的公钥密码系统和基于身份的公钥密码系统之间进行了适当的折衷，取得了较好的效果。下一步的工作将考虑应用无证书的密码系统，以期构造一个更安全的密钥协商方案。

参考文献

1 Mittra S. The Iolus Framework for Scalable Secure Multicasting[C]//Proc. of ACM SIGCOM'97. 1997.

2 Wong C K, Gouda M, Lam S. Secure Group Communications Using Key Graphs[C]//Proc. of ACM SIGCOM'98. 1998.

3 Balenson D, McGrew D, Sherman A. Key Management for Large Dynamic Groups: One-way Function Trees and Amortized Initialization[Z]. (2000-08). draft-irtf-smug-groupkeymgmt-oft-00.txt.

4 Wang Liming, Wu Chuankun. Efficient Key Agreement for Large and Dynamic Multicast Groups[J]. International Journal of Network Security, 2006: 3(1).

5 Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[C]//Proc. of the 21st Annual International Cryptology Conference. 2001: 213-229.

6 Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography[C]//Proc. of Advances in Cryptology-Asiacrypt'03. 2003: 452.