分布式入侵检测系统修复机制

杨 挺，罗光春

(电子科技大学信息中心 成都 610054)

【摘要】提出了一种基于移动代理的新型分布式入侵检测系统的修复机制。该系统是针对WAN环境设计的，数据的处理通过各节点所设置的代理来进行分布式计算，能实现全网络范围内的入侵检测功能，具有良好的可移植性；对网络系统和主机的资源占用较低，减少出现网络瓶颈的可能。讨论了系统各个层次上的修复和抗毁功能，实验证明，该机制具有较好的性能。

关 键 词 多参数; 入侵检测; 决策; 准确性

中图分类号 TP309 文献标识码 A

A Distributed Intrusion Detection System Repairing Mechanism

YANG Ting，LUO Guang-chun

(Information Centre, UEST of China Chengdu 610054)

Abstract A mobile agent distributed intrusion detection system(MADIDS) repairing mechanism based on mobile agent is introduced in this paper. MADIDS is special designed for *WAN* environment. MADIDS Data is calculated by distributed agent at every node. Not only has it carried out a intrusion detection at network range and a well migrate character, but also there is possibility of lowering network bottleneck because of the low cost of network system and host computer resource. Restorability and Invulnerability at every layer of the system has discussed in this paper. Experiment proved that this mechanism is displaying a well performance.

Key words multi-parameter; intrusion detection; decision-making; accuracy

本文提出了一种基于移动Agent的分布式入侵检测系统(Mobile Agent Distributed Intrusion Detection System，MADIDS)的自我修复机制[1-3]。MADIDS采用了分层更新和生成机制降低在WAN中统一配置时的网络开销；并通过Agent自我复制的功能来增加系统的抗毁和自我修复能力，使MADIDS拥有很好的伸缩性、适应性和可用性，比传统入侵检测系统更适应在WAN环境下运行。

1 系统的完整性和有效性

对MADIDS进行的攻击，主要分为对各功能模块(事件产生器、分析器、决策器、数据库等)的攻击和直接对Agent进行攻击，本文重点分析对各模块的攻击，对Agent的防护可参见文献[4-5]。

(1) 检测范围：MADIDS的功能模块广泛分布于WAN上的各个域和各个主机(Host)处。MADIDS需要对各节点上的功能模块和相关数据库进行检测，在此基础上进行修复和抗毁工作。

(2) 完整性检测：为进行完整性检测，系统对各节点上的所有功能部件和数据库，按统一规则进行编码，将其称为完整性特征值(Integrality Eigenvalue，IE)。共6个数据项，如表1所示。如，第3个域中第6个主机上

收稿日期：2005 – 06 – 23

作者简介：杨 挺(1975 –)，男，本科，工程师，主要从事软件工程方面的研究.

的网络事件产生器(Network Event Generator，NEG)，如果是域内配置的第2个NEG，大小为15 323 bytes，其完整性特征值为“ 0306NEG0215323 ”。在此基础上，系统会按一定规则，将Agent移动到对应节点上。Agent会对相关部件或数据库进行检查，并通过对比IE的方式，来检测各部件(或数据库)的完整性。

表1　完整性特征值

编号	1	2	3	4	5	6
内容	域编号	主机编号	功能模块(或数据库)名称	域内同类部件(或数据库)编号	部件(或数据库)的大小值	保留并用于系统扩展

(3) 有效性检测：为验证各功能模块的有效性，可定义对应于各模块的标准测试过程，例如子功能模块，BEA_test对应于基本事件分析器(Basic Event Analyzer，BEA)测试，NEG_test对应于NEG(有部署在域内个别Host上的网络事件产生器)测试等。为保证系统开销较小，该测试过程的代码应包含于对应模块内，作为该模块功能的一部分存在。当系统运行到测试步骤时，测试子模块从本地完成代码加载。测试子模块含有数据和代码两个部分，将数据设定为标准的入侵特征(如某种入侵行为的特征字串)，而将代码设计为调用对应功能模块对此特征字串进行检测，并判断检测返回结果是否正常。当移动Agent进行有效性测试时，只需调用该部件所含的测试子模块，并根据其运行结果来判定对应功能模块是否失效。以BEA的测试过程为例，如图1所示。

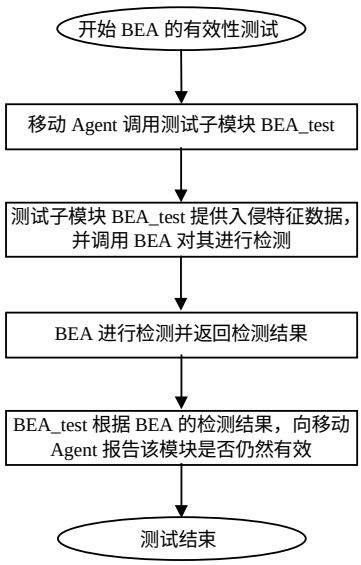

图1　功能部件有效性的检测过程

(4) Agent的种类：针对Host、域服务器(Domain Server，DS)和主服务器(Main Server，MS)这3个层次的自我修复和抗毁工作，系统设置了3种移动Agent，即主机保护代理(Host_Protect_Agent，HPA)、域保护代理(Domain_Protect_Agent，DPA)和主保护代理(Main Protect_Agent，MPA)，分别部署于Host、DS和MS上，它们分工明确、相互协作，共同构成MADIDS系统的整体修复和抗毁子系统。

2　Host层次上的自我修复和抗毁

(1) 每个主机随机生成 HPA，预设一个相对固定的时间幅度 T_l～T_k，只要生成移动 Agent 的间隔介于其间即可。随机生成代理，可以防止入侵者发现各节点的规律，提高代理自身和整个系统的安全性。(2) $Host_1$ 的 HPA 生成后，先判断所在域内其他 Host 运行状态(如 Ping 方法)，然后根据在线 Host 的数量进行自我复制；(3) 复制后的 HPA 移动到域内，除本地主机外的其他所有 Host 上，按照系统预设的规则进行检测；(4) 所要检测的内容包括基于主机的事件产生器(Host Event Generator，HEG)、BEA、事件数据库和个别 NEG，检测的内容主要是这些部件的完整性、有效性；(5) 如果 HPA_1 所在的 $Host_2$ 正常，HPA_1 将返回 $Host_1$ 和 DS，与 HPA 和 DPA 交换信息，并结束运行。在系统正常时，所有 HPA 均按以上方式运行；(6) 如 HPA_1 所在的 $Host_2$ 某个部件出现问题，如 HEG_1 出现失效，HPA_1 将记录相关情况，并移动到 DS 上与 DPA_1 交换信息，待确认信息交换成功后，HPA_1 将返回 $Host_1$ 和 DS，并结束执行；DS 还需要完成对 NEG 的完整性检测，对 NEG 的有效性检测可在 Host 上进行，但由于 NEG 并未部署在所有 Host 上，对其完整性的检测就只能等待所有 HPA 返回到 DS，并与 DPA 交换信息后才能进行。如果 DPA 确认域内 NEG 完整且有效，该检测工作结束，如果存在完整性或有效性问题，DPA 将移动到对应 Host 上，在完成恢复工作后返回；(7) DPA_1 收到相应信息后，将移动到 $Host_2$ 上，并负责完成从 DS 上向 $Host_2$ 重装 HEG_1 的任务，在确认重装成功后，DPA_1 将返回 DS，并结束执行。

由以上设计可见，系统在Host层次上的完整性和有效性，主要依靠Host自身生成HPA并结合DS来加以保证。若干HPA随机生成，并在域内通过复制、移动、检测、通信、判断、重装等动作，来完成系统修复工

作。由于移动Agent在LAN上移动时通信量非常小，而Host层次的系统修复也仅在准确判断后，才在域内DS和Host之间进行一次传输，因而保证了通信开销较小；系统每个在线主机在给定的时间幅度T_l～T_h内，生成用于检测的移动Agent，保证了域内各Host上的所有部件都能得到监控，不会出现遗漏；MADIDS利用HPA和DPA相配合，在短时间内生成移动Agent来检测和处理系统部件所出现的问题，在通信质量较好的LAN内，使Host层次上的所有IDS部件都能得到较好保护，确保了系统修复的及时性。其工作机制如图2所示。

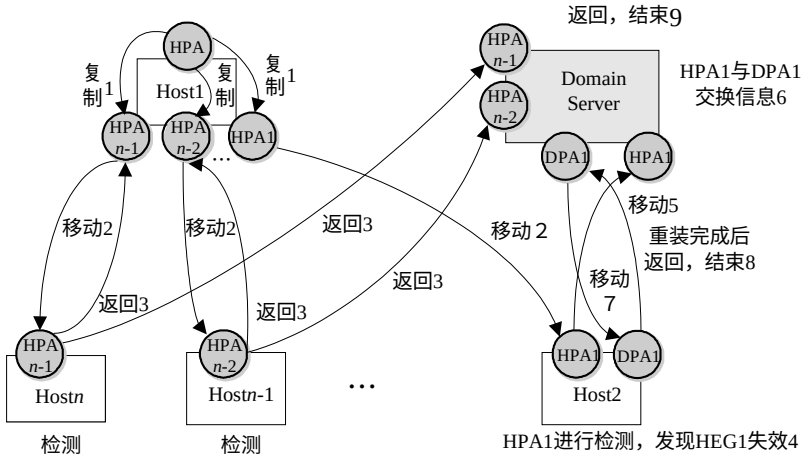

图2 Host层次上的自我修复

一个IDS部件出现问题的持续时间T可按极端情况估计如下：

在最好的情况下，一个Host上的一个部件发生了问题，此时另一Host所生成的HPA正好到达，并正好检测到该故障(T_1)，此时HPA将移动到DS上(T_2)，并将与DPA进行信息交换(T_3)，DPA将移动到Host上确保该部件的顺利传输，并实现正常恢复重装(T_4)，可见在最好情况下的系统恢复时间为：

$$T_{\text{best}}= T_1+T_2+T_3+T_4 \tag{1}$$

在最差情况下，一个Host上的所有部件都发生了问题，此时其他所有Host所生成的HPA都正好离开，在经过T_h后重新生成并到达该Host(T_0)，然后才检测到该系统的各部件存在故障(T_1')，此时HPA将移动到DS上(T_2')，并将与DPA进行信息交换(T_3')，DPA将移动到Host上确保该部件的顺利传输，并实现正常恢复重装(T_4')，所以在最差情况下的系统恢复时间为：

$$T_{\text{worst}}=T_0+T_1'+T_2'+T_3'+T_4' \tag{2}$$

比较T_{best}和T_{worst}可见，两者的差异首先是后者多出了T_0，其次$T_2=T_1'$，而T_1'、T_3'、T_4'均大于T_1、T_3、T_4，这主要是由于发生故障部件较多所致。由于所有计算均发生在本地机器，通信传输发生在LAN内，故只要没有特别的网络或主机故障，T_{best}和T_{worst}的绝对值和它们之间的差值都非常小。由以上分析可见，应用HPA与DPA相结合的方法，完全可以保证系统修复的及时性。

3 Domain Server层次上的自我修复和抗毁

由于不同域之间以及一个域与主服务器MS之间通常为WAN，理想情况下，最好是设计成检测与修复都在域内进行，而不像在Host层次上那样设计成各域之间互相检测，并利用MS来修复。域间修复机制和域内直接修复相比较，将会因WAN通信质量较差而增加系统开销，可能导致系统更新的及时性下降。在MADIDS系统的体系结构下，对DS层次的检测和修复工作不能在域内完成，只能在域间进行。由于引入了移动Agent，相对于传统方式而言，仍在效率上有较大改进。

4 Main Server层次上的自我修复和抗毁

MS作为MADIDS中央控制层次，居于整个系统的核心。为保证其部件功能的安全性，从实际需要出发采用了2个简便易行的方法，它们分别用于预防和恢复。

(1) 最小服务法则(The Least is The Best)：一般而言，在任何情况下1台服务器所提供的服务越多，就越有被攻击的可能，因此在MADIDS中MS被设计为仅提供系统所必须的功能，对其他任何请求均拒绝提供服务。同时可设置各类严格保护措施和机制，以此降低系统被攻击的可能性；

(2) 实际应用场合下可采用双机备份的方式配置两台MS，利用热备份技术保持同步。

5 实验结果

为验证MADIDS的性能，针对其规则更新和自我修复功能进行了实验。由于条件限制，实验环境仅在某校园网内选取3处位置进行。主服务器MS放置于子网202.115.14.1/24内；第1个域的各个节点包括DS1、Host1、Host 2、Host 3放置于子网202.112.10.1/24内；第2个域的各个节点包括DS2、Host4、Host 5、Host 6放置于子网202.115.1.1/24内。

针对系统自我修复功能进行了3组各500次实验，分别为域内1个Host失效、2个Host失效、域服务器DS失效3种情况。设定每个主机随机生成HPA或DPA的产生时间幅度T_l～T_k为15～20 ms。实验中删除Host和DS上的事件数据库(Event Data-base at Host，EDH)、域服务器上的事件数据库(Event Data-base at Domain Server，EDDS)，造成系统的不完整性。实验在3种情况下进行：(1) 1个Host失效的情况：当1个Host失效时，从删除该Host上的数据库开始计时到系统重装完成，耗时在0.8～1.3 s之间；(2) 2个Host失效的情况：利用程序的方式，同时删除两个Host上的数据库并开始计时，直到最后1个Host被系统修复，耗时在0.9～1.6 s之间；(3) DS失效的情况：从删除DS上数据库开始计时，直到系统完成重装，耗时在1.7～4.5 s之间。实验中用于测试的EDH、EDDS、部署在MS上的事件数据库(Event Data-base at Main Server，EDMS)大小均为20 KB。

情况(1)中1个Host修复所需时间周期较短，是由于所有工作均在LAN内进行，情况(2)中2个Host同时需要修复，但由于采用了并行检测和修复的机制，所以耗时并未增加太多，而情况(3)中DS的修复工作需要在WAN上进行数据传输，所以耗时较前两种长。

6 结　论

MADIDS在系统管理中使用了分层次的自我修复机制，这种机制降低了维护系统完整性和一致性的负荷，网络通信较小，非常适合在WAN中使用。经实验验证，MADIDS克服了传统入侵检测系统在体系结构上，难于大规模统一配置和维护的不足，是一种适合在WAN环境运行的新型入侵检测系统。

参　考　文　献

[1] Baumann J, Hohl F, Rothermel K M, et al. Concepts of a mobile agent system[EB/OL]. Http://ateseer . ist. psu. edu/baumam97 mole. html, 1998-05-09

[2] Karnik N M, Tripathi A R. Design issues in mobile-agent programming systems[J]. IEEE Concurrency, 1998, 6(3): 52-61

[3] Luo Guangchun, Lu Xianliang, Li Jiong, et al. MADIDS: A novel distributed IDS based on mobile agent[J]. ACM OSR, 2003, 37(1):46-53

[4] Freier A, Karlton P, Kocher P. The SSL protocol version [S]. 1995

[5] Li Gong, Mueller M, Prafullchandra H, et al. Going beyond the sandbox: An overview of the new security architecture in the Java Development Kit 1.2[C]. In USENIX Symposium on Internet Technologies and Systems, Monterey, California, 1997

编　辑　漆　蓉