一种网络入侵检测系统安全通信协议及其验证

李晓燕 苗长云

(天津工业大学信息与通信工程学院 天津 300160)

摘 要 针对网络入侵检测系统中安全通信存在的一些问题,制定了一种适用于网络入侵检测系统的网络安全通信协议,并对其安全性进行了形式化分析和验证,使得安全性和通信效率并重。

关键词 网络入侵,检测,安全通信协议,形式化验证

中图法分类号 TP309.2 **文献标识码** A

A Kind of Network Security Protocols and Verification

LI Xiao-yan MIAO Chang-yun

(College of Information and Communication Engineering, Tianjin Polytechnic University, Tianjin 300160, China)

Abstract Considering some problems of secure communications between the various modules in distributed intrusion detection system, a kind of network security protocols of applicable to distributed intrusion detection system were poposed. The protocols are proved to be safe in theory and to be a reliable in product testing.

Keywords Network intrusion, Secure communication protocol, Protocol design, Formal verification

1 引言

根据不同的结构和监听策略,入侵检测系统通常分为两类:基于主机的入侵检测系统(HIDS)和基于网络的入侵检测系统(NIDS)。网络入侵检测系统(Network Intrusion Detection System, NIDS)是分层计算机网络安全中普遍采用的防护手段。作为一种防护手段,毫无疑问它本身的安全性是NIDS好坏的重要指标。入侵检测技术是根据利用审计跟踪数据监视活动的思想建立起来的一种积极主动的安全防护技术,可以被定义为对计算机和网络资源的恶意使用行为进行识别和相应处理的系统。它提供对内部攻击、外部攻击和误操作的实时保护,检测计算机网络中违反安全策略的行为,能在网络系统受到危害之前进行拦截和响应。它主要完成以下功能:监视、分析用户及系统活动;系统构造和弱点的审计;识别反映已知进攻的活动模式并向相关人士报警;异常行为模式的统计分析;评估重要系统和数据文件的完整性;操作系统的审计跟踪管理,并识别用户违反安全策略的行为[1]。

目前存在的网络入侵检测系统通信协议大多采用SSL、BEEP和LDAP等协议或者各种数据加密算法,或者采用多种结合的方法来解决入侵检测系统的通信安全性问题。这些方法虽然看似完善,但是也存在着这样那样的问题:采用的协议的安全性和通信效率,往往会偏向两者的任何一方,这都是不妥的;各种数据加密算法解决通信安全的方案,由于缺少了必要的握手协议,使得通信部件很容易受到攻击。

为了提高入侵检测系统自身的安全性,本文针对网络入侵检测系统中安全通信存在的一些问题,提出了一种适用于网络入侵检测系统的网络安全通信协议,该协议不使用第三方网络安全协议,不仅使得通信协议的效率得到了提高,而且消除了第三方安全协议带来的安全隐患,使得安全性和通信效率得以平衡。并在理论上对其安全性进行了形式化验证。

2 安全通信协议

该协议分为两个子协议,即握手子协议和密文传输子协议。握手子协议采用公钥密码体制,用于通信双方会话密钥的协商,以及通信双方的身份认证;密文传输子协议则采用对称密码机制,使用握手协议中协商的会话密钥实现数据的加密传输。

2.1 握手子协议的设计

握手子协议采用通过挑战/应答机制以保证通信的新鲜性,并进行身份认证,该子协议如图1所示。

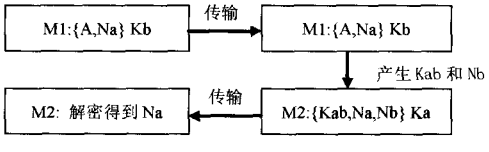

图1 认证子协议

其中M1和M2表式通信双方A和B发送的信息,A和B双方都持有对方的公钥Kb和Ka。A是握手的发起者,它首先产生一个随机数Na,并且得到B的公钥Kb,利用Kb将自己的标识A和产生的随机数Na一起加密成信息M1,将M1发送给B;B接收到消息M1后,首先利用自己私钥对其进行解密,同样产生一个随机数Nb,此外还产生一个会话密钥Kab,并将这Nb和Kab进行存储,最后利用A的公钥Ka将Kab、Na和Nb一起加密为M2,并发送给A;A收到消息M2后,首先利用自己的私钥进行解密,解密后判断消息M2中的Na是否和自己产生的随机Na数相等。如果相等则完成握手,继续下一步的密文传输;如果不相等,则A将丢弃

李晓燕 女,硕士;苗长云 男,教授。

M2，此次握手失败。

在这样设计的情况下，在入侵者不知道 B 的私钥或者 A 的公钥的情况下，握手不会成功，保证了下一步密文传输的安全。

2.2 密文传输子协议的设计

密文传输子协议用于 NIDS 的加密数据数据传输，并在传输过程中保证数据的机密性和完整性。密文传输协议具体设计如下所示：

M3：$A->B$：$\{A,Nb\}Kb,\{M'\}Kab,M''$

在本密文传输协议中，M' 表示传输的 NIDS 数据，M'' 表示用于加密 NIDS 数据的数字签名。在握手协议中 A 成功地验证完消息 M2 后，首先要对将要进行传输的 NIDS 数据 M' 利用会话密钥 Kab 进行加密，然后利用自己的私钥对加密后的数据进行数字签名生成 M''；最后利用 B 的公钥将自己的标识 A 和 B 产生的随机数 Nb 一起加密，并连同加密后的 M' 和 M'' 信息一起传输给 B。B 收到 A 的消息 M3 后，首先验证 Nb 是否正确，然后验证 NIDS 数据的完整性和 NIDS 数据的机密性。

在对 NIDS 数据进行加密和数字签名时，采用的是 XML 加密和 XML 签名技术。XML 加密技术与传统的加密技术最大的区别就是，传统加密技术是对整个数据进行加密，而 XML 加密技术不仅继承了传统机密技术的优点，更可以对单个元素进行加密，这样就灵活性方面要远远高于传统加密技术。因此利用 XML 加密技术的灵活性的特点，仅仅对 NIDS 数据中的较敏感数据进行部分加密，而对其它非敏感数据采用 XML 签名技术，使得数据的机密性既得到了保证，又可以最大限度地减轻系统加密解密的开销[2]。

3 协议的验证

协议的安全性的验证有两种方法：一种是采用模拟攻击的检测方法，通过对各个子协议进行攻击来检验其安全性；另外一种是采用形式化分析方法，运用形式化语言对协议进行安全性分析。其中形式化方法已经被证明是一种强有力的系统分析和验证技术，已经得到了广泛的应用。

本文采用的是 SPIN 系统验证工具对安全协议进行协议的安全性验证。利用建模语言 Promela，对安全协议进行形式化建模后，SPIN 作为模型检测器具体对协议的具体验证步骤是[3]：

(1) 写出需要验证的系统属性要求，用 LTL(Lin2ear Temporal Logic)方程描述；

(2) 利用 SPIN 对系统属性进行验证；

(3) 若属性为假，SPIN 会生成一个 trail 文件，利用该文件进行引导仿真，跟踪协议运行过程，找出攻击序列；

(4) 否则系统属性为真，验证结束。

可以看出，形式化建模是协议分析的非常关键的一步。对协议描述中的 A、B 以及入侵者进行形式化建模，模型如图 2 所示。

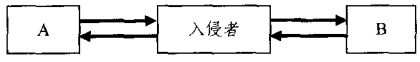

图 2 安全协议的 SPN 模型

安全协议的目的是在加密状态下确保协议主体的相互鉴别，换而言之，如果 A 和 B 成功地运行了一次协议，那么 A 的响应对象是 B，而且 B 的请求对象是 A。会话密钥不会被第三方窃取，也就是说如果 A 成功地与 B 完成了一次协议的运行，则入侵者不可能知道会话密钥 Kab。

结束语 通过对各种网络入侵检测系统通信安全问题的研究，提出了一种新的网络入侵检测系统的安全通信协议，并在理论上进行了验证。如何使得安全性和通信效率并重，是网络入侵检测系统通信协议设计的关键。该协议不使用第三方网络安全协议，不仅使得通信协议的效率得到了提高，又消除了第三方安全协议带来的安全隐患，使得安全性和通信效率得以平衡。

参 考 文 献

[1] 魏兵役. 网络入侵检测系统的分析与研究[J]. 信息与电脑，2010，4

[2] 吴启明. XML 安全加密技术框架[J]. 电脑知识与技术，2007，24

[3] 陈性元，杨艳，任志宇. 网络安全通信协议[M]. 北京：北京高等教育出版社，2009

(上接第 77 页)

表 1 各节点互联信息表

探测的 DSP	父亲孩子节点	孩子节点与其它孩子子孙节点重复
D1	0	0
D2	D1	D5
D4	D2	0
D8	D4	0
D5	D8	0
D3	D1	D7
D6	D3	0
D7	D6	0

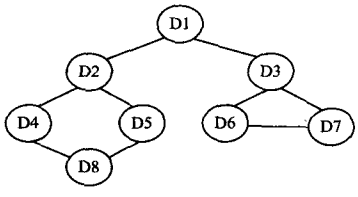

图 3 探测得到的并行 DSP 网络结构

根据上面针对图 2 的改造步骤及表 1 的详细信息，最后得到的改造图如图 3 所示，即是要探测的并行 DSP 网络结构。

结束语 本文针对并行 DSP 系统，设计一种蠕虫算法探测其结构，并分析算法的正确性。本文在蠕虫算法中所提到的基于深度优先历递归法寻找节点和构造结构的具体步骤都是可以实际运用的。随着电子技术的迅猛发展，并行 DSP 技术将大规模地应用到数字信号处理的各个领域。

参 考 文 献

[1] 王哲，王希敏. 并行 DSP 系统消息传递路由算法[J]. 计算机工程，2009(17)：241-243，246

[2] 徐精华，邹雄，王旭成. 基于蠕虫算法的 DSP 网络结构探测[J]. 计算机与现代化，2010(1)：16-18，22

[3] 任骊平，陈王骞. 多 DSP 系统互连方案分析[J]. 电子技术应用，2002(04)：50-52

[4] 林晓静. 基于 TMS320C6416 的并行 DSP 板的设计与实现[D]. 南京：南京理工大学，2007

[5] 严蔚敏. 数据结构(C 语言版)[M]. 北京：清华大学出版社，1997