高技术通讯 2009 年 第 19 卷 第 7 期:706 ~ 712

doi:10.3772/j.issn.1002-0470.2009.07.008

一种自适应容忍入侵的密码协议安全运行防护系统①

郝耀辉②* 郭渊博*** 卢 昱**

(*解放军信息工程大学电子技术学院 郑州 450004)

(**军械工程学院 石家庄 050003)

摘 要 针对密码协议在实际运行中遭受攻击的问题,设计了自适应容忍入侵的密码协议安全运行防护系统。该防护系统主要由入侵检测模块和容忍入侵模块组成。入侵检测模块采用基于特征和异常的混合入侵检测模式,使用有限状态自动机(FSM)匹配密码协议执行中的各状态参数,实时检测密码协议的运行情况,并把检测结果发送给容忍入侵模块,触发容忍入侵模块根据预先设计好的自适应调整策略,对密码协议的运行进行调节,以达到容忍攻击的目的。采用模拟试验对系统模型进行了仿真测试,测试结果表明该模型能够在一定程度上成功检测对密码协议的攻击行为,并具有容忍某些特定类型攻击的能力。

关键词 密码协议,自适应,容忍入侵,入侵检测,有限状态自动机(FSM)

0 引 言

密码协议又称安全协议,其主要目的是保证信息的安全,但如果密码协议本身存在漏洞,攻击者会利用这些漏洞,伪装成合法通信者窃听秘密或者更改信息,对信息系统与通信系统所涉及的业务领域造成巨大危害。虽然目前在密码协议设计、分析领域出现了许多用来保证密码协议的安全性的新方法,但这些方法或多或少都存在一些缺点,不能完全保证设计的密码协议绝对安全。此外,虽已发现一些著名的密码协议存在安全缺陷,但这些协议却仍被广泛应用,这给网络信息安全带来了很大隐患。

美国佛罗里达州立大学 Yasinsac 尝试将网络的入侵检测方法应用到密码协议的执行过程中[1],设定了对密码协议执行过程中攻击检测的条件、环境等[2],并在此基础上,设计了针对密码协议运行过程的入侵检测方法,能实时检测密码协议运行过程中是否有入侵/攻击发生,但此方法采用的是基于特征的误用检测方法,不可避免地存在检测攻击漏报率高的问题。而且,现有的方法也未对检测到攻击后系统如何应对提出具体的解决办法。此外,Tak[3]对密码协议的自适应性进行了研究,分析了影响密码协议安全的各项参数。在以上这些研究的基础上,本文将入侵检测的技术与容忍入侵的原理相结合,应用到密码协议的实际运行中,设计了一种自适应容忍入侵的密码协议安全运行防护系统,以保证在密码协议执行过程中,准确高效地自动检测协议是否遭受攻击,并在检测到攻击后,通过自动实施一些密码协议的自适应调整策略,达到阻止或容忍入侵的目的。

1 系统结构

1.1 设计准备

整个网络中的密码协议用户分为受保护区域中的用户和不受保护区域中的用户两种,并把受保护区域中的密码协议用户分为诚实合法用户和入侵者两种,本系统只负责受保护区域中合法用户使用密码协议时的安全,其余用户的安全则不在考虑的范围内。

密码协议执行中几乎所有的信息数据都是加密的,针对密码协议执行的特殊情况,对密码协议的执行过程中,设定每步分成两个事件:一次发送事件和一次接收事件。如某一协议中有 A 向 B 发送{K}的一步,这一步将被看作两个事件,即对 A 来说,表示 A 传送一个消息给 B,用 A→B 表示;相应对 B 来说,表示 B 从 A 接收到了一个消息,用 B←A 表

① 国家自然科学基金(60503012)和 863 计划(2007AA01Z405)资助项目。

② 女,1978 年生,硕士,讲师;研究方向:网络安全;联系人,E-mail: hao_yaohui@126.com

(收稿日期:2008-04-01)

示[1,2,4,5]。

以对称密钥认证协议(Needham and Schroeder conventional (symmetric) key protocol, NSCKP)为例进行说明,该协议的执行过程由以下5步组成:

(1) A→S: A, B, Na

(2) S→A: {Na, B, Kab, {Kab, A} Kbs} Kas

(3) A→B: {Kab, A} Kb

(4) B→A: {Nb} Kab

(5) A→B: {Nb - 1} Kab

在本系统中的事件将被分成下面十个:

(1) A→S (2) S←A (3) S→A

(4) A←S (5) A→B (6) B←A

(7) B→A (8) A←B (9) A→B

(10) B←A

这些密码协议执行时的事件序列将作为系统中判定攻击行为的重要依据。

1.2 系统基本组成

系统主要有协议事件采集器、入侵检测模块、容忍入侵模块组成,系统总体结构如图1所示。

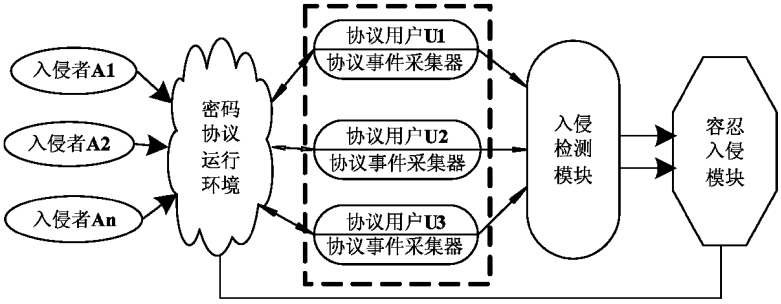

图1 系统总体结构图

(1) 事件采集器

主要负责采集合法的密码协议主体执行密码协议时的事件信息,并把这些事件信息发送到入侵检测模块。

(2) 入侵检测模块

入侵检测模块的功能是对当前网络中是否存在对密码协议的攻击行为做出判断。为了降低误/漏报率,采用特征入侵检测与异常入侵检测相结合的方法。特征入侵检测方法负责检测当前系统中是否存在已知的攻击行为,异常入侵检测方法则对系统中是否存在未知的新型攻击行为做出判断。

(3) 容忍入侵模块

容忍入侵模块的主要工作是依据入侵检测模块报告的检测结果,在攻击发生的情况下,通过动态地改变密码协议的具体配置参数、调整使用的密码协议种类和增加密码协议使用的人为多样性及不可预测性,增大攻击者攻击的难度或迫使攻击者主动放弃攻击行为。

1.3 系统工作机制

系统的工作方式有训练方式和防护方式两种。系统工作在训练方式阶段,主要是收集、统计用于判定当前是否存在对密码协议攻击的各项参数的值;工作在防护方式阶段,则依据训练阶段得到的各参数的值,对比当前密码协议实际运行时各项参数的值,判定当前运行的密码协议是否存在安全隐患,以采取各种有效的策略,对密码协议的运行进行保护。

初始时,在受保护网络区域中的每个合法用户都配置有一个协议事件采集器。实际运行时,事件采集器把收集到的合法用户使用密码协议时的执行信息,传送给入侵检测模块;入侵检测模块依据事件采集器发来的密码协议执行时的事件信息,对密码协议运行过程进行实时检测,判断此时网络区域中是否存在对密码协议的攻击行为,并把检测结果传送给容忍入侵模块;容忍入侵模块由入侵检测模块报告的检测结果触发,决策使用何种安全策略,并把决策结果反馈给网络中密码协议的合法使用者,在密码协议已经受到攻击时,动态调节当前系统中密码协议的运行,达到阻止/容忍入侵的目的。

2 系统中各关键点的考虑

2.1 事件信息构成

在一个网络中,可能同时运行多个密码协议,而一个用户也可能同时参与多个密码协议的运行,为区分这些事件是属于哪个用户参与的哪个密码协议,设定事件采集器传来的事件信息中包含如下内容:密码协议名、密码协议参与者、会话号、事件类型,如图2所示。

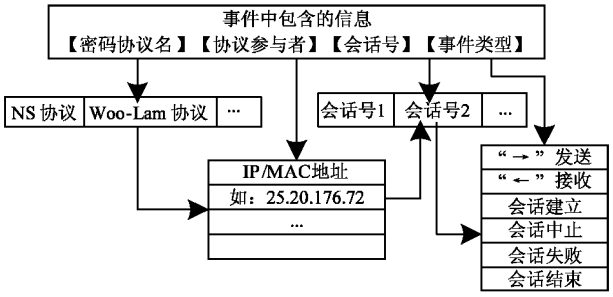

图 2 事件中包含的内容

图 2 中，协议参与者是事件中用于标识协议主体的部分，可采用 IP 或媒体接入控制（MAC）地址信息来表示。根据事件中包含的密码协议名和此协议参与者的名称，可唯一确定此事件是属于哪个用户参与的哪个密码协议。

2.2 入侵检测模块

入侵检测模块主要由存放事件信息的队列、密码协议正常运行的行为概况、密码协议正确运行规则库、密码协议已知攻击特征库、入侵行为判定器组成。其内部结构如图 3 所示。

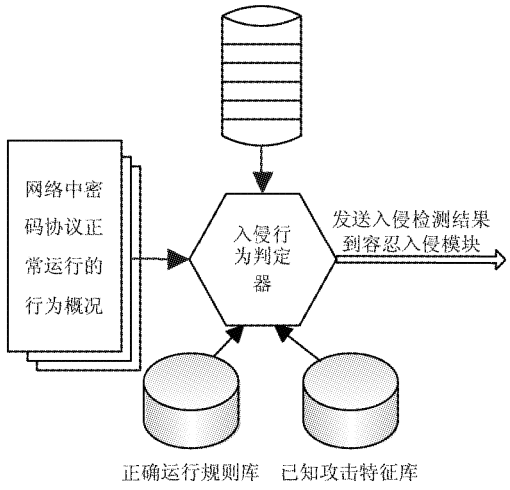

图 3 入侵检测模块内部结构图

下面对各主要部件进行说明。

2.2.1 队列数据结构

判定攻击所需的事件信息都是由事件采集器传送给入侵检测模块的，但在同一时间内可能有许多事件采集器都传送事件信息到入侵检测模块，如果入侵检测模块处理不及时，就会造成事件信息丢失，为保存这些事件信息，设计一个队列数据结构来存放事件采集器传送来的这些事件信息。

2.2.2 规则库和特征库组织形式

密码协议的正确运行规则库和密码协议已知攻击特征库均由一个个相同规格的文本文件组成，每个文本文件中都存放着一种密码协议的正确运行规则或已知其存在攻击形式的运行规则，这些规则格式为[4]：

begin ×× NUM type

state1 principal (/) principal state2 msgNum

state1 principal (/) principal state2 msgNum

--

end。

其中：

begin/end：表示协议正常运行或某种攻击特征在这一行开始/结束；

NUM：一个数字值，表示密码协议的正确运行规则和存在已知攻击时的执行规则，暗示这个特征后紧跟着的是一个正确的协议运行还是一个攻击，NUM≥0 表示特征是一个攻击特征，NUM = －1 表示这个特征是协议的正常运行。

Type：当 NUM≥0 时有效，表示当前规则对应的攻击类型，其值可以是：

R——消息重放攻击；

P——并行会话攻击；

M——中间人攻击；

O——反射攻击

L——交错攻击

C——针对密码算法的攻击

state1：表示有限状态自动机（finite state machine，FSM）在事件发送或接收开始前的状态，如：SS 表示开始状态，S1 表示状态 1；

state2：表示有限状态自动机在事件发生后的状态，S2 表示状态 2；FS 表示结束状态；

/：表示是发送/接收事件，用→/←表示；

principal：表示协议参与者名称，用单一字母标识符表示，如：A，B，S。

msgNum：表示协议正确运行时的消息序列号。

2.2.3 密码协议运行行为概况

密码协议运行的行为概况主要存储密码协议运行时各种参数的值，这些参数是判定当前系统中是否存在对密码协议攻击的依据。参数项主要包括以下几方面的内容：

- 各密码协议执行完所需的平均时间，作为判断超时警报的依据；
- 网络中密码协议会话的最大数目；
- 网络中违规协议会话（如中断/失败的会话）的最大数目。

密码协议的正常运行行为概况,在训练方式阶段统计创建。为降低入侵误报率,对协议行为限定了一个阈值,作为正常行为的最大偏离。各参数的值在限制范围内认为是正常的,超出最大偏离则认为可能有攻击发生。各参数项阈值的计算步骤为:

(1) 依据公式

$$V = \frac{1}{n}\sum_{i=1}^{n}(X_i - \bar{X})^2 \quad (1)$$

计算这些参数项的样本方差,其中 X_i 是上述各个参数项的样本值, $\bar{X}$ 是这些样本的平均值。

(2) 依据公式

$$S = \sqrt{V} \quad (2)$$

计算出各参数项的标准偏差。

(3)依据标准偏差,根据公式

$$UpperLimit = \bar{X} \pm S \quad (3)$$

设置各参数项的上下限。

2.2.4 入侵行为判定器的工作流程

入侵行为判定器根据密码协议的会话号和事件类型,监视密码协议的运行情况,检测是否有攻击行为发生,其主要的工作流程为:

(1) 入侵行为判定器依据事件采集器传来的密码协议执行时的事件信息,判定是否是一个新的密码协议会话开始,如是新会话开始,则创建一个新的有限状态自动机,否则找到此事件对应的有限状态自动机,向前运行有限状态自动机,即有限自动机发生一次状态转变;

(2) 监视当前运行的密码协议的状态转变规则和训练阶段建立的密码协议正确运行状态转变规则库中正确的规则相比对,如直到密码协议运行结束每步的状态转变规则都一致,则此协议正常结束,入侵检测模块发出正常运行报告;如密码协议执行中状态转变不一致,则先采用基于特征的入侵检测技术和密码协议已知攻击特征库中的内容相对比,如符合某一种攻击特征的状态转变规则,表示当前存在攻击行为,入侵检测模块发出入侵警报,并在警报中报告攻击的名称,如重放攻击、中间人攻击等[6];

(3) 对那些未知的攻击方式或可能不直接违反协议执行规则,只是引起网络通信或使用异常的攻击方式,则网络中密码协议的运行和协议正确运行规则库与已知攻击特征库都不符合,为了降低本检测方法的漏报率,再采用基于异常的入侵检测技术,先计算此密码协议从开始到结束所花费的时间,依据训练阶段得到的执行完此密码协议平均所需的时间,判断是否在阈值允许的范围内,如超出设定的阈值范围,则发出超时警报[7,8];

(4) 入侵行为判定器统计在密码协议执行期间,网络中正常结束和失败的密码协议会话数目等参数的值,并依据事件采集器传来的数据、有限状态自动机执行情况的数据等,为该密码协议创建密码协议实际运行行为概况和在训练阶段统计得到的目标协议长期正常行为概况中的内容相比较,来判断攻击,如各项参数的值,超出设定的阈值,入侵检测模块发出可疑行为警报;

(5) 在检测结束后,入侵行为判定器把这些检测结果,发送给容忍入侵模块,触发容忍入侵模块对密码协议的运行进行调节。

2.3 容忍入侵模块

容忍入侵模型主要由以下几个部分组成:密码协议和密码算法分类库、自适应容忍入侵策略调整器、自适应容忍入侵执行部件,其内部结构如图 4 所示[9]。

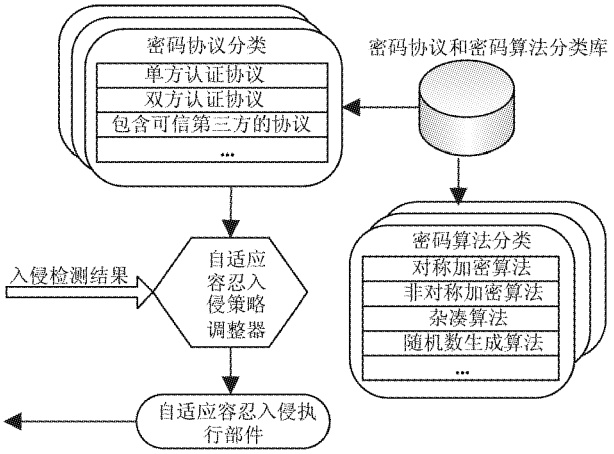

图 4 容忍入侵模块内部结构图

2.3.1 密码协议和密码算法分类库

密码协议和密码算法分类库[10]中存放着现有已知各种不同类型的密码协议及密码算法。并对每个密码协议和密码算法都标识有所属的类型。密码协议类型包括单/两方认证协议、含第三方的认证协议、两方密钥交换协议、含第三方的密钥交换协议等;密码算法类型包括对称加密算法、非对称加密算法、签名算法、杂凑算法、随机数生成算法等。

2.3.2 自适应容忍入侵策略调整器

密码协议自适应容忍入侵策略调整器主要用于在接收到来自密码协议入侵检测模块发送来的入侵报警时,通过对所使用的密码协议或密码算法进行策略自适应调整,以使当前攻击无效,使系统具有容

忍入侵的能力。该策略调整器可实现两种类型的密码协议入侵调整策略,即算法自适应调整策略和参数自适应调整策略。

其中算法自适应调整策略是:当接收到来自入侵检测模块报告遭受到针对密码协议自身或其中所使用的密码算法的消息重放攻击、中间人攻击、并行会话攻击、反射攻击、交错攻击、密码服务滥用攻击时,向密码协议和密码算法分类库请求与当前所使用的密码协议或密码算法同类的其它密码协议或密码算法,替换当前所使用的密码协议或密码算法,在保持当前系统安全功能的情况下,达到当前攻击模式对于未来实施成功攻击无效的目的。

参数自适应调整策略是:当接收到来自入侵检测模块报告遭受到执行时间超时或违反执行参数的可疑警报时,增加当前运行的密码协议或密码协议中使用的密码算法的密钥长度、密码算法的分块长度等参数,以使攻击者再次成功实施攻击所需要耗费的资源不断加大,直至最后放弃攻击;或者动态改变当前密码协议中所使用的密码算法的运行模式,使得当前攻击模式对于未来实施成功攻击无效,并增加所使用密码算法运行模式的人为多样性和不可预测性。

2.3.3 自适应容忍入侵执行部件

通过会话参与方之间的信息交换,密码协议的会话参与方之间才能够实现采用相同的调整策略进行自适应调整。自适应容忍入侵执行部件的主要功能是通知网络中密码协议的合法者具体使用何种策略。而接收到调整策略的密码协议使用者,根据接收的策略,具体设置新一轮密码协议的执行过程。

3 模型仿真与测试

对系统性能的模拟仿真测试,是针对 SSL 协议攻击的检测和容忍效果展开的。我们选用 VC ++ 6.0 对系统进行了模拟开发,其中事件采集器和有限状态自动机均用函数实现。系统的模拟仿真过程执行流程如图 5 所示。

程序中用到的关键数据结构有:

Event: 存储信息采集器报告的所有和事件相关的信息。包括:p1, type, p2, timeStamp,其中:p1 代表事件的第一个参与者,type 用于存储事件类型,如“发送”或“接收”,p2 代表事件的第二个参与者,timeStamp 存储事件发生时的时间。

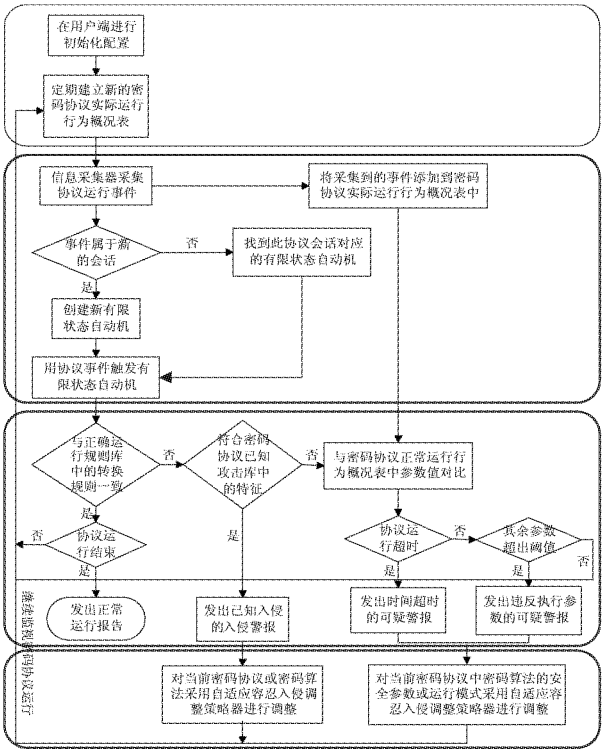

图 5 模拟仿真过程执行流程图

FSM: 表示有限状态自动机。包括:fsmNumber, currentState, protName, numEvts, machineType, attackType,其中:fsmNumber 表示有限状态自动机号,用于唯一确定有限状态自动机;currentState 表示 FSM 的当前状态;numEvts 表示 FSM 中的事件数目;machineType 表示此 FSM 是攻击/正常的;attackType 表示攻击类型。

EventIndex: 用于确定系统监视器接收的事件属于那个协议会话的线程。包括:protName, principals, sessionNum, sessionId,其中:protName 表示协议名称;principals 表示协议有关参与者;sessionNum 由信息采集器产生的协议会话的序列号;sessionId 由协议主体产生的序列号。

ThreadInfo: 保存每一个会话监视线程的轨迹,并保存对一个单一线程相关的信息。包括:protName, sessionNum, sessionId, principals, threaded, threadEventHandle,其中:protName 表示协议名,sessionNum 表示协议会话序列号,sessionId 是会话 ID,随机产生,principals 表示协议参与者,threadId 是线程的唯一标识符,threadEventHandle 是由线程发出的事件句柄。由协议名、会话序列号和协议主体,唯一确定一个协议会话。

PrincipalsSessions: 表示每组协议主体会话的数目,包括:principals, sessionNum,其中:principals 表示

协议有关参与者,sessionNum 由信息采集器产生的协议会话的序列。

具体实验在局域网环境中基于客户-服务器模式进行,采用三台 Pentium4 CPU 1.6GHz、内存 512MB、操作系统为 Windows2003 的 PC 机作为客户机,如图 6 所示。

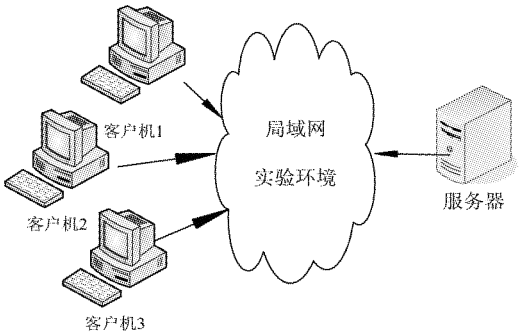

图 6 实验布局图

实验前提为:客户机 1、2 上模拟合法客户,分别以间隔 200ms 和 100ms 的速度不停地向服务器发出 SSL 协议请求,在客户机 3 上模拟攻击者,以间隔 200ms 的速度不停地向服务器发出请求。

具体实验分为以下三个步骤进行。

(1) 监控 SSL 协议在 1 周时间里不包含任何攻击活动的运行行为,经数据采集和处理,获得其正常运行时的各项行为参数,建立 SSL 协议正常运行时的行为概况表,表 1 给出了正常情况下各参数的具体值。

表 1 正常情况下的参数值

协议会话平均执行时间	155.57(ms)
平均失败的会话数目	212.3 次(s)
平均正常的会话数目	899.6 次(s)

(2) 对系统入侵检测能力的测试,参照文献[11],启动客户机 3,模拟在 CBC 填充模式下针对 SSL 协议进行边信道攻击的技术,并启动系统的密码协议入侵检测模块进行检测,经实验测试网络中失败的会话数目达到每分钟 414.72 次,所开发的入侵检测模块函数很快发出入侵警报。

(3) 对系统容忍入侵能力的测试,实验采用参数自适应调整策略来实现容忍入侵模块的内容,选用 Puzzle(Puzzle 由选择随机数进行 Hash 计算的方式得到)作为参数,要求客户机 1、客户机 3 在发出 SSL 协议请求前必须先解答来自服务器的一个 Puzzle,而客户机 2 则不需解答 Puzzle。实验选用 Puzzle 为 6 位二进制数值来进行,由于客户机求解 puzzle 必须要在该 Hash 函数的明文空间进行穷举搜索,则服务器产生 puzzle 与客户机求解 puzzle 所需的系统代价相比要小得多,实验测试结果如图 7 所示。

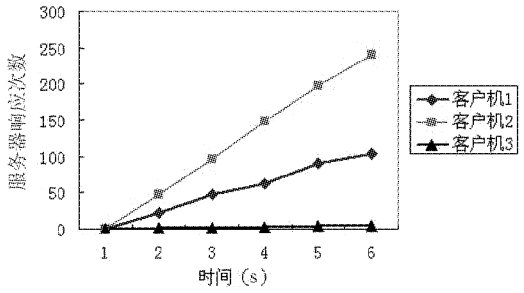

图 7 实验测试结果

攻击者在 25 秒的时间共获得了来自服务器约 5 个左右的响应,因此想要成功实施攻击共需 2048/5×25=10240 秒,即 170 分钟左右;参照文献[11]所述,攻击者在 25 秒的时间共获得了来自服务器的 63 个左右的响应,因此想要成功实施攻击共需 2048/63×25=812 秒,即 13 分钟左右;由此可见,攻击者想要成功实施攻击需要付出的代价变得很大,即该系统可在一定程度上容忍这种类型的攻击。

4 结 论

本文提出了一种可自适应容忍入侵的密码协议安全运行防护系统,通过对该系统的仿真实验测试,表明该系统可有效地检测出密码协议上的攻击,并可在一定程度上减少攻击的发生,为保护密码协议的安全性提供了一条新的研究思路和方法,但对系统性能的定性、定量分析,还需要进一步的实验证实。

参考文献

[1] Yasinsac A. Dynamic analysis of security protocols. In: Proceedings of New Security Paradigms 2000 Workshop, Ballycotton, Ireland, 2000.77-87

[2] Yasinsac A. An environment for security protocol intrusion detection. *Journal of Computer Security*, 2002, 10: 177-188

[3] Tak S W, Lee Y, Park E K. Design and evaluation of adaptive secure protocol for e-commerce. In: Proceedings of IEEE International Conference on Computer Communications and Networks, Scottsdale, USA, 2001. 32-39

[4] Sherwood R W. Methods of Detecting Intrusions in Security Protocols: [Ph. M dissertation]. Tallahassee: The Florida

State University College of Arts and Sciences, 2004.15-28

[5] Leckie T, Yasinsac A. Anomaly-based security protocol attack detection. http:// www. cs. fsu. edu/research/reports/TR-021203.pdf: Florida State University, 2002

[6] Yasinsac A, Melendez E A, Goregaoker S. Implementing an object oriented knowledge based network reference monitor and intrusion detection system. http://www.cs.fsu.edu/research/reports/TR030801.pdf: Florida State University, 2003

[7] Joglekar S P, Tate S R. Embedded monitors for cryptographic protocol intrusion detection and prevention. In: Proceedings of IEEE Conference on Information Technology: Coding and Computing, Las Vegas, USA, 2004. 81-88

[8] Leckie T, Yasinsac A. Metadata for anomaly-based security protocol attack deduction. *IEEE Transactions on Knowledge and Data Engineering*, 2004, 9(16): 1157-1168

[9] Kang K D, Son S H, Stankovic J A. Differentiated real-time data services for e-commerce applications. http://www.cs.virginia. edu/papers/diff-rtds-e-comm-ecr03. pdf: University of Virginia, 2003

[10] Son S H, Zimmerman R, Hansson J. An adaptable security manager for real-time transactions. In: Proceedings of the 12th Euromicro Conference on Real-Time Systems, Stockholm, Sweden, 2000. 63-70

[11] Vaudenay S. Security flaws induced by CBC padding-applications to SSL, IPSEC, WTLS…. In: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology, 2002. London: Springer Verlag, 2002. 534-546

An adaptive intrusion-tolerant approach to protecting operation security of cryptographic protocols

Hao Yaohui[*], Guo Yuanbo[* **], Lu Yu[**]

([*] Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou 450004)

([**] Ordnance Engineering College, Shijiazhuang 050003)

Abstract

To protect the operation security of cryptographic protocols, the paper proposes an adaptive intrusion-tolerant approach which is composed of an intrusion detection module and an intrusion tolerance module. By adopting the mixed intrusion detection mode, the intrusion detection model uses the finite state machine (FSM) to match the parameters in the running of cryptographic protocols, which could conduct real-time detection of the characteristics of the cryptographic protocol operation, and send the detection results to the intrusion tolerance module, making it adjust the running of the cryptographic protocol according to the pre-designed self-adaptive strategy. The simulation demonstrated that this approach could be used to detect to a certain extent the attacks on cryptographic protocols and improve the intrusion-tolerance ability dominantly.

Key words: cryptographic protocol, adaptive, intrusion-tolerant, intrusion detecting, finite state machine (FSM)