# 基于有限自动机的密码协议入侵检测方法*

郝耀辉, 郭渊博, 刘 伟, 李景锋
(解放军信息工程大学 电子技术学院, 郑州 450004)

**摘 要**: 提出了一种在密码协议运行中,基于有限自动机原理检测其上攻击的方法,详细介绍了该方法的工作原理,并通过实例验证了此方法的可行性,最后给出了该检测方法原型系统的测试结果。

**关键词**: 密码协议; 入侵检测; 有限自动机; 实时; 动态
**中图分类号**: TP309 **文献标志码**: A **文章编号**: 1001-3695(2008)01-0230-02

# Intrusion detection method of cryptographic protocol based on finite state machine

HAO Yao-hui, GUO Yuan-bo, LIU Wei, LI Jing-feng
*(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)*

**Abstract:** This paper proposed the analysis method of cryptographic protocols based on FSM, when protocol was running. Introduced principles of the method, verified the method by instance, and provided experimental results of prototype program.

**Key words:** cryptographic protocols; intrusion detection; FSM; real-time; dynamic

密码协议 (又称安全协议)是构建网络安全环境、保护信息系统安全的重要手段之一。然而密码协议本身也存在缺陷和漏洞,所以分析其固有缺陷和发现对它的入侵攻击行为,是保障网络安全通信的前提。入侵检测技术是通过从计算机网络或计算机系统中收集信息并对其进行分析,来发现网络或系统中是否有违反安全策略行为的技术。本文将入侵检测技术应用于密码协议分析中,用有限自动机模拟密码协议执行过程,设计了一种能实时动态监控密码协议运行的入侵检测方法,并对该方法进行了测试。

## 系统结构

该检测系统把网络中的成员分为密码协议的合法参与者和入侵者两种。对每种密码协议建立正确运行状态转变规则库和密码协议已知攻击特征库,分别存储密码协议正确运行时的规则和已发现其上攻击的特征。整个系统中设一个系统监视器。每个密码协议的合法参与者均配置一个监视器终端,负责收集密码协议参与者的活动信息,并将这些信息传给系统监视器。由系统监视器通过构造有限状态自动机,建立这些信息与数据库中存储信息的映射关系,动态分析密码协议各参与者的行为,判断合法网络范围内的安全情况。整个系统结构如图1所示。

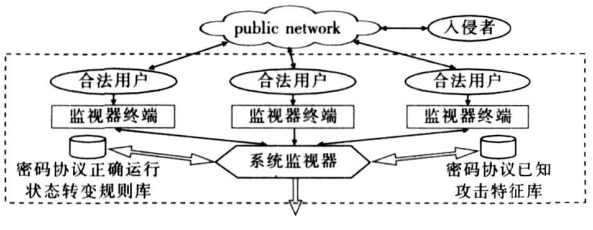


图 1 系统结构图

## . 检测原理

密码协议执行中要进行消息交换,将每次消息交换分成一次发送事件和一次接收事件。每次系统监视器接收一个事件,首先判断是否是一个新的协议会话的第一事件;然后在协议规则库中查找对应协议名存储的特征,构造一个有限状态自动机,并初始化有限自动机在开始状态。当系统监视器再接收到该协议会话的事件时,对应执行有限自动机到下一状态,判断该状态与协议正常运行要到达的状态是否一致。如果一致,系统监视器将有限自动机继续向前运行,如直到有限自动机终态都一致,表示协议运行正常,系统监视器不产生任何警告通告;如果这些事件中有一步与规则库中存储的信息不一致,开始判断是否与攻击特征库中存储的信息相匹配,若当转变到最终状态上时都与某一攻击特征相匹配,表示当前存在攻击行为,系统监视器将发出一个攻击通告;如果与规则库及攻击特征库都不符合,发出一个可疑攻击通告。

## . 数据库结构

在数据库中,密码协议正确运行规则和已知的攻击特征用下面的形式表示:

```
begin ××NUM type
state1 principal ( / ) principal state2 msgNum
state1 principal ( / ) principal state2 msgNum
……
end
```

其中: begin/end表示特征在这一行开始/结束; NUM表示一个数字值,暗示是否这个特征紧跟着是一个正确的协议运行或是一个攻击 (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为这个特征表示的攻击类型; state1表示有限自动机在事件 (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,如 S1表示状态 1, FS表示结束状

**收稿日期**: 2006-11-03; **修回日期**: 2007-04-05 **基金项目**: 国家自然科学基金资助项目 (60472022)

**作者简介**:郝耀辉 (1978-),女,河南兰考人,硕士研究生,主要研究方向为网络安全、数据库技术 (hao_yaohui@126.com);郭渊博 (1975-),男,博士,主要研究方向为分布式系统、秘密共享、容忍入侵等;刘伟 (1963-),男,副教授,硕导,主要研究方向为计算机操作系统;李景锋 (1977-),男,江苏南京人,博士,主要研究方向为网络技术、密码协议等.

态;/表示是发送 /接收事件;principal表示协议的参与者,用单一字母标志符表示,如 A、B、S等;msgNum表示协议正确运行时的消息序列号。

. 有限自动机

用有限状态自动机表示密码协议运行规则,每一种密码协议的运行过程,用一个有限状态自动机(FSM)表示。协议执行的每一步均对应上面划分的一个事件发生,对应到自动机上即发生一个状态转变。

定义有限状态自动机 FSM是一个五元组($\Sigma, Q, s, f, \delta$)。其中:$\Sigma$是 FSM的字母表,是事件字母表,$\Sigma$中的每个元素由事件名及事件要点来描述;$Q$是 FSM的有限状态,表示当前到达协议中的某个位置;$s \in Q$是 FSM的开始状态;$f \in Q$是 FSM的终止状态;$\delta: Q \times \Sigma \to Q$是转变关系,指明在每一状态下由各种输入所导致的转变。

状态机从初始状态起,根据当前状态、输入事件字母和转移函数决定自动机的下一步状态;如果输入结束时,自动机处于终结状态集合 $f$的某一个状态,表示协议运行结束。

## 实例

下面以 Needham and Schroeder conventional (symmetric) key protocol (NSCKP)为例,说明该检测方法的工作原理。

. 正确执行描述

NSCKP可用如下形式描述:

a) A→S: A, B, Na
b) S→A: E(Kas: Na, B, Kab, E(Kbs: Kab, A))
c) A→B: E(Kbs: Kab, A)
d) B→A: E(Kab: Nb)
e) A→B: E(Kab: Nb - 1)

该检测方法中,上面的 NSCKP被表示为下面的形式:

a) A→S　b) S←A　c) S→A　d) A←S　e) A→B
f) B←A　g) B→A　h) A←B　i) A→B　j) B←A

这里每一步的特征被描述成一个事件。A→S表示 A发送一个消息给 S; S←A表示 S从 A接收到了一个消息,即主体 A发送一个消息给主体 S(被当做事件 1),相应地 S接收这个相同的消息被当做截然不同的事件 2。对应有限自动机执行过程如图 2所示。

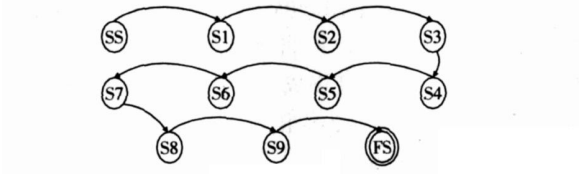


图 2　NSCKP正确执行形式

. 中间人攻击

假设在 NSCKP运行到第三步时,有一攻击者 Z监视着网络并记录了消息 3。这时 Z可伪装成 A,通过下面的步骤,欺骗 B从而获得密钥 K′ab。

a) Z(A) →B: E(Kbs: K′ab, A)
b) B→Z(A): E(K′ab: Nb)
c) Z(A) →B: E(K′ab: Nb - 1)

此时,B相信他仍在协议的正确执行中,而 Z可用盗取的密钥 K′ab,继续伪装成 A与 B通信。

. 检测攻击

上面存在中间人攻击的协议执行,按接收和发送事件可表示为以下六步:

a) Z(A) →B　b) B←Z(A)　c) B →Z(A)
d) Z(A) ←B　e) Z(A) →B　f) B←Z(A)

相应地,数据库中存储的内容为

begin NSCKP 0 S
ss B←A s1 1
s1 B→A s2 2
s2 B←A fs 3
end

这时系统中因攻击者 Z并不是协议的有效成员,不拥有监视器终端,无论他发送或接收消息,这些信息均不能通知给系统监视器,而 B却可以将与他相关的信息报告给系统监视器,即系统监视器只能收到 B的两个接收事件和一个发送事件。这时有限自动机的状态转变形式与规则库中的不一致,系统监视器将这些事件特征与存储在特征库中的攻击信息对比,与中间人攻击类型一致,产生攻击警报。

## 系统实现

该检测方法的原型系统用 VC 6.0实现。在设计和开发系统时,定义了以下的假定前提:

a)协议参与者间的通信是不安全的;

b)协议参与者与监视器终端的通信是可信赖和安全的;

c)监视器终端与系统监视器间的通信是可信和安全的。

为了处理系统在执行中多个并发会话的情况,设计系统监视器每接收一个事件,如符合一个新的协议会话的第一个事件,就产生一个新线程,用于管理对应协议的 FSM。系统监视器的检测流程如图 3所示。

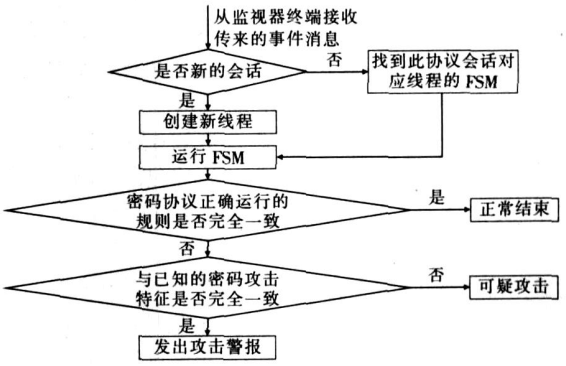


图 3　系统监视器的检测流程

为了确定系统监视器接收的事件属于哪个协议会话线程,定义 threadInfo类保存每个线程的协议名、会话号、参与者名;event类存储单一事件信息;FSM类表示有限自动机。其中包括以下五个方法:

a) createMachine( )。依据数据库中存储的数据建立有限自动机。

b) advanceFSM( )。得到此时发生的 FSM匹配事件状态的下一个状态。

c) checkNormalSession1( )。对一个协议的正常运行,检查 FSM是否可到达它的终态。

d) checkAttack( )。检查对某一攻击类型,FSM是否能前进到它的终态,并发出通告信号。

e) writeToFile( )。将检测到的攻击或可疑行为的信息写入攻击日志文件。

在 Pentium 4 2 GHz处理器的主机上,运行开发的原型程序、密码协议和系统监视器,使用一个真实网络地址的一个四星期访问日志,模拟正常 OpenSSL协议运行。因监视器终端要传送信号给在网络上的协议监视器,将导致网络通信增加。笔者在线测量了网络通信的平均开支,得到超过 1 000个 SSL会话时,平均网络通信增加 840 Byte,约 14.7%。随着运行时间增长,有限自动机状态转变次数也在增加,但 (下转第 234页)

件的完整性校验,在此过程中需要设计可信测量程序,因此,需要考虑可信测量程序的体系结构和功能模块。

c)备份和恢复。在进行完整性校验的过程中,如果发现有被破坏的组件,则不能将运行控制权交给该模块。正确的方法是用先前备份的模块替换该模块,该模块才能被执行。

## 安全性分析

从整个过程中可以看出,只有通过破坏计算机系统的物理安全,即对 0层中 TPM进行修改,才能破坏整个过程。这可通过增强物理安全和加大管理措施得以保障[14,15]。如果信任根的安全得到了保证,整个可信引导过程的安全性也就得到了保证。信任根的安全体现在以下几方面:

a)为了证明 TPM的身份是合法的,可以用公钥证书体系来增强整个验证过程的安全性。将 TPM和由 CA签署的身份证言证书绑定(也可以直接就是一个私钥,称为背书密钥 EK),通过使用代表它身份的密钥签名数据来表明它自身是可信赖的。签名密钥只有 TPM自己知道,并且是公钥对中的私钥。

b)要保证引导组件及其验证码在可信测量模块中的存储是安全的,那么验证码可以不仅是一个哈希值,而且是以证书 C的形式存在,证书中包括一个惟一的部件标志符、一个过期日期和哈希值 H。可信测量模块用 TPM的私钥对 C进行签名存储。当且仅当以下条件成立时,TPM才返回一个验证通过的状态标志:证书 C没有过期;C的签名是有效的;存储在证书中哈希值 H与引导组件的计算值相匹配。

当可信测量模块在报告验证码和度量值时,是用代表它身份的私钥对数据签名,引导组件获取数据后根据签名可以判断数据是否在传送过程中被窜改;同时还可以通过该签名来证明可信测量模块的身份。

## 结束语

可信计算是近年来信息安全界和系统结构领域关注的重点。进一步的工作包括:将该可信引导过程在相关操作系统平台如 Linux,UNIX上的实施;需要进一步研究操作系统动态执行环境的可信性。

**参考文献**:


[1] 程耕国,刘先勇,鲍考明. Linux内核启动过程分析[J]. 计算机工程与设计,2006,27(9):1528-1529.

[2] 方艳湘,黄涛. Linux可信启动的设计与实现[J]. 计算机工程,2006,32(9):51-53.

[3] Trusted Computing Group[EB/OL]. (2001). http//www. trustedcomputinggroup. org

[4] ARBAUGH W A, FARBER T D J, SMITH J M. A secure and reliable bootstrap architecture[C]//Proc of the IEEE Symposium on Security and Privacy. 1997.

[5] CAI Yi. Research on secure operating system for supporting trusted operating platform[D]. Wuhan: Naval University of Engineering, 2005.

[6] 沈昌祥. 构造积极防御综合防护体系[J]. 信息安全与保密,2004(5):17-18.

[7] 周明辉,梅宏. 可信计算初探[J]. 计算机科学,2004,32(7):5-8.

[8] 林闯,彭雪梅. 可信网络研究[J]. 计算机学报,2005,28(25):751-758.

[9] 侯方勇,周进,王志英,等. 可信计算研究[J]. 计算机应用研究,2004,21(12):1-4,22.

[10] 陈钟,刘鹏,刘欣. 可信计算概论[J]. 信息安全与通信保密,2003(11):17-19.

[11] 谭良,周明天. CRL分段—过量发布新模型[J]. 电子学报,2005,33(2):227-230.

[12] 谭良,周明天. CRL增量—过量发布新模型[J]. 计算机科学,2005,32(4):133-136.

[13] 郑宇,何大可,何明星. 基于可信计算的移动终端用户认证方案[J]. 计算机学报,2006,29(8):1255-1264.

[14] QUISQUATER J J, SAMYDE D. Electromagnetic analysis(EMA): measures and countermeasures for smart cards[M]. [S l]: Springer-Verlag, 2001.

[15] BONEH D, DeMILLO R, LIPTON R. On the importance of checking cryptographic protocols for faults[M]. [S l]: Springer-Verlag, 1997.


(上接第 231页)逐渐趋于平稳。两者关系如图 4所示。

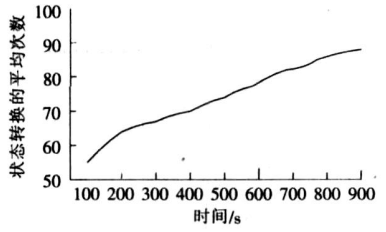


图 4 有限自动机状态转变次数与运行时间的关系

## 结束语

本文提出了一种在应用层分析密码协议攻击的方法,能实时动态地检测密码协议运行,尤其对并行会话攻击,每个协议会话均对应一独立的线程,可同步互斥地检测,及时发现攻击,保护合法区域内的网络安全。最后通过对开发的原型系统测试,证实该方法能有效检测密码协议上的攻击,且对网络性能影响较小;但当协议会话数目较大时,有限自动机的状态转变次数也会相应增大,可能会造成状态空间爆炸,对此有待进一步的研究和改进。

**参考文献**:


[1] HEINTZE N, TYGAR J D. A model for secure protocols and their composition[J]. IEEE Transactions on Software Engineering, 1996,22(1):16-30.

[2] YASINSAC A. Dynamic analysis of security protocols[C]//Proc of New Security Paradigms 2000 Workshop. Ireland: [s n], 2000:77-87.

[3] YASINSAC A. An environment for security protocol intrusion detection[J]. Journal of Computer Security, 2002,10:177-188.

[4] SHERWOOD R W. Methods of detecting intrusions in security protocols[D]. FL, USA: Florida State University Tallahassee, The Florida State University College of Arts and Sciences, 2004.

[5] YASINSAC A. Detecting intrusions in security protocols[C]//Proc of the 7th ACM Conference on Computer and Communications Security. Athens: [s n], 2000.

[6] JOGLEKAR S P, TATE S R. Embedded monitors for cryptographic protocol intrusion detection and prevention[C]//Proc of IEEE Conference on Information Technology: Coding and Computing (ITCC). Orleans: [s n], 2004:81-88.

[7] MAO W. Modern cryptography: theory and practice[M]. 北京:电子工业出版社,2004.

[8] SEKAR R, GUPTA A, FRULLO J, *et al*. Specification based anomaly detection: a new approach for detecting network intrusions[C]//Proc of the 9th ACM Conference on Computer and Communications Security. Washington D C: [s n], 2002:265-274.

[9] 卓继亮,李先贤,李建欣,等. 安全协议的攻击分类及其安全性评估[J]. 计算机研究与发展,2005,42(7):1100-1107.