一种基于通道的 AVISPA 扩展方法研究*

刘 威[a,b], 郭渊博[a,b]
(解放军信息工程大学 a. 网络空间安全学院; b. 数学工程与先进计算国家重点实验室, 郑州 450001)

摘 要: 针对 AVISPA 工具在分析某些消息需要依靠具有特定属性的信道传递的安全协议或服务中存在的问题,提出了一种基于抽象通道的扩展方法。抽象通道具有相关的安全性质保证如认证性,能够对提供安全性质保证的底层服务建模,并基于密码机制和标签等实现了抽象通道。利用扩展后的 AVISPA 工具分析有无消息源认证机制的 Diffie-Hellman 密钥交换协议的安全性,表明了方法的有效性,并且能够简化协议建模过程和增强 AVISPA 工具协议描述分析能力。

关键词: 安全协议; 形式化分析; 安全属性; 抽象通道
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2013)12-3783-03
doi:10.3969/j.issn.1001-3695.2013.12.068

Extension of AVISPA based on concept of channels

LIU Wei[a,b], GUO Yuan-bo[a,b]
(*a. Institute of Cyberspace Security, b. State Key Laboratory of Mathematical Engineering & Advanced Computing, PLA Information Engineering University, Zhengzhou* 450001, *China*)

Abstract: For the transmission of some of protocol messages relies on channels with particular security properties, this paper proposed an extension of AVISPA based on abstract channels. It supplied security guarantees such as authentication by abstract channels, and with which it could model the underlying services providing security guarantees. It realized abstract channels with cryptography schemes and labels, and validated the model by verifying Diffie-Hellman key exchange protocol with message origin authentication using extended AVISPA automatically. The extension can simplify protocol modeling and enhance the power of the mechanized tool AVISPA.

Key words: security protocols; formal analysis; security properties; abstract channels

安全协议是建立在密码体制基础上的一种交互式通信协议,运行在计算机通信网或分布式系统中,是构建安全网络环境的基石。近些年提出的许多安全协议在刚出现的时候都被认为是安全的,但是很快就被证明存在安全漏洞。因此,安全协议形式化分析是一项必要的工作,不仅能够发现安全协议存在的缺陷和漏洞,而且对协议的设计过程具有指导作用。AVISPA(automated validation of Internet security protocols and applications)[1]是一套著名的建立和分析安全协议模型的工具,用于验证各种网络安全协议。AVISPA 具有模块化、表达能力强的形式化语言规范安全协议和属性,集成不同的后端分析工具,实现了多种自动化分析技术,如有限和无限会话的协议验证方法,使得 AVISPA 工具适合大型网络安全协议分析并被广泛采用[2]。

对 AVISPA 工具进行分析可以发现,该工具使用了 Dolev-Yao[3]入侵者模型,即假设通信信道由入侵者完全控制,协议中消息传递必须经过入侵者,并且假设协议中采用的密码算法和密码系统都是安全的。考虑现实应用环境、协议或服务的某些消息需要依靠具有特定属性的信道来传递,如 PBK(purpose built keys)协议[4]假设通信双方信道提供第一条消息完整性保护,接下来的消息可经不安全信道传递。但是现有的工具并不能在此前提之上验证协议,需要对提供这些安全保证的底层服务进行详细分析和形式化描述,这其中涉及到密码操作、随机数使用等,这将对协议分析增加不必要的复杂性。为了避免协议分析者陷入底层密码等服务的细节,在 Dolev-Yao 模型的基础上提出抽象通道概念。通过将提供安全性质保证的底层服务建模为抽象通道,在抽象通道的基础上进行协议分析,能够增加系统表达能力,简化协议建模过程,降低协议分析复杂度。

1 相关知识

AVISPA 融合了四种不同的分析工具[1],能够更好地保证安全协议形式化分析的准确性。AVISPA 使用高层协议规范语言(high level protocol specification language, HLPSL)[5]来描述所要分析的安全协议和被检验的安全目标,然后编写的代码要通过 HLPSL2IF 自动化翻译工具转换成 IF(intermediate format)语言。AVISPA 工具集内的分析工具可以直接读取 IF 语言,分析出安全目标是否满足。如果协议不安全,分析工具会给出导致此事件发生的攻击轨迹,据此可采用相应的安全策略改进协议。AVISPA 的结构如图 1 所示。

1.1 HLPSL

HLPSL 是基于角色(role)的形式化规范语言,具有基于行为时序逻辑(temporal logic of actions, TLA)的说明性语义和

收稿日期: 2013-02-20; **修回日期**: 2013-04-07 **基金项目**: 国家部委基金资助项目(9140C130103120C13062)

作者简介: 刘威(1989-),男,河南太康人,硕士研究生,主要研究方向为信息与网络安全(liu.w.tk@gmail.com);郭渊博(1975-),男,陕西周至人,副教授,硕导,博士,主要研究方向为网络与通信、信息与网络安全.

基于翻译到 IF 的操作性语义，支持分支、多层加密、hash、集合和异或指数运算等描述，也允许入侵者以合法身份参与协议会话[2]。HLPSL 中定义的角色有参与协议的主体和代表协议会话的角色。下面对 HLPSL 作简要介绍：

a)角色。HLPSL 中角色包括基本角色和组合角色两种类型。基本角色定义协议参与者的初始知识和行为，组合角色初始化基本角色、定义协议会话和入侵者初始知识。

b)转换规则。HLPSL 使用转换规则来描述协议诚实参与者的行为。转换规则左端描述转换触发的条件，如参与者状态、收到特定消息等；右端表示条件满足时执行的一系列事件，如生成随机数、参与者发送相应消息等。

c)通道(channel)。HLPSL 使用 channel 通道发送和接收消息。在转换规则左端使用通道，表示在此通道上接收消息；通道用在右端，表示利用通道发送消息。默认的入侵者模型是著名的 Dolev-Yao 模型。在此模型下，入侵者对网络具有完全控制权，主体发送的所有消息都会被送往入侵者。入侵者可以窃听、截取、修改消息(前提是知道必要的密钥)，也能够以任意主体身份发送其构造的消息给任意主体。

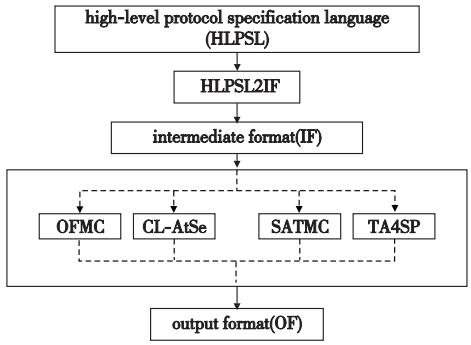

图1 AVISPA安全协议分析工具结构

1.2 IF

AVISPA 中间层语言 IF 是基于术语重写系统的底层工具无关语言，设计用来描述状态转换系统，易于协议分析工具分析。IF 具有清晰且定义明确的语义[6]。IF 规范主要包含初始状态、状态转换规则和攻击状态。若使用转换规则从初始状态出发没有攻击状态是可达的，则称协议是安全的。

初始状态描述入侵者的初始知识和诚实主体的状态。IF 状态是 fact 类型变量的集合。这里介绍常用的两个 fact 类型，其他类型的 fact 这里不作介绍。iknows(m)，表示在这个状态中入侵者知道消息 m，它具有持续性，据此可以简化规则的公式描述；$\text{state}_A(m_1, m_2, \cdots, m_n)$，是利用消息 $m_1, m_2, \cdots, m_n$ 来描述诚实主体的局部状态，其中下标 A 标示主体的角色。

IF 规范的转换规则与 HLPSL 的转换规则相对应，具有形式：$L \mid \text{Cond} = [V] \Rightarrow R$。其中：$L$ 和 R 是状态，V 是变量的集合，这些变量将会用新鲜数值初始化，R 只包含来自 L 或 V 中的变量；Cond 是一组条件的集合，可以是等式或不等式，或者是 fact 的否定式。转换规则用来描述入侵者的能力和诚实协议参与者的行为。例如，用下面形式的一组规则来定义 Dolev-Yao 入侵者模型，描述入侵者的行为能力：

$$\text{iknows}(M).\ \text{iknows}(K) \Rightarrow \text{iknows}(\{M\}_K)$$

$$\text{iknows}(\{M\}_K).\ \text{iknows}(\text{inv}(K)) \Rightarrow \text{iknows}(M)$$

$$\text{iknows}(\{M\}_{\text{inv}(K)}) \Rightarrow M$$

由于 iknows(.)具有持续性，转换规则右端可以省略左端的 iknows(.)。第一条规则描述非对称加密或签名；第二条规则描述知道相应密钥的情况下，可以解密一条加密的消息；第三条规则表示数字签名消息的明文总是可以得到的。

诚实用户的状态转换规则通常有此形式：

$$\text{state}_R(\text{msglist}).\ \text{iknows}(\text{msg}_{\text{in}}) = [V] \Rightarrow \text{iknows}(\text{msg}_{\text{out}}).\ \text{state}_R(\text{msglist}')$$

这条规则描述诚实主体状态的转换关系，该主体扮演协议中的角色 R，其当前局部状态用消息列表 msglist 描述。该主体收到一条消息 msg_{in}，生成了新值 V，并更新其局部状态为 msglist′和发送消息 msg_{out}作为回应。这里，收到和发送的消息都是通过不安全信道传输的。

2 AVISPA 通道扩展

不同类型的抽象通道可以作为保障通信安全的手段应用到安全协议和 Web 服务中。本文主要考虑三种基本类型的抽象通道：认证、机密和安全通道。为了实现抽象通道，需要修改 HLPSL 以允许协议分析者能够利用抽象通道发送和接收消息，同时需要扩展 IF 以实现底层对抽象通道的支持。

2.1 抽象通道概念

为了便于说明三种基本类型的抽象通道，本文定义 $R_i \rightarrow R_j$ 为连接主体 R_i 和另一主体 R_j 的通道，并使用标签区分不同类型的通道[7]。

$A(R_i \rightarrow R_j, \text{Msg})$表示从 R_i 到 R_j 的认证通道。R_j 能确信通过此通道接收的消息 Msg 来自于 R_i，此通道保证了消息发送者身份不变性。

$C(R_i \rightarrow R_j, \text{Msg})$表示从 R_i 到 R_j 的机密通道。R_i 能确信通过此通道发送的消息 Msg 仅有 R_j 能够读到，任何入侵者不能获知此通道上消息的内容。

$S(R_i \rightarrow R_j, \text{Msg})$表示从 R_i 到 R_j 的安全通道。使用此通道发送消息，能够同时保证消息的认证性和机密性。

2.2 通道类型定义

在 HLPSL 引入两个新概念：抽象通道类型和消息参数。抽象通道类型有认证、机密和安全通道，符号化为 channel(authentic)、channel(confidential)和 channel(secure)。这样定义抽象通道类型，由于声明方法保持一致，可以与 Dolev-Yao 通道类型兼容，例如 Auth_AB：channel(authentic)表示 Auth_AB 是一个认证通道，在其上发送消息，接收者能够确信消息的来源。但由于抽象通道类型的特殊性，需要引入附加信息到抽象通道中。

使用抽象通道发送和接收消息时需要使用消息参数，消息参数指定一个 to 和一个 from 地址。当发送消息时，from 域标志发送消息的主体，to 域标志预定接收此消息的主体。当接收消息时，from 域标志消息的发送者，to 域标志接收此消息的主体。抽象通道使用此信息推理消息的源和目的地址，下层可以相应地实现抽象通道的行为。

抽象通道类型使用必须指明消息参数。唯一不要求消息参数的通道类型是 Dolev-Yao 通道，这样可以保证语言的兼容性。例如在协议描述中使用认证通道——Auth_AB(A,B,M)，表示主体 B 可以认证主体 A 的身份，相信消息 M 是由主体 A 发送的而不是其他主体冒充 A 发送的。使用认证通道可以对提供身份认证的 Diffie-Hellman 密钥交换协议建模其认证性，进而分析密钥交换协议的安全性。

2.3　通道的翻译过程

HLPSL 的语义是通过翻译成 IF 来定义的,这样有利于模型检测和自动化验证。通过把通道的发送和接收动作合理地翻译到底层术语重写系统,实现通道的行为。对于不安全通道,在诚实主体的转换规则中,收到和发送消息用 iknows(M)代替,因为 Dolev-Yao 模型下,入侵者就是网络,所有的消息都经过入侵者。

对于认证通道、机密通道和安全通道等,结合后端协议分析工具在不安全通道上可以采用密码机制等实现抽象通道的相关属性。认证通道的行为利用对发送者消息数字签名来实现,且把预定接收者作为签名的一部分;保密通道的行为可看做接收者公钥的消息加密;而安全通道可综合认证通道和保密通道的性质实现。表 1 具体说明抽象通道的翻译过程。

表 1　抽象通道的翻译过程

channel	HLPSL	IF
Dolev-Yao	SND(M)orRCV(M)	iknows(M)
authentic	Auth_AB(A,B,M)	iknows($\{\text{atag},B,M\}_{\text{inv(ak}(A))}$)
confidential	Conf_AB(A,B,M)	iknows($\{\text{ctag},M\}_{\text{ck}(B)}$)
secure	Sec_AB(A,B,M)	iknows($\{\{\text{stag},B,M\}_{\text{inv(ak}(A))}\}_{\text{ck}(B)}$)

针对此模型,引入了新符号 atag、ctag、stag、ak 和 ck。这里 atag、ctag 和 stag 是标签用来区分抽象通道类型,ak 和 ck 是公共密钥表,分别用于签名和加密。假设每一个主体包括入侵者知道公钥表以及它们自己的私钥,因此,抽象通道模型下入侵者增加的初始知识有{ak,ck,inv(ak(i)), inv(ck (i)),atag,ctag,stag}。使用的编码对于本文的目的是有效的,但并不是唯一的,对于这种实现方式还有其他可能的方法。例如,可能选择不区分签名和加密密钥,但是必须保证签名绝不能解密一条加密的消息。

对于认证和安全通道,本文在消息的签名部分包含了预定接收者的名字。这样可以确保消息不能被再次发送给一个不同的接收者。考虑安全通道的一种可能编码不包含这样一个名字:$\{\{\text{stag},M\}_{\text{inv(ak}(A))}\}_{\text{ck}(B)}$。一个主体 X 用不合法手段获得了主体 B 的私钥,能解开外层加密获得$\{\text{stag},M\}_{\text{inv(ak}(A))}$并使用主体 C 的公钥重新加密发送给主体 C。消息 M 就错误地成了由 A 发送给 C 的,这样一个错误经常是安全协议中问题的根源,如文献[8]。在消息签名部分包含接收者名字,能够阻止此类型攻击。认证通道也是如此,保证安全通道结合了认证和保密通道的属性。

标签还决定消息的含义(从生成消息的主体视角),消息应具有相应通道类型的安全属性,并且接收者根据协议仅仅接收具有正确标签的消息。

3　实例验证及结果分析

以 Diffie-Hellman 密钥交换协议(DHKE)[9]为例说明抽象通道类型在协议分析中的使用。设 p 为 512 bit 以上大素数,$g<p$,p、g 公开,典型的基于离散数对的 DHKE 协议主要包含以下步骤:

a)主体 Alice 随机选择 $x<p$,计算 $X=g^x \pmod p$,并将 X 发送给主体 Bob,其中 x 由 Alice 秘密保存。

b)主体 Bob 随机选择 $y<p$,计算 $Y=g^y \pmod p$,并将 Y 发送给 Alice,其中 y 由 Bob 秘密保存。

c)Alice 通过自己的 x 秘密计算 $Y^x \pmod p=(g^y)^x \pmod p)=g^{xy} \pmod p$。

d)Bob 通过自己的 y 秘密计算 $X^y \pmod p=(g^x)^y \pmod p=g^{xy} \pmod p$。

主体 Alice 和 Bob 拥有相同的数据 $g^{xy} \pmod p$作为共同的秘密密钥进行保密通信。这里协议使用算法的安全性主要依赖于有限域上的离散数对问题,已证明是安全的。但协议使用不安全信道传输消息 X 和 Y,并没有提供通信双方 Alice 和 Bob 的身份验证服务,因此它很容易受到中间人攻击[10]。

利用 HLPSL 对上述 DHKE 协议进行建模分析其安全性,限于篇幅具体过程不再叙述,分析结果如图 2 所示。AVISPA 工具给出的分析结果是协议不安全并给出了攻击路线。入侵者 I 可以截获 Bob 发送来的消息并给 Alice 发送自己构造的消息,该消息具有 Bob 的用户 ID 但使用了 I 生成的公开密钥 X',Alice 收到 I 的消息后,将 X'和 Bob 的用户 ID 存储在一起。类似地,I 使用 X'向 Bob 发送好像来自 Alice 的消息。这样,I 可以同时与 Alice 和 Bob 建立共享密钥,破坏合法用户传递秘密数据的安全性。

由以上分析发现,DHKE 协议发生中间人攻击的原因是通信双方无法验证消息的来源。考虑为 DHKE 协议引入消息来源认证机制,为通信双方提供身份认证服务。利用提出的基本抽象通道类型里的认证通道对新协议中消息认证部分建模,主体 Alice 状态转移部分代码如下:

```
%%   Extended HLPSL
  init State := 0
  transition
  1. State = 0 ∧ RCV(start) = |>
  State′: = 2 ∧ X′: = new()
                ∧ Auth_AB(A,B,exp(G,X′))
                ∧ witness(A,B,authen,exp(G,X′))
  3. State = 2 ∧ Auth_BA(B,A,exp(G,Y′)) = |>
  State′: = 4 ∧ Msg′: = new()
                ∧ SND({Msg′}_Kab)
                ∧ secret(Msg′,msg,{A,B})
```

代码中 Auth_AB( )是认证通道,对消息 exp(G,X)来源身份认证部分建模,为消息提供认证保护机制;witness( )用于验证消息 exp(G,X)的认证性;secret( )用于验证消息 Msg 的机密性。利用扩展的 AVISPA 工具进行安全性分析,结果如图 3 所示。分析结果表明,提供消息源验证功能的 DHKE 协议是安全的,能够保证消息安全传输不会被第三方知道,也就是共享密钥是安全的。

图2　原始DHKE协议分析结果

图3　具有身份认证的DHKE协议分析结果

4　结束语

本文提出了抽象通道的概念,并对 HLPSL 进行抽象通道扩展,实现了三种类型的抽象通道。利用扩展后的工具对有无消息源认证机制的 DHKE 协议进行验证,实验结果与预期一致,表明提出的基于通道的扩展方法是有效的,能够简化协议分析过程,而且文中的扩展方法扩展性强,便于实现其他类型的抽象通道,如匿名通道。

(下转第 3803 页)

对于数据集 C 的查准率最高,三种算法对于数据集 B 的查准率最低。综合三个数据集的测试结果,算法 3 的效果最好。

对实验结果进行分析,数据集 A 中的内容主要是一些网络入侵行为的数据,这些数据的特征比较明显,传统的数据流分析手段基本都对这些特征进行了优化,因此检测效果较好,算法 1 略优于算法 2,本文的 NBD 算法经过充分的预处理也达到了不错的查准率。数据集 B 来源于某市基于互联网电子政务信息系统的内网核心交换机,经过抓包分析,这些数据包中不仅包含电子政务信息系统运行所产生的信息,还包含了大量来自互联网的数据和一些即时通信、P2P 应用等程序所产生的数据,进而还可能包含一些木马病毒等恶意程序产生的数据。此外,政务办公系统中传输的数据有较强的时效性,不同时间段内,其中的数据成分也有很大不同,这给基于统计分析的算法 1 造成了一些困难,此时基本协议解析的算法 2 效果好于算法 1,本文的 NBD 算法将数据流解析与网络行为结合达到了更好的检测效果。数据集 C 来源于本课题组开发的 OA 办公系统,其中所捕获的数据较为单一,主要为信息系统运行所产生的 Web 访问数据。由于数据较为纯净,三种算法的检测效果均较数据集 B 有所提高,但本文的 NBD 算法优势更为明显。分析其原因是由于针对某一具体的信息系统,其中的访问数据主要为 HTTP,数据流之间的流量特征和协议区别不是很明显。相反对于本文的 NBD 算法,能够捕获系统运行过程中的行为信息,提高了检测的准确率。

由实验可以发现,本文所提出的 NBD 算法在三种不同条件下,其效果均优于其他两种方法。但是本文提出的算法亦存在不足,该算法需要预先进行处理,提取数据流中的事件并建立相应的网络行为分析图,且检测效果与分析图的选择有较大关系。不过,具体到某一个应用环境中,其中的特定行为模式在一定时间内一般变化不大,采用本方法可以实现更好的检测效果。

4　结束语

对数据流进行分析,获取数据流中的潜在规律,能够为许多现实应用提供重要的决策支持。本文提出了一种基于数据流分析的网络行为检测方法。通过对网络数据流进行建模分析,提出一种基于与或图的网络行为描述方法;在此基础上又设计了基于数据流分析的网络行为检测算法,提高了对网络行为的检测能力。本文所提出的数据流分析方法可适用于基于数据流的访问控制、审计分析、行为预测等诸多领域,具有广泛的应用价值。

参考文献:

[1] 余晓永. 基于网络行为分析的入侵检测系统研究[D]. 合肥:合肥工业大学,2009.

[2] 胡柳武. 网络行为检测与评估技术研究[D]. 北京:北方工业大学,2012.

[3] BABCOCK A K, BABU S, DATAR M. Model and issues in data stream systems[C]//Proc of the 21st ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems. New York:ACM Press,2002:1-16.

[4] 祝然威, 王鹏, 刘马全. 基于计数的数据流频繁项挖掘算法[J]. 计算机研究与发展,2011,48(10):1803-1811.

[5] 常建龙,曹锋,周傲英. 基于滑动窗口的进化数据流聚类[J]. 软件学报,2007,18(4):905-918.

[6] 杨博,刘大有,LIU Ji-ming,等. 复杂网络聚类方法[J]. 软件学报,2009,20(1):54-66.

[7] 延皓. 基于流量监测的网络用户行为分析[D]. 北京:北京邮电大学,2011.

[8] 李军,曹文君,李杨. FB-NBAS:一种基于流的网络行为分析模型[J]. 计算机工程,2008,34(3):165-167.

[9] LIU Yi-qun, CEN Rong-wei, ZHANG Min, *et al*. Identifying Web spam with user behavior analysis[C]//Proc of AIRWeb. 2008.

[10] BIANCO A, MARDENTE G, MELLIA M, *et al*. Web user-session inference by means of clustering techniques[J]. IEEE/ACM Trans on Networking,2009,17(2):405-416.

[11] 陈亮,龚俭,徐选. 基于特征串的应用层协议识别[J]. 计算机工程与应用,2006,42(24):16-19.

[12] MEISS M, DUNCAN J, GONCALVES B, *et al*. What's in a session: tracking individual behavior on the Web[C]//Proc of the 20th ACM Conference on Hypertext and Hypermedia. 2009:173-182.

[13] 牛瑞. 主机网络行为模式特征与辨识研究[D]. 北京:北京化工大学,2008.

[14] 单棣斌,陈性元,张斌,等. 基于数据流分析与识别的 Web 资源访问控制[J]. 计算机工程,2008,34(23):53-55.

[15] LUGER G F. Artificial intelligence:structures and strategies for complex problem solving[M]. [S.l.]:Pearson Education,2002:89-91.

[16] 谢希仁. 计算机网络[M]. 4 版. 北京:电子工业出版社,2003:20-23.

[17] 张文,沈磊. 基于特征进程的 P2P 流量识别[J]. 计算机工程,2008,34(15):120-122.

(上接第 3785 页)

参考文献:

[1] VIGANO L. Automated security protocol analysis with the AVISPA tool[J]. Electronic Notes in Theoretical Computer Science,2006,155:61-86.

[2] ARMANDO A, BASIN D, BOICHUT Y, *et al*. The AVISPA tool for the automated validation of Internet security protocols and applications[C]//Lecture Notes in Computer Science, vol 3576. Berlin:Springer-Verlag,2005:281-285.

[3] DOLEV D, YAO A C. On the security of public-key protocols[J]. IEEE Trans on Information Theory,1983,29(2):198-208.

[4] BRADNER S, MANKIN A, SCHILLER J. A framework for purpose-built keys (PBK)[EB/OL]. [2013-01-20]. http://tools.ietf.org/search/draft-bradner-pbk-frame-06.

[5] The AVISPA Team. The HLPSL tutorial:a beginner's guide to modeling and analysing Internet security protocols[EB/OL]. [2013-01-20]. http://www.avispa-project.org.

[6] The AVISPA Team. AVISPA v1.1 user manual[EB/OL]. [2013-01-20]. http://www.avispa-project.org.

[7] DILLOWAY C, LOWE G. On the specification of secure channels[C]//Proc of the 7th International Workshop on Issues in the Theory of Security. 2007:118-123.

[8] CERVESATO I, JAGGARD A D, SCEDROV A, *et al*. Breaking and fixing public-key Kerberos[J]. Information and Computation,2008,206(2-4):402-424.

[9] 冯超,张权,唐朝京. 计算可靠的 Diffie-Hellman 密钥交换协议自动证明[J]. 通信学报,2011,32(10):118-121.

[10] 徐恒,陈恭亮,杨福祥. 密钥交换中中间人攻击的防范[J]. 信息安全与通信保密,2009(2):90-92.