密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2014,1(5): 504–512

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-81033101

安全协议形式化分析研究*

高 尚, 胡爱群, 石 乐, 陈先棒

东南大学 信息科学与工程学院 信息安全研究中心, 南京 210096
通讯作者: 胡爱群, E-mail: aqhu@seu.edu.cn

摘 要: 计算机网络中, 安全协议为通信双方的信息交互提供安全保证, 是计算机网络安全的基础. 而当安全协议中存在安全漏洞时, 会对信息安全产生重大威胁, 造成数据泄露、身份被冒用等危害. 因此, 对于安全协议安全性的研究, 历来都属于安全领域的重要研究方向. 目前的安全性分析方法主要是通过协议形式化分析与验证来实现. 形式化分析方法的理论体系大致可分为三类: 模态逻辑技术、模型检测技术和定理证明技术. 在不同类别的理论体系中, 所使用的技术方法各有不同, 对安全协议分析的侧重点也略有不同. 对于每一种理论体系, 研究者们也提出了不同的方法, 以及针对经典方案的改进来提高形式化分析的准确性. 对于复合协议, 其主要问题是通过对多种现有可靠安全协议加以组合, 构成新的协议并保持其安全性可靠. 对于复合协议的安全性分析, 也有异于普通的安全协议形式化分析. 本文总结了各种类别中的主要分析方法, 并比较了每种方法的优缺点, 同时特别针对复合协议的安全性分析技术进行了概述. 最后指出了形式化分析方法中需要解决的问题, 以及下一步的研究方向.

关键词: 安全协议; 协议形式化分析; 复合协议
中图法分类号: TP309.7 **文献标识码**: A DOI: 10.13868/j.cnki.jcr.000047

中文引用格式: 高尚, 胡爱群, 石乐, 陈先棒. 安全协议形式化分析研究[J]. 密码学报, 2014, 1(5): 504–512.
英文引用格式: Gao S, Hu A Q, Shi L, Chen X B. A survey on formal analysis of security protocols[J]. Journal of Cryptologic Research, 2014, 1(5): 504–512.

A Survey on Formal Analysis of Security Protocols

GAO Shang, HU Ai-Qun, SHI Le, CHEN Xian-Bang

Information Security Research Center, Department of Information Science and Technology, Southeast University, Nanjing 210096, China
Corresponding author: HU Ai-Qun, E-mail: aqhu@seu.edu.cn

Abstract: Security protocols are basis for computer network security, and provide important secure insurance for information exchanging. It may cause great threat to the information security such as data leakage and fraudulent identity when there are flaws in security protocols. Therefore, it has always been a hot research area for the security of these protocols. The nowadays study for them is mainly through formal analysis. It can be classified into three types for theses protocols analysis; they are the model logic axiomatic technology, the model

* 基金项目: 国家重点基础研究发展项目(973 计划)(2013CB338003)
收稿日期: 2014-9-30 定稿日期: 2014-10-04

checking technology and the theorem proving technology. Each technology uses different ideas and lays different emphasis for each type. For each technology, researches also propose different methods and improvements for classic methods to improve the accuracy of formal analysis. For composed protocols, the main problem is to merge several secure protocols into one new protocol and ensure its security at the same time. In this paper, we first make a survey on various kinds of method in different analysis technologies, and conclude advantages and disadvantages of each method. Furthermore, we make an overview of the security analysis for composed protocols. Finally, we point out several problems and some research directions for further study in formal analysis of security protocols.

Key words: security protocols; formal analysis; composed protocols

1 引言

随着信息化的不断进步和发展, 计算机网络得到普及. 在众多网络协议中, 安全协议为通信双方提供信息交互安全的可靠保证, 因此成为网络协议中最重要的协议. 安全协议可以解决网络通信中的参与者身份认证、消息完整性检验、匿名通信、抗抵赖和认证等问题.

安全协议是保证信息安全的重要方法, 但是其也可能存在漏洞, 导致无法达到预期的安全性. 因此, 对于安全协议的安全性分析便显得尤为重要. 目前的分析方法是对安全协议进行形式化分析. 形式化分析方法的理论体系可分为三类: 模态逻辑技术、模型检测技术和定理证明技术. 不同体系中, 对安全性分析的侧重略有不同. 本文对目前主流的形式化分析方法进行了归纳总结, 并分析比较了各种方法的优缺点. 此外, 本文对复合协议的安全性检测进行了概述. 最后分析了下一步的研究方向.

1.1 安全协议基本概念

协议指两个或两个以上的参与者, 采取一系列步骤以完成某项特定的任务. 在协议交互过程中, 通信者可能会对消息有机密性或对对方有身份验证等有一定要求, 而安全协议就是在传统的协议交互过程中, 采取一系列的密码算法, 来满足通信者的上述要求的协议. 根据通信者的不同要求, 安全协议可以划分为以下几类:

(1) 密钥交换协议: 该类协议一般为通信双方或多方之间协商一个会话密钥. 该会话密钥一般通过主密钥来产生.

(2) 认证协议: 该类协议主要目的是确定通信过程中某些信息, 这些信息包括通信对方的身份、消息的目的等. 主要用来防止伪造、篡改和否认等攻击.

(3) 认证及密钥交换协议: 该协议结合了上述两种协议的目的, 首先进行认证确定身份等信息, 通过认证后进行密钥交换来确定会话密钥. 目前互联网中的安全协议大部分是该类协议.

1.2 形式化分析的分类

目前的安全协议形式化分析工作, 主要是基于模态逻辑技术、模型检测技术和定理证明技术三种理论体系展开的[1−3].

模态逻辑技术通过信仰逻辑分析方法和知识逻辑分析方法来分析在安全协议过程中主体的信仰和知识的变化. 模态逻辑方法的基本思想包括三点: 执行前, 主体拥有初始信仰和知识; 执行时, 主体之前互相传递信仰和知识; 执行结束, 主体能否达获取期望的目标信仰或知识.

模型检测技术中, 采用模拟和分析硬件数字电路工程的技术, 将安全协议看成一个分布式系统, 并为该系统定义安全属性或不变关系. 根据协议推导其中各个主体的状态来判断系统在每个可达的全局状态上是否满足安全属性或不变关系.

定理证明技术通过将安全协议描述为公理系统, 将目标描述成需要证明的定理. 安全协议是否符合安全目标则对应于公理系统中的目标定理是否成立.

1.3 形式化分析的发展

最早从事安全协议形式化分析的是 Needham 和 Schroeder. 二人于 1978 年提出了安全协议形式化分析的思想, 但是其主要工作是仅仅建立了 Needham-Schroeder 安全协议[4]. 真正的具有实质性的工作是在 1983 年由 Dolev 和 Yao 为验证安全协议的安全性而建立的 Dolev-Yao 模型[5], 该模型对网络的攻击者进行了定义以及行为能力描述. 但 Dolev-Yao 模型的能力也是有限的, 仅可以进行部分漏洞查找, 而且也无法在状态变迁过程中加入其他用户. 在 Dolev-Yao 模型提出后, 许多学者对其进行可扩展和改进, 如 Dolev、Even 和 Karp 提出的 Dolev-Even-Karp 模型[6]、Nieh 提出的与状态空间相关的加密协议模型[7]等. 此外, 安全协议分析工具也相继被研发出来, 如 Interrogator[8]、Longley-Rigby tool[9]和 NRL 协议分析器[10,11]. 其中, NRL 协议分析器的状态空间是无限的, 也成功地应用于许多协议分析场景.

1989 年, Burrows、Abadi 和 Needham 提出了著名的 BAN 逻辑[12]. BAN 逻辑通过对协议过程和假设进行形式化, 并通过一系列的推理准则进行推理来判断是否能得到预期结果. BAN 逻辑具有简洁直观的特点, 并且容易理解也易于使用. 但同时, BAN 逻辑也存在着一些缺点, 如对完整的逻辑语义的缺乏, 以及无法对新鲜性建立模型. 针对 BAN 逻辑的不足之处, 人们也提出了众多改进方案, 包括 GNY 逻辑[13]、AT 逻辑[14]、VO 逻辑[15]、SVO 逻辑[16]等. 这些改进逻辑模型均属于类 BAN 逻辑.

1996 年, Lowe 使用通信顺序进程对安全协议进行分析[17], 并得到了不错的结果. 由此开始, CSP 模型在安全协议形式化分析中得到了应用及发展, 并迅速成为研究的热潮. Schneider 通过使用 CSP 语言, 提出了对认证属性进行分析验证的一般方法.

定理证明技术是安全协议形式化分析中新的研究热点. 这方面的工作开始于 Kemmerer 的 Ina Jo 和 ITP 的研究[18]. 此外, 还有 Bilignana 的 Coq 证明系统[19]、Snekkenes 的公理证明器 HOL[20]、Isabelle 定理证明系统[21]等. 近几年来, 又提出了归纳方法[22]和串空间方法[23]. 这两种方法与 Petri 网有着密切的关系, 其验证过程可由模型检测工具和定理证明器来完成, 具有更广阔的前景, 因此也成为研究的热点.

目前的安全协议形式化理论在分析协议安全的应用中, 主要分为形式化分析、形式化设计和自动化工具开发三个方向.

1.4 文章结构

本文第 1 节主要阐述安全协议形式化分析研究的背景, 并对安全协议形式化分析进行分类总结; 第 2 节对模态逻辑技术加以总结, 并对其中的经典方法进行概述; 第 3 节对模型检测技术加以总结, 同时根据发展历史对经典方案进行概述; 第 4 节对定理证明技术以及其中的具体方法进行总结概述; 第 5 节对复合协议安全性分析的问题进行了说明, 同时总结了现有技术方案; 第 6 节从协议形式化分析发展的角度对新的问题以及下一步的研究方向进行了展望.

2 模态逻辑技术

模态逻辑技术是一个演绎推理的过程. 这种技术通过分析通信过程中双方发送和接收的消息, 根据一系列的推理公理来判断安全协议是否能达到预期的目的. 在这种理论体系中, 推理过程大致可以分为以下 4 步进行[2,3].

(1) 将安全协议过程理想化, 进行形式化描述;

(2) 设定安全协议的初始化假设;

(3) 对安全协议的目标进行形式化描述;

(4) 从假设和协议过程的事实出发, 使用形式化逻辑对其进行推导分析, 得到最终状态时各个主体的信仰和知识, 判断其是否达到安全目标.

2.1 BAN 逻辑

BAN 逻辑[12]是最早提出的基于模态逻辑技术的形式化分析方法, 是安全协议分析的里程碑. 其因简单、直观、便于掌握使用的特点得到了广泛的应用. BAN 逻辑是基于信仰的形式化分析方法, 具有 7 类 19 条推理规则, 通过协议过程中消息的接收和发送的事实, 来判断协议的主体的最终信仰是否与预期结果相符.

在应用过程中, 人们也发现了 BAN 逻辑中存在的缺陷, 包括协议理想化过程不规范、协议的初始化假设不合理、缺乏完备性、缺乏一个定义良好明确的语义等问题. 为了解决这些问题, 基于 BAN 逻辑的类 BAN 逻辑也相继提出.

2.2 GNY 逻辑

GNY 逻辑[13]是第一个对 BAN 逻辑进行扩展的类 BAN 逻辑, 其各种规则总共合计 44 条. GNY 逻辑试图消除对主体诚实的假设、消息源假设和可识别假设, 具体从下面六个方面对 BAN 逻辑进行改进: 推广了逻辑分析应用范围、增强逻辑分析能力、对形式化协议时的明文进行保留、增加了“拥有”集合、引入“可识别”的概念以及引入“不是由此首发”的概念.

GNY 逻辑试图针对 BAN 逻辑的不足进行修正, 但是效果并不明显. 同时, 由于其本身过于复杂, 许多学者认为 GNY 逻辑在实际应用中行不通. 但是 GNY 逻辑为 BAN 逻辑的改进指明了方向.

2.3 AT 逻辑

AT 逻辑[14]在 BAN 逻辑提出不久后出现. AT 逻辑首次提出了逻辑系统的语义模型, 使表达能力更强. AT 逻辑从语义角度出发, 改进了 BAN 逻辑, 同时给出了形式化语义, 并证明了其推理的合理性. AT 逻辑对 BAN 逻辑的改进具体包括四个方面: 从语义角度分析修改了 BAN 逻辑, 整理了 BAN 逻辑的推理规则, 除去了语义和实现细节混合的部分、对一部分逻辑构件使用了更加直接的定义、引进了全部命题连接词, 将推理规则改写成公式, 简化了推理规则以及给出了形式化语义, 并证明了推理系统的合理性.

相比 BAN 逻辑, AT 逻辑更接近传统的模态逻辑, 包含详细的计算模型和模型语义, 极大地推动了 BAN 逻辑的发展. 但同时, AT 逻辑也有不足之处, 比如未能提供基于公钥体系的分析方案, 以及个别公理存在一定缺陷等问题.

2.4 SVO 逻辑

SVO 逻辑[16]是 Syverson 和 Van Oorschot 综合了 BAN 逻辑、GNY 逻辑、AT 逻辑和 VO 逻辑的优点提出的, 它为逻辑系统建立了合理的理论模型, 并在形式化语义方面对 AT 逻辑进行了重新定义. 其主要特点体现在四个方面: 提出了较为清晰的模态理论语义、消除了逻辑形式化表述和推理规则方面可能引发的模糊问题、具有极好的扩展能力以及简单实用的特点.

SVO 逻辑的提出, 标志着类 BAN 逻辑的成熟.

2.5 Kailar 逻辑

Kailar[19]逻辑是针对电子商务中的不可否认性和可追究性等安全属性而提出的. BAN 逻辑和类 BAN 逻辑无法解决主体向第三方证明另一方对某个动作或对象的发起有责任的问题, 而 Kailar 逻辑恰好可以解决这类问题.

2.6 Bieber 逻辑

BAN 逻辑和类 BAN 逻辑都是基于主体信仰的. 其最主要的一个问题是该信仰有可能是错误的, 但是

其本人并不知道该信仰是错误的. 针对这个问题, P. Bieber 基于 CKT5, 提出了基于知识的安全协议分析逻辑[24](Bieber 逻辑). 该逻辑主要的运行模式为不确定性通信模式, 即协议消息不会丢失, 但是协议消息的发送方和接收方的身份是不确定的.

2.7 非单调逻辑

之前提到的逻辑分析方法都是针对知识和信仰的单调推理函数, 一旦主体获得了某些知识或者拥有了某些信仰之后, 其永远知道或信仰这些事情. 显然, 这种条件在某些场合下显然是不适用的. 为此, Rubin 博士提出非单调逻辑分析方法[25]来解决这一问题. 该方法具有四个主要特点: 是首个能解决非单调地推理安全协议知识方法、无需理想化假设、分析过程和形式化描述紧密结合以及形式化描述非常接近协议的实现过程.

3 模型检测技术

模型检测技术的基本思路是根据有限状态机理论, 通过定义状态集和状态迁移函数为安全协议系统建立模型, 通过穷尽所有空间状态来判断某些特殊状态是否可达, 或者是否可以生成一条特殊的状态转移路径, 来判断是否可以达到安全期望. 模型检测技术一般将安全协议看作是一个分布式系统, 并为该系统定义安全属性或不变关系. 在分析过程中, 通过判断安全状态或不变关系是否能得到满足来判断安全目标是否能够得到实现. 模型检测方法具有高度自动化、可以针对漏洞自动生成攻击实例的特点, 在形式化分析领域取得了很大的成功[2,3].

3.1 Dolev-Yao 模型

Dolev-Yao 模型对模型检测技术有着重要的影响, 各种模型检测技术都是基于 Dolev-Yao 模型提出的. 在 Dolev-Yao 模型中, 分别刻画了密码系统模型和攻击者模型. 攻击者的能力包括: 熟悉加解密算法、知道参与协议的实体及其公钥、拥有自己的加解密密钥、对网络有完全控制能力、可以用其拥有的密钥进行加解密操作、可以插入新消息、可以重放任何消息、可以生成随机数.

Dolev-Yao 模型也存在部分缺点, 如无法针对安全漏洞进行分析, 以及将攻击者能力设定过强导致的拒绝服务攻击使得电子商务协议的匿名性无法得到保证.

3.2 通信顺序进程方法

在通信顺序进程(communicating sequential processes, CSP)方法[17]中, 协议的参与者被解释成 CSP 的进程, 消息被解释成事件, 协议被解释成 CSP 进程的集合. 这些进程并行运行, 并且在运行过程中与它们的环境进行交互. 对安全协议的验证就是从协议说明中抽取一个模型, 然后使用故障发散提炼(failures divergence refinement, FDR)来检测协议是否存在问题.

3.3 NRL 协议分析器

NRL 协议分析器是基于 Dolev-Yao 模型的术语重写模型开发的. NRL 协议分析器模型与 Dolev-Yao 模型的区别在于 Dolev-Yao 模型将协议看作是产生“词”的机器, 而在 NRL 模型中, 是产生“词”、“信仰”和“时间”的机器. NRL 协议分析模型中, 每个参与的主体都有一个信仰集, 而信仰是随着消息的接收或产生而发生变化的; 而消息又是由词构成, 其发送取决于主体的信仰和主体接收到的消息; 时间则代表了词的产生或信仰的修改等状态转换过程. 因此攻击者可以利用协议的执行来产生词、信仰和事件等.

3.4 Murφ 模型检测技术

Murφ 模型检测技术最初应用于工业协议的验证. 随后受 FDR 等协议分析工具在 CSP 中应用的启发, 也尝试将 Murφ 模型检测技术应用于安全协议分析领域, 并取得了成功. Murφ 描述语言是一种描述有限状

态异步并发系统的高级程序编程语言, Murφ编译器则将协议描述生成一个用于验证协议属性的验证器, 由验证器通过状态枚举来自动检查是否所有的状态都能够满足规定的属性. 其中, 状态枚举算法已经支持深度优先和广度优先算法, 并将已达状态存储于状态列表中避免重复访问, 提高了效率.

3.5 Brutus 模型检测技术

Brutus 模型检测技术采用自己的数学模型对密码协议进行建模, 基于一阶逻辑描述协议的安全属性, 并采用状态空间搜索和自然推理相结合的方法, 完成对安全属性的验证. 在进行状态空间搜索过程中, Brutus 采用了两种状态缩减技术: 偏序状态缩减技术和对称状态缩减技术.

4 定理证明技术

定理证明试图将模态逻辑技术的简洁性和模型检测技术的彻底性结合起来, 避免模态逻辑中不明确不完善和模型检测中的空间爆炸问题. 其将协议的证明规约到证明一些循环不变式中, 与证明程序正确性的过程一样[2,3].

4.1 Paulson 归纳法

Paulson 归纳法[22]将安全协议形式化成所有可能的“迹”的集合, 而“迹”是安全协议的通信事件. Paulson 协议模型中包含攻击者及消息丢失等情况, 因此在协议执行过程中, 主体并不知道消息真正的发送者, 并且可能会转发一些其并不知道内容的消息. 对于攻击者来说, 当其获取一些私钥时, 可以对消息进行加解密、伪造等. 因此, 攻击者可以是“主动攻击者”. Paulson 归纳法利用定理 Isabelle 证明器, 在迹上通过归纳的方法来证明协议的安全属性.

4.2 Schneider 阶函数

因安全协议的合法主体与恶意攻击者的共存, 并且协议中可以有意想不到的信息交互, 这使得即使在完美的密码体系假设下, 安全协议也可能存在漏洞. 协议安全性分析的目的在于找出可能存在的漏洞, 或者证明攻击是不可能发生的. Schneider 提出了阶函数[26]来验证恶意环境下的协议特性. 阶函数对系统中所有可能的消息赋值, 结果用作消息的可循环不变式, 并运用不变式技术对协议的安全性进行证明.

4.3 串空间

串空间模型理论[23]将协议运行的各个状态和整体的过程转化为集合和有向图的形式进行描述, 并利用协议运行的特性定义集合中各个状态间的偏序关系, 通过对集合中最小元的定义和证明来判断是否存在攻击节点. 相对于其他形式化方法往往存在的晦涩复杂和使用受限等问题, 串空间的设计非常巧妙和简洁. 串空间具有许多优点, 包括对某些数据项的属性给出了明确的语义; 允许精确陈述和验证各种正确概念、可以用图示方法辅助分析证明显得简洁直观等. 串空间模型中的证明要依据详细的协议行为, 因此相比基于信仰逻辑类证明更具有可信性.

4.4 重写逼近法

不同于之前的形式化分析发现对协议中存在被攻击的可能, 重写逼近法[27]对于安全协议的分析是证明一个更困难的问题: 安全协议不存在任何攻击. 重写逼近法的基本证明过程时首先将安全协议表示为一项重写系统, 将初始通信集描述为树状自动机, 然后通过极度逼近可达项集合来自动计算消息集的超集, 最后对机密性等安全属性的证明就可以通过自动证明逼近集合与相应的违禁集合的交集是空集来实现. 树状自动机模型包括无限的主体、无限的交互会话以及一个功能强大的攻击者描述.

4.5 不变式产生技术

归纳推理是安全协议自动化验证领域中的一项重要技术. 在协议并行执行, 同时攻击者可以任意操作

数据的环境下, 怎样基于无限的消息集合进行归纳推理是研究的重点. 一般可以通过构造一个不受协议主体行为影响的不变式来实现这一点[24]. 采用这种不变式产生技术的协议分析方法包括 NRL 分析器使用的语言、Schneider 的阶函数、串空间的理想等. 这些技术的共同点是采用消息集合对其进行描述, 该消息集合的某些属性不随协议合法参与者或者攻击者的行为变化而变化. 这种属性分为两大类, 一类刻画攻击者不可知的项, 或只能在特定条件下获知的项; 另一类刻画攻击者可以获知的项.

5 复合协议模型

由于新设计的安全协议往往存在着许多漏洞, 在新设计的协议提出后, 人们需要重新进行安全性分析及改进, 加重了安全协议形式化分析的工作量. 因此, 如何高效的利用现有的安全协议, 将现有安全协议进行复合, 产生新的安全协议也成了研究的热点. 复合协议的研究重点在于假设两个协议可以合成一个新的协议, 如果这两个协议是安全的, 那么在何种条件下新的协议也是安全的.

5.1 扩展串空间

Fabrege 等人通过扩展串空间理论[28], 提出协议可复合的充分条件, 即若共享相同网络及密钥结构的协议满足特定的条件, 如充分不同的消息结构, 则子安全属性的可复合性是可以保证的. 然而很多标准协议并不满足这些充分条件, 且只能验证并行复合协议, 不能验证顺序复合协议.

5.2 HT 模型

HT 模型[29]是 Heintze 和 Tygar 提出的推证安全协议的基础, 采用了基于模型的定义协议安全性质的方法. 不同于扩展串空间的思想, 协议复合逻辑的基本思想是, 若安全的协议相互不违反对方的协议不变式, 则复合后仍是安全的, 不仅可以验证并行复合协议, 还可以验证顺序复合协议. 其最主要的特点是对协议的合成. HT 模型定义了什么会发生, 因此, 协议安全性的研究变为了是否会发生不好的行为. 通信的主体处于分布式网络环境中, 在公共信道上发送和接收消息. 主体内部状态决定了他们的行为. 一些主体不依据状态执行, 而另一些主体可能会部分诚实. 协议被视为主体可能采取行为的一个约束. 每个主体与一个将当前状态映射至下一状态的函数相关联. 协议复合逻辑已用于现实生活中复合协议的验证, 但由于证明过程主观, 其至今仍未实现自动化.

6 安全协议形式化分析的前景与挑战

随着计算机网络的发展, 人们对于网络服务的各种需求也发生了变化. 因此, 对于安全协议的要求也产生了不同的需求, 也成为了目前形式化分析今后的研究方向. 这些包括:

(1) 新的威胁和新的需求

新的威胁来自于拒绝服务(denial of service, DoS)攻击. DoS 攻击的目标是消耗服务器资源, 包括连接数量和计算能力等. 对于这类攻击, 目前的安全协议都无法抵抗. 认证可以确定用户的身份, 对某些 DoS 攻击有一定的抵抗效果; 但同时认证过程也是 DoS 攻击的一种手段, 通过消耗认证资源达到 DoS 的目的.

新的需求包括匿名通信等. 随着电子商务的发展, 对匿名通信的需求也变得紧迫. 匿名协议依赖于混淆区分请求来源与去向的消息流量, 并且在匿名通信中, 网络节点的个数会很多. 因此, 目前的安全协议形式化分析技术没有对匿名通信的情况进行分析, 而且基本都无法直接使用.

(2) 安全协议自动设计研究

目前所有的形式化分析都是针对已给出的安全协议来分析其安全性, 然而如何实现安全协议的自动化设计并没有成为研究的重点. 许多形式化分析中的安全条件为自动化设计提供了基础, 可以依据需求以及形式化分析中, 该需求对应的安全条件来设计安全协议, 并在设计完成之后进行形式化分析, 验证它的

安全性.

(3) 融合计算流派和逻辑流派的形式化分析

计算流派包括随机预言机模型等, 其主要思路是将攻击难度归结于数学的概率; 逻辑流派包括串空间等, 结合给定的定理进行推理证明. 在两大流派的研究方向中提出了各种形式化分析方法, 但是对于结合两大流派优点的形式化分析方法却并没有提出. 因此, 设计一种融合了两大流派优点形式化方法也成为形式化分析的未来发展方向之一.

References

[1] Feng D G, Fan H. Survey on theories and methods of formal analyses for security protocols[J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2003, 20(4): 389–406.
冯登国, 范红. 安全协议形式化分析理论与方法研究综述[J]. 中国科学院研究生院学报, 2003, 20(4): 389–406.

[2] 王亚弟, 束妮娜, 韩继红, 等. 密码协议形式化分析[M]. 北京: 机械工业出版社, 2006: 38, 91, 112.

[3] 李建华, 张爱新, 薛质, 等. 网络安全协议的形式化分析与验证[M]. 北京: 机械工业出版社, 2010: 19, 58, 93.

[4] Needham R M, Schroeder M D. Using encryption for authentication in large networks of computers[J]. Communications of the ACM, 1978, 21(12): 993–999.

[5] Dolev D, Yao A C. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198–208.

[6] Dolev D, Even S, Karp R M. On the security of ping-pong protocols[J]. Information and Control, 1982, 55(1): 57–68.

[7] Nieh B B, Tavares S E. Modelling and analyzing cryptographic protocols using Petri Nets[C]. In: Advances in Cryptology—AUSCRYPT '92. Springer Berlin Heidelberg, 1993: 275–295.

[8] Millen J K, Clark S C, Freedman S B. The interrogator: protocol security analysis[J]. IEEE Transactions on Software Engineering, 1987 (2): 274–288.

[9] Longley D, Rigby S. An automatic search for security flaws in key management schemes[J]. Computers & Security, 1992, 11(1): 75–89.

[10] Meadows C. A model of computation for the NRL protocol analyzer[C]. In: Proceedings of Computer Security Foundations Workshop VII, 1994. CSFW 7. IEEE, 1994: 84–89.

[11] Meadows C. Analysis of the internet key exchange protocol using the NRL protocol analyzer[C]. In: Proceedings of the 1999 IEEE Symposium on Security and Privacy. IEEE, 1999: 216–231.

[12] Burrows M, Abadi M, Needham R M. A logic of authentication[J]. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 1989, 426(1871): 233–271.

[13] Gong L, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols[C]. In: Proceedings of 1990 IEEE Computer Society Symposium on Research in Security and Privacy. IEEE, 1990: 234–248.

[14] Abadi M, Tuttle M R. A semantics for a logic of authentication[C]. In: Proceedings of the 10th Annual ACM Symposium on Principles of Distributed Computing. ACM, 1991: 201–216.

[15] van Oorschot P. Extending cryptographic logics of belief to key agreement protocols[C]. In: Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, 1993: 232–243.

[16] Syverson P F, Van Oorschot P C. A unified cryptographic protocol logic[R]. Washington D. C.: Naval research lab, 1996.

[17] Lowe G, Roscoe B. Using CSP to detect errors in the TMN protocol[J]. IEEE Transactions on Software Engineering, 1997, 23(10): 659–669.

[18] Kemmerer R, Meadows C, Millen J. Three systems for cryptographic protocol analysis[J]. Journal of Cryptology, 1994, 7(2): 79–130.

[19] Dutertre B, Schneider S. Using a PVS embedding of CSP to verify authentication protocols[M]. In: Theorem Proving in Higher Order Logics. Springer Berlin Heidelberg, 1997: 121–136.

[20] Brackin S. A HOL formalization of CAPSL semantics[C]. In: Proceedings of the 21st National Conference on Information Systems Security. IEEE, 1998.

[21] Bella G, Paulson L C. Using Isabelle to prove properties of the Kerberos authentication system[C]. In: DIMACS Workshop on Design and Formal Verification of Security Protocols. 1997.

[22] Paulson L C. The inductive approach to verifying cryptographic protocols[J]. Journal of Computer Security, 1998, 6(1): 85–128.

[23] Thayer Fabrega F J, Herzog J C, Guttman J D. Strand spaces: Why is a security protocol correct?[C]. In: Proceedings of 1998 IEEE Symposium on Security and Privacy. IEEE, 1998: 160–171.

[24] Clarke E M, Grumberg O, Peled D. Model Checking[M]. MIT press, 1999.

[25] Moore R C. Semantical considerations on nonmonotonic logic[J]. Artificial Intelligence, 1985, 25(1): 75–94.

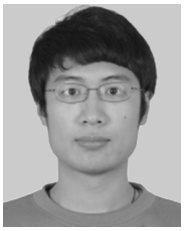
[26] Schneider S. Using CSP for Protocol Analysis: the Needham-Schroeder Public-key Protocol[M]. University of London, Royal Holloway, Department of Computer Science, 1996.

[27] Boichut Y, Genet T, Jensen T, et al. Rewriting approximations for fast prototyping of static analyzers[M]. In: Term Rewriting and Applications. Springer Berlin Heidelberg, 2007: 48–62.

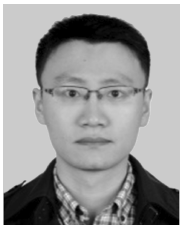
[28] Thayer Fabrega F J, Herzog J C, Guttman J D. Mixed strand spaces[C]. In: Proceedings of the 12th IEEE Computer Security Foundations Workshop. IEEE, 1999: 72–82.

[29] Datta A, Derek A, Mitchell J C, et al. Protocol composition logic (PCL)[J]. Electronic Notes in Theoretical Computer Science, 2007, 172: 311–358.

作者信息



高尚(1989–), 安徽无为人, 工学硕士. 主要研究领域为信息安全, 网络安全.
E-mail: goldensaintgao@gmail.com



石乐(1989–), 湖南长沙人, 工学博士. 主要研究领域为信息安全.
E-mail: happystone.sl@gmail.com

胡爱群(1965–), 江苏如皋人, 工学博士, 教授, 博导. 主要研究领域为信息安全.
E-mail: aqhu@seu.edu.cn

陈先棒(1990–), 浙江温州人, 工学硕士. 主要研究领域为信息安全.
E-mail: chenxianbang90@gmail.com