

河南省计算机学会
组编

计算机研究 新进展



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

计算机研究 新进展

清华大学出版社

河南省计算机学会 2006 年学术年会论文集

计算机研究新进展

河南省计算机学会 组编

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

计算机研究新进展 / 河南省计算机学会组编. —北京: 电子工业出版社, 2006.12

ISBN 7-121-03569-3

I. 计… II. 河… III. 电子计算机—文集 IV. TP3-53

中国版本图书馆 CIP 数据核字 (2006) 第 143369 号

责任编辑: 张 旭

印 刷: 北京季蜂印刷有限公司

装 订: 北京季蜂印刷有限公司

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本: 850×1168 1/16 印张: 20 字数: 660 千字

印 次: 2006 年 12 月第 1 次印刷

定 价: 48.00 元

凡所购买电子工业出版社图书有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系电话:
(010) 68279077; 邮购电话: (010) 88254888。

质量投诉请发邮件至 zlts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热: (010) 88258888。

序

忆往昔峥嵘岁月稠。河南省计算机学会自1987年5月成立以来,已走过了19年的历程。19年来发展道路坎坷不平,但学会团结全体会员和广大的计算机科技工作者,为使计算机科学技术在我省的经济建设、科技发展以及各项事业的发展中发挥更大的作用做出了应有的贡献。

长江后浪推前浪,奔腾到海不停息。河南省计算机学会2005年进行了换届选举,成立了第四届理事会。第四届理事会成员朝气蓬勃,勇于开拓创新,上任以来,积极树立经营学会的理念,为构筑“三主一家”(即学会要作为河南省计算机学术交流的主渠道,科学普及的主战场,国内外民间学术交流的主要代表,成为会员之家)做了大量的工作。本次学术年会是河南省计算机学会第四届理事会组织的第一次全省计算机科学与技术的学术会议,为大会会员进行学术交流搭建了一个宽广的平台。我衷心祝贺会议的胜利召开,特别是对本次会议学术论文集的出版感到由衷的高兴。在这里要特别感谢电子工业出版社对我们河南省计算机学会的大力支持和鼎力相助!

计算机科学技术的迅猛发展,已充分显示了其与社会发展与人类进步中的巨大作用,实现全面信息化已成为当今世界经济与社会发展的必然趋势。为更好地促进计算机科学领域的学术交流,学会将为广大会员和计算机科技工作者提供更多更好的服务,使学会成为会员之家。

令人欣喜的是本次会议选录出版的学术论文涉及的领域之广、选题之新、水平之高都是前所未有的。这些不仅反映了是作者在自己从事的领域刻苦钻研,用汗水浇灌的结果,而且也充分表明我省广大计算机科技工作者近年来在计算机科学技术的开发、工程和应用等方面都做出了很大的成绩,硕果累累,值得称赞。

雄关漫道真如铁,而今迈步从头越。让我们携起手来,为缩小与先进省市计算机科学技术水平的差距而努力!为使计算机科学技术在我省的经济建设和各项事业的发展中做出更大的贡献而努力。

祝本次年会圆满成功!

河南省计算机学会名誉理事长 苏锦祥

2006年11月16日

前 言

河南省计算机学会第四届理事会自 2005 年 7 月成立以来,以全新的姿态朝气蓬勃地开展着各项工作,努力贯彻学会的办会宗旨,团结和组织河南省计算机科技工作者以经济建设为中心,坚持科学技术是第一生产力的思想,实施科教兴豫和可持续发展战略,促进计算机科技的繁荣和发展,促进计算机科技的普及和推广,促进计算机科技人才的成长和提高,致力于“三主一家”的建设,积极打造学术交流的平台,为广大计算机科技工作者服务。

2006 年 8 月 19 日,在河南省计算机学会常务理事工作会议上,通过了年底前召开 2006 学术年会的决定。自此学会紧锣密鼓地开始了会议征文等筹备工作。截至 11 月 5 日,会务组共收到论文 80 余篇。经组织专家评审后选定了 64 篇,收录到本论文集中。此次收录的论文,大多是来自于高校的教师,也有不少是在校研究生所写。论文涉及面广,立意新颖,有较强的学术交流性。

河南省计算机学会 2006 学术年会是河南省计算机学会第四届理事会成立以来的第一次学术会议,也是几年来河南省计算机领域难得的一次盛会,是老友新朋齐相聚、相互交流谋发展的促进会,是一次推进新技术发展的展示会,是河南省计算机科学技术水平的检阅会,是促进会员之间友好交流的联谊会。学会真诚地欢迎广大计算机科技工作者及各高校、企事业的领导积极参加,进行学术交流,为推进河南省计算机技术的发展共同努力。学会网址: <http://www.hnpcs.com>。

本论文集能够正式出版,我们要感谢为论文审稿、修改的专家学者们,同时也由衷地感谢电子工业出版社的友好支持和大力帮助。

河南省计算机学会
2006 年 11 月 16 日

目 录

研 究 型

Andrew RPC 协议的两种形式化方法的比较	1
A Comparison Between Two Formal Analysis Methods on Andrew Secure RPC Protocol	
赵 琳 赵东明 周清雷	
IPv6 组网中实现隧道代理的研究	6
Research on Implementation of Tunnel Broker in IPv6 Networking	
谢 辉	
Peer-to-Peer 网络模型研究及应用	11
Research of Peer-to-Peer Network Architecture and Application	
孙智军 庄 雷	
Risks Versus Intendence Policies to Information Systems Engineering in China	16
Liu Yong, Fang Deying, Guo Gencheng	
笔迹鉴别中去噪算法的研究	22
The Noise-exenterating Research On Computer Handwriting Identification	
郭小波 曲宏山 刘永平	
冲突事件中不确定性时间知识的表示和推理	25
Uncertain Temporal Knowledge Representation and Reasoning of Conflict Events	
马军霞 叶阳东	
电子商务推荐系统中推荐方法研究	30
On Study of the Recommending Methods Based on Web Usage Mining Used in E-commerce Recommendation System	
景 丽 陈广宇	
公式时钟自动机: 一种新的形式化验证工具	35
Formula-Clock Automata: A New Tool of Formalized Verification	
杨一峰 李琳娜 赵东明	
虹膜识别系统的研究	39
Research of Iris Recognition System	
明 兰 顾晓丰	
定位目标的模型及算法	43
Model and Algorithm of Locating Target	
刘春红 石虎山 裘雪红	
基于 VLBP 神经网络的管理信息系统研究	47
Research on Management Information System Based on VLBP Neural Network	
史霄波 王亚丽	

基于无线传感器网络的路由协议研究	51
Research of routing protocol for Wireless Sensor Networks	
夏 静 庄 雷 白 雨	
CPCAR 基于正相关关联规则的分类	55
CPCAR: Classification Based on Positively Correlated Association Rules	
李睿楠 王春凯 范 明	
集群环境下并行聚类算法的研究与分析	60
Research and Analysis of Parallel Clustering Algorithm for Cluster System	
宋 伟 宋 玉	
穷举口令破解过程中的缩水技术研究	65
Research on A ShrinkTechnology on Brute Force Policy	
刘 旭 常 艳	
Web 智能信息检索技术研究	70
Researches on Intelligent Information Retrieval on Web	
宋晓莉 白秀玲	
特征语义扩展在文本分类中的应用	74
Semantic Extension of Feature in Text Categorization	
郝丽萍 替红英 范 明	
无线传感器网络 MAC 协议分析	79
Analysis of Wireless sensor network MAC protocol	
白 雨 夏 静 庄 雷	
一种分布式人机交互界面资源调度模型	83
A Scheduling Model of Human-computer Interactive Interface Resourcein Distributed System	
张明川 孙长嵩	
一种基于内容的 XML 文档访问控制模型	89
A Content-Based Access Control Model for XML Document	
王维林 张来顺	
一种有效的 XML 树模式查询优化算法	95
An Efficient Algorithm of XML Tree Pattern Query Optimization	
李九英 张来顺	
移动 IP 的安全性研究	99
The research of mobile IP security	
张 蕾 苏锦海 张永福	
一种新的基于决策熵的决策表约简方法	105
New Reduction Method Based on Decision Information Entropy in Decision Table	
孙 林 徐久成 马媛媛	

缓冲区溢出漏洞检测模型研究	110
Buffer overflow vulnerability detection model research	
	胡定文 吴 灏
基于 SSE 的分裂基算法	114
Split-Radix algorithm based on SSE	
	张昆帆 裴喜龙 王天鹏 程 翥
基于代码安全的防护技术研究	118
Research on Protection Technology based on Code Secure	
	郭卫兴 刘 旭 吴 灏
基于 IB 理论的连续优化算法	125
Sequential Optimization Algorithm Based on Information Bottleneck Theory	
	张 洁 叶阳东

设 计 型

操作系统内核模块加载控制系统设计	132
Design of Kernel Module Loading ControlSystem for Operating System	
	易 宇 王亚琪 吴 灏
基于.NET 的交互式网络教学平台设计	139
Design of Interactive Network Education Platform on .NET	
	杨 华
基于 802.11i 的 WLAN 漫游解决方案	142
A Roaming Scheme for WLAN based on 802.11i Protocol	
	程 立 张浩军
基于 DOM 和 Script 的网络图形交互研究	145
Alternation Research of WebMap Based on Dom and Script	
	和万礼 吴芬芬
基于 LonWorks 的智能网络测控系统设计	149
The design of measurement and controlling system based on LonWorks	
	赵俊锋 孙新德
基于中间件技术的并行编程环境的设计与实现	155
Design and Implementation of a Middleware-based parallel programming Environment	
	周 蓓 王 磊 任 涛 黄永忠
民主评议信息处理系统的设计与实现	161
The design and implementation of information dealing system on democratic evaluation	
	李小鹏 李亚敏 李 中 吴 果

电子教案的结构设计与制作	165
The Structure and Design of Teaching Presentations	钱晓捷 杨镇江
嵌入式 GIS 中间件平台体系结构设计	168
The Architecture Design of Embedded GIS Middleware Studio	李 婧 胡泽明
容忍入侵的自适应安全通信系统模型与设计	172
A Novel and Intrusion-Tolerant Approach to Adaptive Secure Communication	郭渊博 韦大伟 王亚弟
用于《计算机网络》教学的协议分析器设计	178
Design of a Protocol Analysis Used for Computer Network Teaching	潘宇科 穆玲玲 刘晓艳
虚拟教研室实现研究	182
Study on the Implement to Virtual Teaching and Research Section	张永强
一种基于 TCP 封装的 IPsec 和 NAT 协同方案	186
A Solution to Compatibility between IPsec and NAT Based on TCP Encapsulation	曹利峰 杜学绘 陈性元
一种基于图的分布式系统脆弱性评估模型的设计	191
Design of a graph-based model for evaluating the vulnerability of distributed system	廖 凯 张来顺 郭渊博
构建安全的电子商务应用程序	196
Building security electron business application program	赵传慧
助学贷款信息管理系统的研究与设计	201
Research and Design of the Government Education Aid Loan Information System	杨战胜 崔志恒
基于 .Net 平台的 Office 技能考试系统的 设计和实现	205
The Design and implement of Technical Test System for Office based on .Net	张聪品 张笑冬 徐久成

综 述 型

OTA 消息 PUSH 技术研究	211
Research on Push Technology of OTA Message	郭 节 张永强
FAT32 文件系统的数据恢复技术研究及应用	214
Data Recovery Technology and Applications Based on FAT32 File System	刘 旭 常 艳
管理信息系统中用户权限管理的实现	221
The Implementation Of User Rights ManagementIn Management Information System	丁 锐
基于 BP 神经网络的棉花销售市场智能分析	224
Based on BP neural network cotton vendition market intelligent analyzing	王利红
机器人定位信号的集中处理设计	227
The Design of integrated processing of Robot's location signal	李泉溪 郭海儒 李鸿征
地区集控自动化系统的设计与实现	230
The design and implement of area centralizing control automatic system	张海中 付晋卫 马 安
超市进销存管理系统的设计与实现	236
Design and implement of supermarket's MIS	吕俊亚
基于 web 信息系统的 IWSS	239
Web-based Information System——IWSS	李 芳 邓大治
基于数字水印的多媒体版权保护管理系统	244
According to the multi-media copyright protection management system of the digital watermarking	马书群
基于 H.264 的嵌入式网络视频服务器	249
The Embedded Network Video Server based on H.264	张晓健 李 伟 张小雨 瞿宏伟
MIS 系统通用界面设计的快速开发方法	253
Research on the Fast Development Methods of General Editor Based on MIS	李冠峰 王红艺

VoIP 解决方案的研究	258
Study about the account for VoIP	
	穆维新 方向前
大规模网络拓扑发现研究综述	262
A summarize on large-scale network topology discovery	
	王清贤 寇晓蕊 罗军勇 王 慧 李 响
计算机网络安全综述	271
Summary of Computer Network Security	
	牛丹梅 王少锋
基于 LM-BP 网络模型的中国能耗短期预测	276
The short-term prediction of the energy consumption in China achieved through LM_BP neural network	
	郭海如 崔雪梅 李海青
计算机犯罪中电子证据的提取和固定	281
Collecting and Solidifying Electronic Evidence In The Cyber Crime	
	王翠玲 刘 磊
高校计算机专业教学中对“三结合”实践教学法的探讨与研究	286
A Research OF According to " THREE IN ONE" Teaching Method of Computer Professional Teaching in University	
	杨春蕾 王红艺
可信计算技术研究	290
Research on Trusted Computing	
	刘胜利 祝跃飞 王清贤
入侵防护系统浅析	297
Analysis of Intrusion Prevention System	
	杨振会, 谢立清
图像信息隐写技术研究进展	300
Image Steganography Technique - State of the Art	
	王清贤, 马付恩, 罗向阳
河南省计算机学会介绍	307

Andrew RPC 协议的两种形式化方法的比较

赵琳, 赵东明, 周清雷

(郑州大学信息工程学院, 河南 郑州 450052)

摘要: 本文主要介绍了 BAN 逻辑和串空间模型这两种有效的分析认证协议的形式化方法, 并且以 Andrew secure RPC 协议为例, 说明了两种方法的不同特点。

关键词: BAN 逻辑; 串空间模型; Andrew secure RPC 协议

A Comparison Between Two Formal Analysis Methods on Andrew Secure RPC Protocol

Zhao Lin, Zhao Dongming, Zhou Qinglei

Abstract: BAN logic and strand spaces model are two popular approaches to formal analysis for authentication protocols. In this paper, the different characteristics of the above approaches are outlined through Andrew secure RPC protocol.

Keywords: BAN logic; Strand Spaces; Andrew secure RPC protocol

1 引言

形式化方法就是用数学与逻辑的方法对系统进行描述和验证。形式化方法在协议的验证和设计方面有着广泛的应用。它采用一种正规的、标准的方法对协议进行分析, 以检查协议是否满足其安全目标, 形式化方法基于严格的数学基础, 具有精确的语法和语义, 能够检测到安全协议中的细微的漏洞。因而现在大量的研究工作集中在了形式化的方法上^[1]。

BAN 逻辑^[2]和串空间模型^[3], 是两种有效地分析认证协议的形式化方法。其中, 串空间模型是近几年兴起的一种新型方法, 它具有 BAN 逻辑所不具备的优势。

2 BAN 逻辑

2.1 BAN 逻辑简介

1989 年, Burrows, Abadi 和 Needham 率先以逻辑形式方法提出了对 Kerberos 等几个著名的协议进行了分析, 找出了其中已知和未知的漏洞。BAN 逻辑^[2]的成功极大地激发了密码研究者对安全协议形式化分析的兴趣。但它仍然存在着很大缺陷。BAN 逻辑只能分析协议的认证性质, 而不能分析协议的保密性质, 然而在现实中, 通常的密钥分配协议需要同时实现保密性和认证性两个重要目标。

其基本理论见参考文献 2。

2.2 实例

Andrew secure RPC 协议的初始协议:

(1) $A \rightarrow B: A, \{N_a\}_{k_{ab}}$; (2) $B \rightarrow A: \{N_a + 1, N_b\}_{k_{ab}}$; (3) $A \rightarrow B: \{N_b + 1\}_{k_{ab}}$; (4) $B \rightarrow A: \{k'_{ab}, N'_b\}_{k_{ab}}$ 。

其中, N_a 和 N_b 是一次随机数; N'_b 是在随后的通信中使用的初始序列号; 第 (1) 条消息 A 传送一个一次随机数和它的标识符, 在第 (2) 条消息中 B 又将其送回。如果 A 认为收到的消息正确, 那么它又回送 B 一个一次随机数。在 B 收到并检验第 (3) 条消息后, 它发送一个新的会话密钥给 A , 随机数被送回时都要加 1^[4]。

这个初始协议是不安全的。从协议的第(4)条消息可以看出,第(4)条消息是 B 发给 A 的,但是 A 收到以后,无法确认这条消息是新鲜的。第(4)条消息中不含有表明新鲜性的任何信息。也就是说,攻击者可以用以前的旧消息回放给 A ,然后冒充 B 和 A 通信。

改进后的协议:

(1) $A \rightarrow B: A, N_a$; (2) $B \rightarrow A: \{N_a, K_{ab}'\}_{k_{ab}}$; (3) $A \rightarrow B: \{N_a\}_{k_{ab}'}$; (4) $B \rightarrow A: N_b'$ 。

初始假设为:

(1) $A \models A \xleftrightarrow{k_{ab}} B$; (2) $B \models A \xleftrightarrow{k_{ab}} B$; (3) $A \models (B \sim A \xleftrightarrow{k_{ab}} B)$; (4) $B \models A \xleftrightarrow{k_{ab}} B$;
(5) $A \models \#(N_a)$; (6) $B \models \#(N_b)$; (7) $B \models \#(N_b')$ 。

对改进后的协议理想化如下:

(1) $B \rightarrow A: \{N_a, A \xleftrightarrow{k_{ab}} B\}_{k_{ab}}$; (2) $A \rightarrow B: \{A \xleftrightarrow{k_{ab}} B\}_{k_{ab}'}$ 。

证明目标为:

A believes $A \xleftrightarrow{k_{ab}} B$ 即: $A \models A \xleftrightarrow{k_{ab}} B$

B believes $A \xleftrightarrow{k_{ab}} B$ 即: $B \models A \xleftrightarrow{k_{ab}} B$

A believes B believes $A \xleftrightarrow{k_{ab}} B$ 即: $A \models B \models A \xleftrightarrow{k_{ab}} B$

B believes A believes $A \xleftrightarrow{k_{ab}} B$ 即: $B \models A \models A \xleftrightarrow{k_{ab}} B$

下面给出理想化协议的分析过程:

当 A 收到第(1)条消息时,根据消息意义规则可知: $\frac{A \models A \xleftrightarrow{k_{ab}} B, A \triangleleft \{N_a, A \xleftrightarrow{k_{ab}} B\}_{k_{ab}}}{A \models B \sim \{N_a, A \xleftrightarrow{k_{ab}} B\}}$

根据随机数验证规则: $\frac{A \models \#(N_a)}{A \models \#(N_a, A \xleftrightarrow{k_{ab}} B)}$

根据随机数验证规则: $\frac{A \models \#(A \xleftrightarrow{k_{ab}} B), A \models B \sim (A \xleftrightarrow{k_{ab}} B)}{A \models B \models (A \xleftrightarrow{k_{ab}} B)}$

当 B 收到第(2)条消息时,根据消息意义规则: $\frac{B \models (A \xleftrightarrow{k_{ab}} B), B \triangleleft \{A \xleftrightarrow{k_{ab}} B\}_{k_{ab}'}}{B \models A \sim \{A \xleftrightarrow{k_{ab}} B\}}$

根据随机数验证规则: $\frac{B \models \#(A \xleftrightarrow{k_{ab}} B), B \models A \sim \{A \xleftrightarrow{k_{ab}} B\}}{B \models A \models \{A \xleftrightarrow{k_{ab}} B\}}$

由BAN逻辑证明可知,满足了协议的需求。

3 串空间模型

3.1 串空间模型简介

1998年, Fabrega, Herzog 和 Guttman 建立了串空间模型 (strand spaces) [3], 将安全协议的形式化分析技术推向一个新的高度。串空间模型是一种结合定理证明和协议迹的混合方法, 它是一种新型有效的安全协议形式化分析方法。它可以有效地分析安全协议的机密性和认证性。

串空间模型认证协议的目标规约为认证性和机密性。当认证性和机密性都满足时, 认证协议是正确的。

串空间模型的基本理论见参考文献3。

3.2 Andrew secure RPC 协议的证明

3.2.1 一致性: 响应者的保证

命题 3-1 假设下述条件成立:

(1) Σ 是一个 RPC 空间, C 是 Σ 中的一个丛, $s \in \text{Resp}[A, B, N_a, N_b, K_{ab}, K_{ab}']$, 且 $C - \text{height}(s) = 4$;

(2) $K_{ab}^{-1} \notin K_p$;

(3) $K_{ab} \neq K'_{ab}$, 且 K'_{ab} 在 Σ 中是唯一起源的。

于是, C 中包含一个发起者串 $t \in \text{Init}[A, B, N_a, N_b, K_{ab}, K'_{ab}]$, 且 $C - \text{hight}(t) = 3$ 。

证明: 设节点 $\langle s, 2 \rangle$ 的输出值 $\{N_a, K'_{ab}\}_{k_{ab}}$ 记为 n_0 , 它的项为 v_0 。

引理 3-1 K'_{ab} 起源于 n_0 。

证明: 由假设 $K'_{ab} \subset v_0$, 且 n_0 的符号为正。因此, 只需证明 $K'_{ab} \not\subset n'$, 其中 n' 是与节点 n_0 在同一个串上的前驱节点 $\langle s, 1 \rangle$ 。

引理 3-2 可以考虑以下集合 $S = \{K'_{ab} \subset \text{term}(n) \wedge v_0 \not\subset \text{term}(n)\}$ 有一个极小元 n_2 , 节点 n_2 是正则节点且符号为正。

证明: 因为该集合不为空, 所以至少存在一个极小元。需要证明 n_2 不可能在一个攻击者串上。

① M 型, 其迹为 $\langle +t \rangle$, 其中 $t \in T$, 显然, 不可能。

② F 型, 其迹为 $\langle -t \rangle$, 其中 $t \in T$, 同样不可能。

③ T 型, 其迹为 $\langle -g, +g, +g \rangle$, 若 $K'_{ab} \subset g$, 则与 n_2 的极小性矛盾, 所以不可能。

④ K 型, 其迹为 $\langle +K \rangle$, 其中 $K \in K_p$, 显然, 不可能。

⑤ E 型, 其迹为 $\langle -K, -h, +\{h\}_k \rangle$, 则 $K'_{ab} \subset h$ 或者 $K'_{ab} = K$, 但是 $K \in K_p$, 所以 $K'_{ab} = K$ 。若 $K'_{ab} \subset h$, 则与 n_2 的极小性矛盾, 所以不可能。

⑥ D 型, 其迹为 $\langle -K^{-1}, -\{h\}_k, +h \rangle$, 若 $K'_{ab} \subset h$, 则 $K'_{ab} \subset \{h\}_k$, 那么与 n_2 的极小性矛盾, 所以不可能。

⑦ C 型, 其迹为 $\langle -g, -h, +gh \rangle$, 与 n_2 的极小性矛盾, 所以不可能。

⑧ S 型, 其迹为 $\langle -gh, +g, +h \rangle$ 。则 $\text{term}(n_2) = g$ 或者 $\text{term}(n_2) = h$ 成立, 证明类似。

若 $\text{term}(n_2) = g$, 则 $K'_{ab} \subset g$, $v_0 \not\subset g$, 由 n_2 的极小性有 $v_0 \subset gh$, 并且 $v_0 \neq gh$, 因此 $v_0 \subset h$ 。令

$T = \{m \in C : m < n_2 \wedge gh \subset \text{term}(m)\}$, 则 T 中每个元素都是攻击者节点, 因为没有正则节点包含子项 gh (其中 h 包含加密子项)。

因为 $\langle p, 1 \rangle \in T$, 所以 T 是非空集合。由串空间模型基本理论可知, T 中包含一个极小元 m 。且 m 的符号为正。下面考察 m 可能出现在什么类型的攻击者串 p' 上。

① M 型, 其迹为 $\langle +t \rangle$, 其中 $t \in T$, 不可能。

② F 型, 其迹为 $\langle -t \rangle$, 其中 $t \in T$, 不可能。

③ T 型, 其迹为 $\langle -g, +g, +g \rangle$, 不可能。

④ K 型, 其迹为 $\langle +K \rangle$, 其中 $K \in K_p$, 不可能。

⑤ E 型, 其迹为 $\langle -K, -h, +\{h\}_k \rangle$, 可推出 $gh \subset \text{term}(\langle p', 2 \rangle)$ 并且 $\langle p', 2 \rangle < m$, 所以和 m 的极小性矛盾, 因此不可能。

⑥ D 型, 其迹为 $\langle -K^{-1}, -\{h\}_k, +h \rangle$, 可推出 $gh \subset \text{term}(\langle p', 2 \rangle)$ 并且 $\langle p', 2 \rangle < m$, 所以和 m 的极小性矛盾, 因此不可能。

⑦ C 型, 其迹为 $\langle -g, -h, +gh \rangle$, 可推出 $gh = \text{term}(m)$, 而 $\text{term}(\langle p', 1 \rangle) = \text{term}(n_2)$ 且 $\langle p', 1 \rangle < n_2$, 所以和 n_2 的极小性矛盾, 因此不可能。

⑧ S 型, 其迹为 $\langle -gh, +g, +h \rangle$, 可推出 $gh \subset \text{term}(\langle p', 1 \rangle)$ 并且 $\langle p', 1 \rangle < m$, 所以和 m 的极小性矛盾, 因此不可能。

引理 3-3 存在一个串 t 上的节点 n_2 的前驱节点 n_1 , 且 $\text{term}(n_1) = \{N_a, K'_{ab}\}_{k_{ab}}$ 。

证明: 由串空间模型基本理论可知, K'_{ab} 起源于 n_0 , 且由它的假设条件可知, K'_{ab} 在 Σ 中是唯一起源的。因为 $v_0 \subset \text{term}(n_0)$, 且 $v_0 \not\subset \text{term}(n_2)$ 。所以 $n_0 \neq n_2$ 。因此, K'_{ab} 不起源于 n_2 。从而在串 t 上有一个 n_2 的前驱节点 n_1 , 使得 $K'_{ab} \subset \text{term}(n_1)$ 。由 n_2 的极小性, 有 $v_0 = \{N_a, K'_{ab}\}_{k_{ab}} \subset \text{term}(n_1)$ 。但是, 没有正则节点以一个加密项为其真子项, 因此必有 $\{N_a, K'_{ab}\}_{k_{ab}} = \text{term}(n_1)$ 。

引理 3-4 包含 n_1 和 n_2 的正则串 t 是一个从 C 中的发起者串。

证明: 节点 n_2 是一个符号为正的正则节点, 且它的前驱节点 n_1 具有形式 $\{x, k\}_k$ 。如果它是一个响应者串, 那么只能在此节点之后跟着一个符号为负的节点, 所以 t 是一个发起者串。而且, n_1 和 n_2 分别是 t 上的第二个和第三个节点, 所以 $C - \text{height}(t) = 3$ 。

命题 3-2 设 Σ 是一个 RPC 空间, 且 K_{ab}' 在 Σ 中是唯一起源的。于是, 对任意 A, B 和 K_{ab}' , 最多只存在一个串 $t \in \text{Init}[A, B, N_a, N_b, K_{ab}, K_{ab}']$ 。

证明: 因为 K_{ab}' 在 Σ 中是唯一起源的, 因此, 存在唯一的发起者串。

3.2.2 K_{ab}' 的机密性

命题 3-3 假设下述条件成立:

(1) Σ 是一个 RPC 空间, C 是 Σ 中的一个丛, $s \in \text{Resp}[A, B, N_a, N_b, K_{ab}, K_{ab}']$, 且 $C - \text{height}(s) = 4$;

(2) $K_{ab}' \notin K_p$;

(3) $K_{ab} \neq K_{ab}'$, 且 K_{ab}' 在 Σ 中是唯一起源的。

于是, 对于任意满足 $K_{ab}' \subset \text{term}(m)$ 的节点, 有 $\{N_a, K_{ab}'\}_{k_{ab}} \subset \text{term}(m)$ 成立, 或者 $\{N_a\}_{k_{ab}} \subset \text{term}(m)$ 成立。特别地, $K_{ab}' = \text{term}(m)$ 。

证明: 将节点 $\langle s, 2 \rangle$ 记为 n_0 , 它的项 $\{N_a, K_{ab}'\}_{k_{ab}}$ 记为 v_0 , 将节点 $\langle s, 3 \rangle$ 记为 n_3 , 它的项 $\{N_a\}_{k_{ab}}$ 记为 v_3 。考虑以下集合 S 是个空集, 如果 S 是一个非空集合, 那么这个集合中至少存在一个极小元。

$$S = \{n \in C : K_{ab}' \subset \text{term}(n) \wedge v_0 \not\subset \text{term}(n) \wedge v_3 \not\subset \text{term}(n)\}.$$

引理 3-5 S 的极小元不是正则节点。

证明: 反设存在一个极小元 m 是正则节点, 且 m 的符号为正。

① 假设 m 位于响应者串 s 上。

只有 $\langle s, 2 \rangle$, $\langle s, 4 \rangle$ 的符号为正, 那么根据 S 集的定义可知, m 不可能位于发起者串 s 上。

② m 也不可能位于响应者串 $s' \neq s$ 上, 否则有 $m = \langle s', 2 \rangle$ 或者 $m = \langle s', 4 \rangle$ 。

假设 $m = \langle s', 2 \rangle$, 那么可推出 K_{ab}' 起源于 $\langle s', 2 \rangle$, 和 K_{ab}' 唯一起源于 n_0 矛盾。

假设 $m = \langle s', 4 \rangle$, 不可能。

③ 假设 m 位于一个发起者串 s' 上, 则有 $m = \langle s', 1 \rangle$ 或者 $m = \langle s', 3 \rangle$ 。

假设 $m = \langle s', 1 \rangle$, 不可能。

假设 $m = \langle s', 3 \rangle$, 那么根据 S 集的定义可知, m 不可能位于发起者串 s' 上。

引理 3-6 S 的极小元不是攻击者节点。

证明: 假设 S 的极小元 m 位于攻击者串上。此引理的证明和引理 3-2 非常相似。

3.2.3 一致性: 发起者的保证

欲证明发起者的保证, 先要来看 K_{ab} 的机密性。 K_{ab} 的机密性是必然的, 是所有证明的前提, 如果 K_{ab} 泄露的话, 那么这个协议当然是不安全的。再来看 N_a 的新鲜性。 N_a 在 Σ 中是唯一起源的, 因此 N_a 是“新鲜”的。由 K_{ab} 的机密性和 N_a 的新鲜性, 协议可以就 K_{ab}' 达成一致。

但是, 我们可以从第 (1)、(4) 条消息中看出, N_a , N_b 的机密性是不满足的。根据串空间理论可知, 攻击者可以通过 S 型串来获取和发送 N_a , 通过 T 型串来获取和发送 N_b 。因此, 虽然在理想状态下, 改进后的 Andrew secure RPC 协议可以满足给客户机分发一个新的会话密钥 K_{ab}' 的要求, 但它仍然存在着安全缺陷。

因此, 系统存在着如下攻击:

1.1A $\rightarrow I(B): A, N_a$

2.1I(B) $\rightarrow A: B, N_a$

2.2A $\rightarrow I(B): \{N_a, K_{ab}'\}_{k_{ab}}$

$$1.2I(B) \rightarrow A:\{N_a, K'_{ab}\}_{k_{ab}}$$

$$1.3A \rightarrow I(B):\{N_a\}_{k_{ab}}$$

$$2.3I(B) \rightarrow A:\{N_a\}_{k_{ab}}$$

$$1.4I(B) \rightarrow A:N_i$$

$$2.4A \rightarrow I(B):N_b$$

4 结论

在 BAN 逻辑中, 首先初始假设难以确定, 而假设对于分析结论的正确与否至关重要。其次, 理想化过程因含糊度大而难以确定。理想化步骤虽然有通常的指导, 但其自身却是非形式化的, 即没有形式化的方法来探究理想化过程的有效性和正确性。此外, 由于 BAN 逻辑不能对知识进行推理, 因此, BAN 逻辑只能分析协议的认证性质, 而不能分析协议的机密性^[5]。

串空间模型是现有安全协议形式化方法中最为直观、简洁、严格和有效的方法。它的直观性表现在使用一种节点间存在因果关系的有向图来表示协议的运行。它的简洁性表现在对于小型协议完全可以使用手工的方法完成证明。它的严格性表现在它使用了节点之间的因果关系来确保证明的逻辑性和证明的正确性^[1]。

以改进后的 Andrew secure RPC 协议为例, 用 BAN 逻辑证明满足需求, 但是用串空间证明则发现了缺陷。

参考文献

- [1] 卿斯汉. 安全协议的设计和逻辑分析. 软件学报, 2003, 14(7).
- [2] Michael Burrows and Martin Abadi and Roger Needham. BAN concrete Andrew Secure RPC. Last modified November 14, 2002.
- [3] F Thayer, JC Herzog, JD Guttman. Strand spaces: Why is a security protocol correct? //Proc of 1998 IEEE Symp on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 1998.
- [4] 白汉利, 蔡红柳, 郑广. 基于形式方法的 AndrewRPC 认证协议的分析与改进. 计算机工程与设计, 2005, 26(7).
- [5] 刘锋. 安全协议模型检验技术第三章. 国防科技大学.