无线安全协议设计方法研究

顾 翔[1,2] 张 臻[1,3] 邱建林[1]

(南通大学计算机科学与技术学院 南通 226019)[1] (南京邮电大学计算机学院 南京 210003)[2]

(南京航空航天大学信息科学与技术学院 南京 210016)[3]

摘 要 探讨了无线安全协议设计的一般步骤,包括应用环境抽象、特定应用网络弱点分析、待设计安全协议要达到的目标、现有相近协议优缺点分析、具体协议设计、协议安全性证明。作为实例,按照这些步骤,设计了一个新的无线网络认证协议。实践表明,这些设计步骤操作性较强,可以较好地指导无线安全协议设计,对于其它小型应用层协议的设计也有一定的参考作用。

关键词 无线局域网,安全协议,认证协议,形式化技术,协议设计

中图法分类号 TP309 **文献标识码** A

Research on Wireless Security Protocol Design

GU Xiang[1,2] ZHANG Zhen[1,3] QIU Jian-lin[1]

(School of Computer Science and Technology, Nantong University, Nantong 226019, China)[1]

(School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[2]

(College of Information Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)[3]

Abstract Discussed general steps of a wireless security protocol design, including abstracting of application environment, analyzing weakness of application-specific network, confirming objectives of protocol to be designed, analyzing advantages and disadvantages of the existing similar protocols, designing protocol, proofing protocol security. And in accordance with these steps, a new wireless network authentication protocol was designed as an example. Practice shows that these steps could guide the designing of wireless security protocols better. They could also be used to guide the designing of some small application-layer protocols.

Keywords Wireless LAN, Security protocol, Authentication protocol, Formal technology, Protocol design

1 引言

无线局域网与有线局域网有很多不同之处,其面临的安全威胁更多于有线网络,包括信道上传输的数据所面临的威胁和网络中主机所面临的威胁。基于密码学基础的安全协议在保证通信安全方面起着至关重要的作用。尽管一些标准化组织先后发布了一批无线安全协议标准,然而在实际工作中,一些特定应用还是要求设计、实现针对性更加具体的安全协议。为此,本文就无线安全协议的一般设计方法进行了研究,在实践中摸索了一套协议设计步骤。

2 无线安全协议的设计步骤

我们总结出无线安全协议一般设计方法分为6个步骤,包括应用环境抽象、特定应用网络弱点分析、待设计安全协议要达到的目标、现有相近协议优缺点分析、具体协议设计、协议安全性证明。前面的4个步骤是基础,目的在于提高安全协议设计效率和保证协议安全性。

2.1 应用环境抽象

由于无线局域网的特点,需要根据不同的应用环境使用针对性不同的协议。一般用户部门内部有着自己的网络特点和特殊应用,因此对应用环境进行抽象是首先要做的工作。

在进行应用环境抽象时,需要考虑的问题有:

(1)应用环境中的资源分类。这里的资源是指无线局域网内的用户和各种服务器以及它们各自提供的服务。一个网络所拥有的设备很多,功能也不相同,这些机器遵循共同的规则进行资源访问。当设计一个应用于该网络的安全协议时,首先应该对资源进行分类。对于普通的无线局域网,如家庭无线局域网、小型公司,可以简单地分为通信请求者和应答者。对于一些特别的请求者或应答者,如无线传感器网中的传感器节点,由于它们自身计算能力和能源非常有限,因此在应用环境假设阶段就必须事先加以特殊考虑。不同类型的资源在网络中的角色和行为各不相同。

(2)应用环境中的密钥管理。管理密钥有很多方法,面对不同的网络有不同的选择。例如普通的小型无线局域网,通

到稿日期:2010-08-23 返修日期:2010-12-25 本文受国家自然科学基金(60773041),江苏省高校自然科学研究计划项目(08KJB520009),南通市应用研究计划项目(K2008005)资助。

顾 翔(1973-),男,博士,副教授,硕士生导师,主要研究方向为协议工程、形式化技术、无线网络安全,E-mail:gu_x@ntu_edu_cn;张 臻(1987-),男,硕士生,主要研究方向为信息安全;邱建林(1965-),男,教授,硕士生导师,主要研究方向为逻辑综合、信息安全。

过安全信道事先交换密钥是可行的。在大型企业中，通过一个统一的服务器分配密钥可以节省大量时间。

(3)攻击者模型是安全协议设计的重要组成部分。Dolev和Yao将协议本身和协议所采用的具体密码系统分开，在假定密码系统是"完善"的基础上讨论认证协议本身的正确性、安全性、冗余性等问题。他们还建立了攻击者模型，不能低估攻击者的知识和能力。在安全协议设计时，需要遵循Dolev和Yao的这些基本思想[1]。

2.2 特定应用网络的弱点分析

网络弱点分析必须立足于特定应用环境。由于网络安全级别的不同，不同网络面对着不同的攻击者。普通用户无需使用安全级别很高的协议，例如WPA2协议，该协议需要一个额外的认证服务器RADIUS，普通用户无法满足这种要求，而且在使用高级别、高复杂协议的同时，往往也带来了耗时、耗资源的问题。普通用户使用对等安全协议已经足够，对于这样的网络，密钥管理可以而且应当简化。此时，密钥管理的简单化就不应再视为网络弱点。

网络弱点分析意在通过针对网络特点分析网络易受到的攻击。必须假设攻击者具有丰富知识和强大能力。设计者应该清楚现有的常见攻击和研究潜在的攻击类型，分析现有网络容易受何种攻击。例如，并不是所有的网络都容易受到拒绝服务攻击，临时组建的无线局域网不用担心会受到拒绝服务攻击，它更容易受到身份认证类型的攻击。此外，由于无线局域网中发送数据容易受到干扰而延长接收时间。这种不平稳导致时间戳难以利用。而时间差的产生导致重放攻击更容易实施，因此无线网络环境下一般更需要着重考虑重放攻击。

2.3 待设计的安全协议要达到的目标

通过第二步的分析，找出了特定应用网络的弱点。这些弱点也正是在设计具体协议中要解决的问题，即安全协议的目标是以解决这些弱点为基础的。

安全协议的目标应该是明确可行的，无二义性。协议目标可以是认证通信主体的身份、在主体之间分配会话密钥或引入合法主体到信任域等其中的一个或多个。目标的可行性在于不能脱离实际，不能过于复杂。

不同的安全协议有不同的目标，这些目标之间的差异常常是很微妙的。协议设计者、分析者和实现者都应该明确协议所要达到的具体目标，最大限度地保证协议安全性。文献[2]中给出了一个认证协议的外部目标的描述示例。

2.4 现有相近协议优缺点分析

现有协议优缺点分析是一个重要环节。前述3个步骤并未涉及到具体协议，而这一步则是在前面的基础上寻找与应用环境和协议目标相近的现有协议，并进行分析，以资借鉴。

学习和分析现有相近协议，可以有效提高所设计协议的质量。随着网络环境的不断变化，尤其在无线局域网中，设备移动和更换频繁，曾经安全的协议在攻击者知识越来越丰富的情况下会暴露出新的缺陷。安全协议的微妙之处在于，一点很小的改动会引起本质性的变化。分析协议应该借助于形式化分析方法。非形式化方法分析协议容易出现主观臆断，得出错误结论。

通过研究现有协议，发现其可能存在的安全缺陷，研究相应的改进措施，提出新的改进方案。这一方法对WLAN技术的使用、研究和发展产生过深远影响。例如从WEP到WPA再到WPA2，就很好地说明了这一点。

2.5 具体协议设计

这一步骤开始设计安全协议。前面诸多步骤为这一环节提供了大量信息和资料，可以根据应用环境抽象分配协议主体，接着在后3步中思考协议的轮廓。弱点分析结合目标再借助已有协议的特点，可设计出一个协议初稿。

这一步骤并不要求立刻设计出一个可行且已经达到目标的协议。设计出来的协议还需要得到进一步的证明，确定是否可行。通过反复证明和修改，最终达到要求。

无线局域网的协议设计还应该考虑到网络特点。由于无线特点，消息暴露，攻击者将变得更多，协议应该有很强的抗篡改性。除了加密的信息，暴露的明文信息应该不足以被攻击者利用来破解密文。文献[2]中给出过9条安全协议设计原则，其中最重要的一点，是"永远不低估攻击者的能力"。

2.6 协议安全性证明

协议证明在协议设计过程中至关重要。即使是很简单的安全协议，光靠主观分析是很难完全发现安全缺陷的。设计者也不能只等到攻击者发现协议缺陷后再加以改进。即使是一些已经成为标准的协议，也依然存在着一些可以被攻击者利用的安全缺陷[3]。为了最大程度保证协议安全性，需要对其进行证明。在现行的安全协议证明方法中，主要有两类：第一类是靠软件模拟协议实现和攻击者；第二类是使用形式化分析方法分析协议。通常协议设计者更多使用形式化技术。

BAN逻辑为安全协议的形式化分析提供了一种有效的工具。它只在抽象层次上讨论协议安全性，并不考虑由协议实现、加密体制所带来的安全缺陷。这也正适合设计安全协议的原则。作为一种多类型模态逻辑，它曾经成功揭示出安全协议的设计缺陷。通过BAN逻辑分析，曾经发现了CCITT X.509标准推荐草案中的安全漏洞。

Rubin逻辑是另一种分析安全协议的形式化方法，它是基于信念的、非单调的推理逻辑。Bubin逻辑要求协议设计者在规范协议时明确地对协议的条件做出假设。它对协议的规范非常接近于实际的分布式系统中的协议实现。

此外，常用的安全性证明方法还有模型检测(串空间模型、SMV模型)等方法[4]。采用形式化分析方法分析安全协议，可以大大提高所设计协议的安全性。通过分析，可以有效地发现该协议的缺陷甚至冗余部分，然后继续改进和分析协议，可以设计出符合目标的协议。形式化分析方法相对于软件模拟方法，更容易实现，花费时间和资源更少。

3 设计示例：一个新的无线认证协议

设计了一个新的无线局域网认证协议，来验证前面所提出的安全协议设计步骤是可行且高效的。本协议应用于一般小型无线局域网，如家庭无线局域网、小型企业和临时组建的无线局域网，用以进行通信主体身份的认证，从而建立起安全的通信信道。

3.1 新协议的应用环境抽象

参与者：通信请求者和应答者。对小型无线局域网而言，再加入其他的设备，例如额外的证书发放服务设备，是浪费资源的。请求者和应答者均为普通用户，具备一般能力，电源足够，计算能力良好。

密钥管理：采用共享密钥认证。认证先假定每个站点都

通过一个独立于无线局域网络的安全信道，已经接收到一秘密共享密钥，这对于小型无线局域网是可行的。在协议认证后，参与者之间将使用动态密钥。

加密算法：假设加密算法是安全可靠的。

攻击者：使用 Dolev-Yao 模型，假设攻击者拥有足够的知识和能力实现网络中所有可能的攻击。

3.2 网络弱点分析

本网络是无线局域网，有如下可被攻击者利用的弱点：

(1)信道开放，无法阻止攻击者窃听、恶意修改并转发；

(2)传输介质(无线电波)在空气中的传播会因多种原因(例如障碍物)发生信号衰减，导致信息的不稳定，甚至会丢失；

(3)网络用户需要常常移动设备(尤其是移动用户)，甚至设备丢失或失窃；

(4)攻击者容易伪装成合法用户；

(5)容易受到中间人攻击、DOS 攻击。

3.3 新协议要达到的目标

新协议采用共享密钥认证。这种密钥管理假定每个站点都通过一个独立于无线局域网络的安全信道获得密钥，因此可以将这个密钥作为通信时加密密钥。为了防止攻击者非法接入和窃取到信息，认证协议需要达到的目标为：认证主体的身份，建立起安全的通信信道；交换动态密钥的组成部分，供用户今后会话使用。

鉴于无线局域网的特点和对现有协议的分析，新协议需要特别注意以下问题：

(1)应当是双向认证，以防止虚假接入。

(2)密钥应当是动态的。这样可以有效防止已知密文的攻击。密钥向量应当加密，提高安全性。

(3)认证过程简单。协议不宜过于复杂，对于小型点对点无线局域网络，复杂的认证可能导致网络流量增加，影响网络速度。冗余度低也是安全协议本身的要求。

(4)动态密钥的效果与主体间交换以后会话密钥的效果相同。

3.4 现有相近协议分析

无线网络中常用的认证协议有 Helsinki 协议、WEP 协议、WPA 协议等。

Helsinki 协议是国际标准 ISO/IEC DIS 11770-3 中提出的认证协议草案。协议有两个参与者，即协议发起者和协议响应者。协议目的是为协议主体安全地分配一个共享会话密钥。Helsinki 是不安全的，存在安全缺陷[5]，不能达到它的安全目标。攻击者可以对它实行一种内部攻击，即攻击者必须是合法的协议主体。攻击者可以通过两个回合的协议运行，使需要通讯的二位合法主体都相信已经成功地建立了通信。实际是二位主体都无法正常通信。问题出在协议的第二步，没有明确指出消息的来源，从而造成消息的重放。因此攻击者虽然不知道消息的真实内容，却可以转发给其他主体，使之相信该消息来源于攻击者。因而此协议不能满足本网络的安全需求。

WEP 协议是 802.11b 标准中一个最基本的协议，有两个参与者。数据的加密解密使用一个密钥，即采用对称加密机制。WEP 协议采用 RC4 流密码算法来加密从接入点或无线网卡发送出去的数据包。它使用初始化向量 IV，使得密钥可以动态变化，避免使用重复的密钥流，因此提高了安全性。然而 IV 以明文的形式包含在通信的数据包中，加之 IV 长度只有 3 字节，也就是最多可能有 224 个密钥。无线局域网的设备通常传输的是 1500 字节的数据包，所以大概 10M 左右的数据就出现 IV 重复。通过相同密文的对比，攻击者就有可能破解密文，得到密钥。WEP 协议采用单向认证，而不是双向认证，因此不能防止虚假接入。即接入点能鉴别用户，但是用户不能鉴别接入点。假设一个虚假接入点放在无线局域网内，它可以通过劫持合法用户的数据包进行拒绝服务攻击。因此，虽然此协议参与者少，但安全性不能满足本网络。

WPA 协议是 WEP 协议的升级版，可以与原有采用 WEP 协议的 WI-FI 产品兼容。WPA 对原有 WEP 协议的主要改进是引入了 TKIP，将 IV 的长度由 24 位加长到 48 位，并采用动态生成以及通过认证服务器来分配的多组密钥取代了 WEP 的单一静态密钥。WPA 协议由申请者、认证方和认证服务器 3 部分组成，适合大型企业公司。WPA 采用新的序号规则，防止重放攻击以及采用密钥更新机制，及时提供全新的加密密钥和完整性校验密钥，防止密钥重用带来的安全威胁。虽然 WPA 协议已经把初始化向量加长，提高了无线网络的安全性，但是增加初始化向量 IV 的长度只能在有限程度上提高破解难度，比如延长破解信息收集时间或加长暴力破解的时间，并不能从根本上解决问题。WPA 协议不适合小型无线局域网，单一的无线局域网不可能找到一台服务器作为认证服务器。

3.5 新协议设计

设计新协议的工作开始于协议主体 A、B 需要通信的时候。假设 A 是通信发起者，即请求者，B 为应答者。开始时 A 发送消息 M1 给 B；B 收到消息，处理后发送 M2 响应 A；A 收到响应 M2，验证 B 的身份，如果正确则发送消息 M3 给 B；B 收到消息 M3 后验证 A 的身份，如果正确则建立通信信道。协议工作过程如图 1 所示。

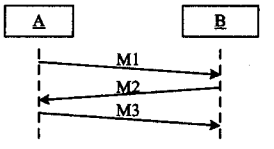

图 1 协议工作过程

新协议中相关符号说明如下：

A：请求者；B：应答者；

A_{MAC}：A 的 ID，可以是 MAC 地址或组员身份号等；

B_{MAC}：B 的 ID，可以是 MAC 地址或组员身份号等；

K_{ABM}：K_{AB}＋hash{B_{MAC}}，“＋”表示通过某种算法把 K_{AB} 和 hash{B_{MAC}}进行组合；

IV：临时密钥向量，用于与 KAB 结合生成动态密钥，并起到临时值的作用；

K_{ABIV}：K_{AB}＋IV；

SUM：数据报检验和。

协议的工作过程为：

M1：A－＞B：{ IV，A_{MAC}，SUM}K_{ABM}

M2：B－＞A：{ IV′，B_{MAC}，SUM}K_{ABIV}

M3：A－＞B：{ IV″，SUM}$K_{ABIV'}$

具体工作过程解释如下：

A 发送给 B 一个用 K_{ABM} 加密的请求报文 M1。密文包括

IV、A的自身ID(A_{MAC})和检验和。用K_{ABM}加密，可以避免IV暴露在密文之外，防止密钥容易被猜测和IV重复时被轻易知晓的威胁。无需加长密钥，也可提高密钥安全性。

B收到A的信息后，解密，检验SUM，这里既能防止篡改，又使得IV有临时新鲜性的功能，用于防止重放攻击。然后记下A_{MAC}，用IV与K_{AB}组合成动态密钥K_{ABIV}。发送M2给A，用K_{ABIV}加密。密文内容包括IV′、B的自身ID(B_{MAC})和完整性信息。IV′为新的临时密钥向量。

当A收到M2后，解密并验证临时值。如果正确，则检查B_{MAC}是否与自己要请求的应答方一致。一致则发送M3，IV″和完整性信息。

B收到M3，解密检查，正确则建立好连接。

新协议使用动态密钥。初始密钥为K_{ABM}。如果排除暴力破解密码(这是弱密钥问题，属于协议的具体实现)，针对密钥的攻击一般是使用数学工具分析密钥与密文的关系。协议中通过散列B的身份，使之与密钥组合，可以达到打乱密钥的目的，降低借助密钥进行攻击的可能性，而且可以避免攻击者使用旧消息来发动对A、B以外其他主体的重放攻击。后续密钥是交叉使用的，即A使用B提供的IV来与原密钥进行组合，而B使用A提供的IV来与原密钥进行组合。M2用于验证B的身份，M3可以用于验证A的身份，从而提供双向认证。

3.6 新协议安全性证明

下面使用BAN逻辑对新协议安全性进行证明。

建立协议的初始假设集合如下：

P1：A believes fresh(IVa)

P2：B believes fresh(IVb)

P3：B believes A controls $A \overset{IVa}{\leftrightarrow} B$

P4：A believes B controls $A \overset{IVb}{\leftrightarrow} B$

P5：A believes $A \overset{KAB}{\leftrightarrow} B$

P6：B believes $A \overset{KAB}{\leftrightarrow} B$

建立协议的理想化协议模型如下：

(1)A−>B：$\{A \overset{IVa}{\leftrightarrow} B\}K_{ABM}$ from A

(2)B−>A：$\{A \overset{IVb}{\leftrightarrow} B\}K_{ABIVa}$ from B

(3)A−>B：$\{A \overset{IVa}{\leftrightarrow} B\}K_{ABIVb}$ from A

A_{MAC}，B_{MAC}用于区分消息的来源。IV和IV′来自A。又由于IV是作为以后密钥的一部分，可以视其为密钥，记为IVa。同理，IV′记为IVb。SUM用于验证消息完整性，防止篡改，在证明中可以省略，由IVa，IVb来达到同一目的。B在M2中生成密钥，用到IVa，相当于给A发送了IVa。A在M3中生成密钥，用到IVb，相当于给B发送了IVb。K_{ABIVa}，K_{ABIVb}和K_{ABM}与K_{AB}在证明中效果相同，K_{ABIVa}，K_{ABIVb}和K_{ABM}在协议实现上密码复杂强度大于K_{AB}，即证明时使用P5和P6已经足够。

根据BAN逻辑，对协议的解释如下：

(1)B sees $\{A \overset{IVa}{\leftrightarrow} B,\}K_{ABM}$ from A

(2)A sees $\{A \overset{IVb}{\leftrightarrow} B, IVa\}K_{ABIVa}$ from B

(3)B sees $\{A \overset{IVa}{\leftrightarrow} B, IVb\}K_{ABIVb}$ from A

新协议希望达到的目标是：

B believes A believes $A \overset{IVa}{\leftrightarrow} B$

A believes B believes $A \overset{IVb}{\leftrightarrow} B$

A believes $A \overset{IVa}{\leftrightarrow} B$

B believes $A \overset{IVb}{\leftrightarrow} B$

新协议安全性证明如下：

B收到消息M1后，结合初始假设P6和消息含义规则，有：

① B believes A said($A \overset{IVa}{\leftrightarrow} B$)

A收到消息M2后，结合初始假设P5和消息含义规则，有：

② A believes B said($A \overset{IVb}{\leftrightarrow} B$, IVa)

由P1，应用消息新鲜性规则，得：

③ A believes fresh($A \overset{IVb}{\leftrightarrow} B$, IVa)

由②式和③式，应用临时值验证规则，可得：

④ A believes B believes($A \overset{IVb}{\leftrightarrow} B$, IVa)

应用信念规则将($A \overset{IVb}{\leftrightarrow} B$, IVa)拆开，得

⑤ A believes B believes $A \overset{IVb}{\leftrightarrow} B$

于是应用初始假设P4和⑤式，由管辖规则，得：

⑥ A believes $A \overset{IVb}{\leftrightarrow} B$

B收到消息M3后，结合初始假设P6和消息含义规则，有：

⑦ B believes A said($A \overset{IVa}{\leftrightarrow} B$, IVb)

由P2，应用消息新鲜性规则，得：

⑧ B believes fresh($A \overset{IVa}{\leftrightarrow} B$, IVb)

由⑦式和⑧式，应用临时值验证规则，可得：

⑨ B believes A believes($A \overset{IVa}{\leftrightarrow} B$, IVb)

应用初始假设P3和⑨式，根据管辖规则，可得：

⑩ B believes $A \overset{IVa}{\leftrightarrow} B$

最终可以得到的结果为：

B believes A believes $A \overset{IVa}{\leftrightarrow} B$

A believes B believes $A \overset{IVb}{\leftrightarrow} B$

A believes $A \overset{IVa}{\leftrightarrow} B$

B believes $A \overset{IVb}{\leftrightarrow} B$

即协议达到预期安全性目标。

新协议通信中只需3条消息。第一次密码建立时，使用了应答者的身份。双方后续密码将使用对方提供的密钥向量，且所有数据不暴露于明文。协议运行后将建立起安全的通信信道。此协议与其他相关协议对比如表1所列。

表1 新协议与其他认证协议的对比

	Helsinki协议	WEP协议	WPA协议	本文设计的协议
主体数量	2	2	3	2
性能	认证简单	认证简单	认证复杂	认证简单
安全性	易受中间人攻击	单向认证	安全性高	安全性较高

结束语 协议开发需要遵循一定的规范和流程。我们所总结的协议设计步骤是在实践基础中逐步总结出来的，适用于小型应用层协议，特别是无线安全协议的快速开发。按照这些步骤，设计了一些适用于无线局域网的协议，并在文中给出了一个认证协议的示例。在这些步骤中，第6步安全性证明是较为困难的，也是至关重要的一个环节。它将是我们下

一步研究的重点，期望能够找到更好的一般性证明方法。

参 考 文 献

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

[2] 卿斯汉. 安全协议[M]. 北京：清华大学出版社，2005

[3] 薛雨杨，周颢，赵保华. 无线局域网 802.1X 协议安全性分析与检测[J]. 西安交通大学学报，2009，43(10)：52-55

[4] 皮建勇，杨雷，刘心松，等. 一种新的安全协议及其串空间模型分析[J]. 计算机科学，2010，37(1)：118-121

[5] 张玉清，王春琳，冯登国. 运行模式法分析 ISO/IEC 密钥建立协议[J]. 通信学报，2005，26(2)：15-18

(上接第 81 页)

$$go(s,a\circ\alpha)=go(step(s,a),\alpha) \quad (3)$$

因为 $p_2 \sim > p_1$，由 delete 函数的定义得

右边

$$go(t,delete(a\circ\alpha,p_1))=go(t,a\circ delete(\alpha,p_1))$$
$$=go(step(t,a),delete(\alpha,p_1)) \quad (4)$$

p_1 满足单步隔离性，因此有

$$s \overset{p_1}{=} t \Rightarrow step(s,a) \overset{p_1}{=} step(s,a)$$

根据归纳假设

$go(s,\alpha) \overset{p_1}{=} go(t,delete(\alpha,p_1))$，所以

$$go(step(s,a),\alpha) \overset{p_1}{=} go(step(t,a),delete(\alpha,p_1)) \quad (5)$$

由式(3)－式(5)可得

$$go(s,a\circ\alpha) \overset{p_1}{=} go(t,delete(a\circ\alpha,p_1))$$

所以，当序列长度为 $n+1$ 时式(2)成立。

于是式(2)对任意长度的动作序列都成立。

令 $s=t=s_0$，由式(2)可得

$$go(s_0,\alpha) \overset{p_1}{=} go(s_0,delete(\alpha,p_1))$$

由于应用程序 p_1 满足结果隔离性质，根据定理 2，可得应用程序 p_1 是运行可信的。

同理可证应用程序 $p_2,p_3,\cdots,p_n$ 是运行可信的。

应用可信的概念包括：应用的静态可信和动态可信。因此应用程序 $p_1,p_2,\cdots,p_n$ 是可信的，即 $trust(p_1)=True$，$trust(p_2)=True,\cdots,trust(p_n)=True$。

3.4 应用环境的可信

在系统 $M1$ 中有 n 个运行的应用程序，任意时刻，可以有一个或多个应用同时运行。由此，可以认为如果系统中的所有应用都可信，就表明系统 $M1$ 是可信的。

定义 7 若一个应用程序 q 是可信的，则系统 $M1$ 的状态 $s\in S_T$ 执行 q 后的状态也是可信的，即

$$step(s,q)=\begin{cases} s_1 s_1\in S_T, & \text{if } trust(q)=True \\ False, & else \end{cases}$$

定理 3 若系统 $M1$ 中执行的所有应用程序都可信，则系统 $M1$ 是可信的。

证明：在系统 $M1$ 下，因为 $p_1,p_2,\cdots,p_n\in P$，并且 $trust(p_1)=True,trust(p_2)=True,\cdots,trust(p_n)=True$，则

$$go(s_0,(p_1\circ p_2\circ\cdots))=go(step(s_0,p_1),(p_2\circ\cdots))$$
$$=go(s_{p_1},(p_2\circ\cdots))$$
$$=go(step(s_{p_1},p_2),\cdots)$$
$$=go(s_{p_1p_2},\cdots)$$
$$\cdots$$
$$=s_n$$

所以系统 $M1$ 是可信的。

推论 1 信任链传递模型能够保证应用的静态可信和动态可信，保证信任链在应用环境中传递，从而保证了整个应用环境的可信。

证明：由定理 1、定理 2 以及定理 3 可知，该信任链传递模型可以保证任何一新运行应用的静态可信和动态可信，从而使应用环境中的信任链传递至该应用，保证了整个应用环境的可信。

结束语 本文提出了一个满足通用的生产信息系统的动态化的信任链传递模型，并基于无干扰理论将系统抽象为应用程序、动作和状态输出，利用应用间的干扰性对提出的信任链传递模型进行了形式化描述和证明。

参 考 文 献

[1] Trusted Computing Group. TCG Specification Architecture Overview, Version1. 2 [OL]. http://www.trusted_computinggroup.org, 2003

[2] 沈昌祥，张焕国，冯登国，等. 信息安全综述[J]. 中国科学 E 辑：信息科学，2007，37(2)：129-150

[3] Trusted Computing Group. TCG Specification Architecture Overview[EB/OL]. https://www.trustedcomputinggroup.org/groups/TCG_1_2_Architecture_Overview.pdf, 2007-8-8

[4] Rushb J. Noninterference, transitivity, and Channel-Control Security policies [R]. CSL-92-02. Menlo Park: Stanford Research Institute, 1992

[5] 黄强. 基于可信计算的终端安全体系结构研究[D]. 武汉：海军工程大学，2007

[6] Goguen J A, Meseguer J. Security policies and security models [C]// Proc of the 1982 IEEE Symp on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1982: 11-20

[7] Mclena J. Security model s and information flow[C]// Proc of the 1990 IEEE Symp on Research in Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1990: 177-186

[8] Phalloran C O. A calculus of information flow[C]// Proc of 1st European Symp on Research in Computer Security. Berlin: Springer-Verlag. 1990: 147-159

[9] 张兴，陈幼雷，沈昌祥. 基于进程的无干扰可信模型[J]. 通信学报，2009，30(3)：7-11

[10] 赵佳. 基于无干扰理论的可信链模型[J]. 计算机研究与发展，2008，45(6)：974-980

[11] 王飞，刘威鹏，沈昌祥. 应用可信传递模型研究[J]. 计算机工程与应用，2007，43(29)：1-3

[12] 谭良，徐志伟. 基于可信计算平台的信任链传递研究进展[J]. 计算机科学，2008，35(10)：15-18