IGRS 与 UPnP 设备互连的安全机制研究 *

谭 珏[1,2], 何 哲[1], 陈援非[1], 朱珍民[1]
(1. 中国科学院 计算技术研究所 普适计算研究中心, 北京 100080; 2. 湘潭大学 信息工程学院, 湖南 湘潭 411105)

摘 要: 对 IGRS 的安全机制、UPnP 的安全机制、IGRS 与 UPnP 基于非安全管道上的互连方法进行了研究分析, 提出了一种 IGRS 与 UPnP 互连的安全机制,保障它们之间互连的安全性,有效防止了网络中针对非安全互连漏洞的各种攻击。

关键词: 信息设备资源共享协同服务协议; 通用即插即用协议; 协议机制; 管道; 安全互连
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)07-2411-03
doi:10.3969/j.issn.1001-3695.2010.07.003

Survey on IGRS and UPnP devices security interconnection mechanism

TAN Jue[1,2], HE Zhe[1], CHEN Yuan-fei[1], ZHU Zhen-min[1]
(1. *Research Center for Pervasive Computing, Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100080, *China*; 2. *College of Information Technology, Xiangtan University, Xiangtan Hunan* 411105, *China*)

Abstract: Through the analysis of IGRS and UPnP security mechanism, this paper put forward a new security mechanism built on the basis of non-security pipes to protect the interconnections of heterogeneous devices. This method successfully protected interconnection from all kinds of network attacks.

Key words: IGRS; UPnP; protocol mechanism; pipe; security interconnection

随着计算机技术与通信技术的飞速发展,众多的信息设备生产商在市场驱动下,开发出了功能多样和强大的设备和仪器,实现这些异构而多样化的信息设备互连互通成为信息技术产品的发展趋势,国际上已有许多标准化组织和企业联盟在进行相关的技术标准制定工作。其中最具代表性的是信息设备资源共享协同服务(IGRS)和通用即插即用(UPnP)两大主流信息设备互连互通协议。IGRS 组织有会员 100 多家,UPnP 组织的成员达到 890 家之多,都拥有非常广泛的末端用户群。IGRS 和 UPnP 的应用范围也非常广泛,在家庭自动化、打印、图片处理、音频/视频娱乐、厨房设备、汽车网络和公共集会场所等类似网络中都有应用。实现支持不同标准的设备间的相互识别和互连互通是用户的一致愿望。IGRS 设备工作组在制定 IGRS 基础协议时,已经对 IGRS 设备与 UPnP 设备的基础互连提出了解决办法,对于分别支持 IGRS 协议和 UPnP 协议的信息设备,可以通过扩展访问接口描述实现它们之间的互连互通。但是,这两类设备的互连互通是建立在非安全管道上,存在一定的安全隐患,须寻求一种安全机制保障互连的安全性。本文通过对 IGRS 和 UPnP 在非安全管道互连互通机制的分析,提出了一种 IGRS 和 UPnP 互连的安全机制。

1 IGRS 和 UPnP 简介

1.1 IGRS

IGRS 是为了实现信息技术设备智能互连、资源共享、协同服务而制定的标准,基于“闪联”标准的设备不仅能够连接,而且可以使不同的设备共享信息资源和功能资源,并充分地组合利用每个设备的功能,创造出更多更丰富的应用服务。为了便于对网络中资源的共享使用,IGRS 在传输层和网络层也制定了相应的协议标准。“闪联”标准框架[1]如图 1 所示。

IGRS 安全规范定义了其上各个协议中的安全交互机制,包括基于服务的访问控制机制和相应的身份认证、授权等机制。IGRS 定义了两个不同层次的安全,一层是设备间的安全,即协议中所谓的“管道”;另一层是用户与服务间的安全,即协议中所谓的“会话”。

1.2 UPnP

UPnP 是由微软推出的新一代网络中间件技术,现在由通用即插即用论坛维护升级,其目标是使家庭网络(数据共享、通信和娱乐)和公司网络中的各种设备能通过简单无缝连接实现广播网、互联网、移动设备之间的互连。

UPnP 标准框架[2]如图 2 所示。UPnP 论坛定义了 UPnP 设备和控制点的安全准则[3,4]。在发现阶段,定义了安全设备和安全控制台相互发现的过程和所需要的安全操作。在描述阶段设备生产商可以为设备定义和编写相关的安全控制台和安全设备描述文件。在控制、事件、展现三个阶段,设置安全会话的密钥,对交互消息进行加密、解密、执行等操作来确保 UPnP 控制点与设备的交互安全。如果用户或者生产厂商需要实施自己的安全扩展,可以在 UPnP 厂商层次上由生产商自定义

收稿日期: 2009-11-22; **修回日期**: 2010-01-04 **基金项目**: 国家“863”计划资助项目(2009AA011902)

作者简介:谭珏(1984-),男,湖南邵阳人,硕士研究生,主要研究方向为嵌入式系统(tj3984@sina.com);何哲(1976-),男,四川南江人,工程师,硕士,主要研究方向为普适计算、嵌入式系统;陈援非(1976-),男,山东济宁人,研究员,博士,主要研究方向为普适计算、嵌入式系统; 朱珍民(1962-),男,湖南慈利人,教授,博士,主要研究方向为普适计算、嵌入式系统.

和实现。

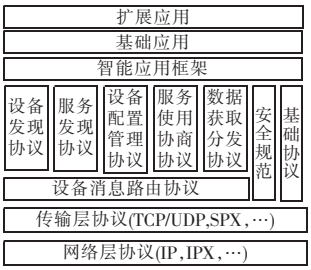


图 1　IGRS 标准框架

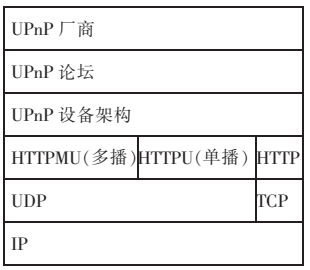


图 2　UPnP 标准框架

1.3　UPnP 与 IGRS 的互连

“闪联”在 IGRS 制定之初就考虑到了 IGRS 设备与 UPnP 设备的互连问题并进行了可行性分析[5]。

1)设备间寻址机制　UPnP 网络基于 IP 寻址,而 IGRS 协议中设备间的寻址可以由 IGRS 协议以外的机制来实现。两个协议均可以共同使用静态 IP、动态 DHCP 或 Auto-IP 的寻址方式。

2)设备/服务发现机制　UPnP 的设备/服务发现机制采用 SSDP,IGRS 的设备/服务发现机制同样建立在 SSDP 基础上。通过 SSDP 可以实现 IGRS 与 UPnP 设备/服务的相互发现。

3)设备/服务描述机制　UPnP 使用 XML 语法,IGRS 也使用 XML 语法。虽然实现模板不同,但是在 IGRS 服务描述中加入 UPnP 描述扩展,使得 UPnP 设备可以识别 IGRS 服务;对 UPnP 服务消息进行解析实现 IGRS 设备对 UPnP 服务的识别。

4)服务访问控制和调用机制　UPnP 的服务调用机制采用 SOAP(简单对象访问协议)传送消息,IGRS 则定义了基于会话的服务调用机制,同样支持 SOAP。通过各自的标准消息解析和改写可以实现服务调用。

5)服务事件与通知机制　UPnP 采用 GENA(通用事件通知架构)机制实现服务事件与通知机制;IGRS 则采用基于管道(安全/非安全)的机制实现,通过不同机制的分析与转换可以实现事件通知。

2　IGRS 和 UPnP 各自的安全互连

2.1　UPnP 设备间互连安全机制

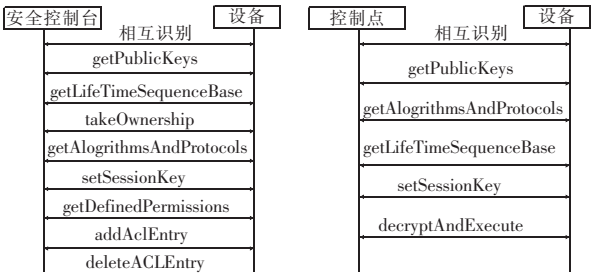
UPnP 安全文档中定义了安全相关的函数和数据结构及相关策略[3,4,6]。其过程分为初始化和安全运行两个阶段。

初始化阶段如图 3(a)[7]所示,主要工作包括:a)安全控制台获取设备公钥并通过散列算法对公钥求取散列值并与设备的安全 ID 比对,进行身份认证;b)安全控制台与设备双方协商,设置安全会话密钥进行会话,控制点获得设备的所有权;c)对网络中的可以访问和拥有设备的控制点进行指定,编辑设备的访问控制列表等,通过这些操作对设备指定不同用户(控制点)的访问权限。执行了这些操作以后,进入安全运行阶段。

安全运行阶段如图 3(b)[7]所示,主要工作包括当初始化阶段通过身份验证及设备权限设置完成以后,进入安全运行阶段。安全阶段的任务是防止黑客的重放攻击,双方进行会话密钥的协商,协商完成后进行通信和服务调用。

2.2　IGRS 设备间互连安全机制

IGRS 设备间的互连较 UPnP 复杂,IGRS 设备间的安全互连过程如图 4 所示。



(a) 设备安全机制初始化阶段　(b) 设备安全机制的安全运行阶段

图 3　UPnP 设备安全机制

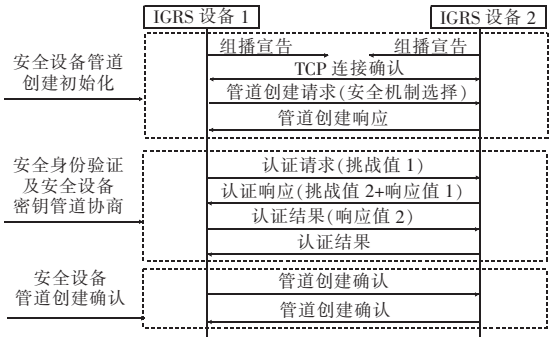


图 4　IGRS 安全设备管道创建过程

在互连的 IGRS 设备之间,通过组播宣告其在网络中的存在后,比较双方都支持的安全机制算法,根据需要选择其一作为双方交互的安全机制。在安全机制选择中,IGRS 支持四种安全机制[8]。IGRS 设备 1 和 2 的安全身份认证为双向挑战/应答过程,需交互的 IGRS 设备 1 和 2 在完成前期相关步骤成功后,相互发送管道创建成功的确认消息;管道成功创建以后,建立 IGRS 用户与服务间的会话关系。

3　IGRS 与 UPnP 之间存在的互连安全问题分析

传统的 IGRS 设备与 UPnP 设备在非安全管道上基础互连,未采用任何安全机制,存在严重的安全隐患。其中存在的安全问题如表 1 所示。

表 1　非安全通道互连安全问题

存在问题	问题描述	解决方法
设备冒充	无认证,身份冒充	加入身份认证机制
消息窃听	攻击者窃听互连中通信消息	对通信消息进行加密
消息完整	攻击者对通信消息进行窜改	采用数字签名机制
拒绝服务	网络中设备无法正常工作	多次身份认证失败后对设备请求不再响应
重放	攻击者实施重放攻击	对网络中的通信消息的序列号更新

1)安全互连的可行性分析　IGRS 与 UPnP 有互操作的基础,可以在非安全管道上进行互操作。同样,改造相关的通信消息模板并对相应的消息和服务调用消息进行扩展,可以实现安全互操作。

2)安全互连的原则　IGRS 和 UPnP 设备有各自的标准和接口,遵循它们各自的功能和属性的基础,对接口进行扩展,避免相同标准下的设备经过扩展和改造以后不能相互识别及访问的问题。

3)安全互连的切入点　根据两个标准的不同定义,找出定义部分的灵活性接口,最大限度地在不改变标准的前提下实现互连的高安全。

4)安全互连的目标　目前 IGRS 与 UPnP 互连只是通过非安全管道对一些服务描述和消息进行简单改写,安全程度很低,达不到安全保密性要求。

在普通互连的基础上,本文从以下几个方面考虑,提出了 UPnP 与 IGRS 的互连安全机制。这几个方面的安全要求是最基本的,却又正是普通互连所缺少的。

a)认证(authentication)。对持有某个标志的用户或设备进行身份鉴别,以确认持有某个标志的用户的真实性。非安全管道中虽然存在设备标志,但是作用仅仅局限于区别不同类型的设备,没有对设备的身份进行认证。

b)消息完整性(integrity)。对互连过程中的消息的完整性进行检查。一般使用消息认证码(MAC)或者安全散列函数加数字签名完成。非安全管道的连接中,没有对消息进行完整性验证,可能会收到窜改过后的消息。

c)防止重放攻击(freshness)。无线环境中的消息很容易被窃听,即使是有线网络中也同样存在相似的问题。因此,需要防止用户登录消息、调用服务消息的泄露、防止重放攻击。在网络中的 IGRS 和 UPnP 设备对于消息的序列号没有更新机制,很容易被黑客利用普通的重放攻击漏洞。

d)访问控制(authorization)。设备根据管理员的需要建立访问控制列表,有对用户访问设备的行为进行访问控制的能力。普通互连没有此种能力对用户或者设备访问权限进行控制。

e)保密性(secrecy)。消息的内容不应以明文的形式在网络中传输才能有效防止他人的窃听。具有安全特性的设备应该具有对消息内容进行加密和解密的能力。非安全管道只是简单的互连,消息的安全加密更加无从谈起。

针对以上五个严重的安全问题,普通的非安全管道显得无能为力,无法满足人们对于安全性的要求。对于以上几个问题,应该研究新的机制来改进和提高互连的安全性。

4　IGRS 与 UPnP 之间互连的安全机制

在此互连互通的安全机制实现方案中,保留 IGRS 设备间的安全互连方式,遵循 UPnP 的安全控制台和 UPnP 设备间的 UPnP 论坛定义的相关安全准则,在这些基础上建立有效的安全互连机制。这样做的好处是保持了 IGRS 和 UPnP 设备各自的安全标准和接口,不会因为与不同标准设备间的互连而导致不同于各自内部标准的接口和安全策略的设备出现,而导致新的互连问题的产生。此过程中尽量保持设备各自标准的独立性,其安全互连过程如图 5 所示。

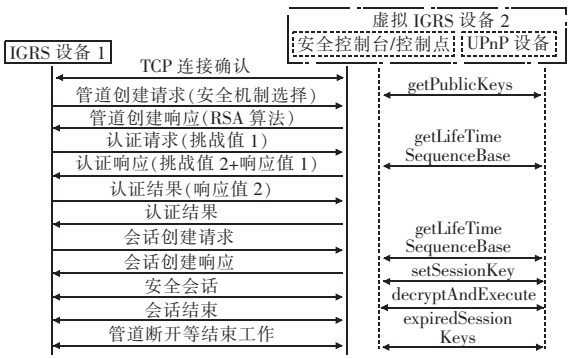


图 5　IGRS 与 UPnP 安全互连过程示意图

图 5 中,UPnP 设备运行安全控制台实现 UPnP 设备的安全属性并且运行相应的消息转换机制在网络上虚拟成一个 IGRS 设备。其中,实线表示的是 IGRS 消息,长线加点表示的是 UPnP 转换成 IGRS 的消息,虚线表示 UPnP 安全控制台与 UPnP 设备之间的消息。图 5 中,虚拟设备是 UPnP 相关设备(包括安全控制台)的扩展,它监听网络上的 IGRS 消息并将这些消息转换为 UPnP 消息,其自身在网络中发送的 UPnP 消息也转换为 IGRS 消息发布到网络中,这样网络中的 IGRS 设备就会发现这些运行在 UPnP 设备上的虚拟 IGRS 设备。

下面是一些重要的安全相关的服务调用[3,5]:

a)GetLifeTimeSequenceBase,得到不重复的随机序列号。

b)GetAlgorithmsAndProtocols,得到设备支持的算法和协议。

c)SetSessionKeys,设置会话密钥。

d)DecryptAndExecute,执行加密的命令(返回加密的结果)。

安全互连过程如下:

a)发现和连接。IGRS 设备和虚拟 IGRS 设备在网络上宣告自己与发现对方,然后进行 TCP 连接,准备进入管道创建阶段。

b)管道的创建。IGRS 设备发送管道连接请求,虚拟 IGRS 设备接收到此消息,转换为内部 UPnP 消息,内部安全控制台调用 getPublicKey( )取得公钥,再将消息封装成 IGRS 格式以发送 IGRS 管道创建响应消息。在双方约定的安全算法选择过程中,此方案采用 RSA 公钥算法。接下来是双方的身份验证、消息加密以及消息鉴别的过程。此过程中,为了防止重放攻击,IGRS 设备随机数产生函数,而虚拟 UPnP 设备则通过安全控制台来调用安全服务 getLifteTimeSequenceBase( ),按照 IGRS 管道身份认证的方法进行安全身份认证挑战。当验证成功后,可以发现设备上提供的服务,但是暂时不能够调用。在这个过程中,黑客可能会使用拒绝服务攻击,可以采用带流量检测的包过滤或者是 XML 防火墙[9]。如果多次在较短的间隔内收到来自同一个设备请求并且在这段时间内反复认证失败,则认为是拒绝服务攻击,在较长的一段时间内不再响应该设备的任何请求。

c)会话的创建。IGRS 设备发送创建会话请求给虚拟 IGRS 设备,接收到消息后虚拟 IGRS 设备调用相关的安全服务 getLifeTimeSequenceBase( )和 setSessionKeys( ),获取安全会话密钥附在响应消息中发送给 IGRS 设备。会话创建成功后,进入会话阶段。

d)安全会话。此阶段中,虚拟 IGRS 设备执行对于服务调用中的会话加密消息进行 decrypeAndExecute( ),同样,IGRS 设备也对接收的虚拟 IGRS 设备消息进行响应,完成相应的功能调用。

e)会话的结束。服务调用结束,双方协商会话结束。此时虚拟 IGRS 设备通过安全控制台执行会话密钥过期的服务调用,注销过期的密钥,结束双方会话。

f)结束。设备之间管道断开、设备离线等。

互连过程安全性分析如下:

a)TCP 连接和发现,发现网络中的互连设备。在网络中的设备只能够被发现,并不能够调用设备上的服务。客户和设备必须经过后续相互认证过程才能够互连,并设计严密的安全步骤,保证无法绕过身份认证。

b)管道创建。在创建过程中,两端都采用公钥算法对各自的身份进行挑战和认证。此过程都有随机数产生,有效防止黑客的重放攻击;同时也有效地解决了表 1 中提到的设备冒充问题;设备间的消息进行加密,阻止不速之客窃听。

(下转第 2420 页)

[22] TUERK T, SCHNEIDER K, GORDON M. Model checking PSL using HOL and SMV [EB/OL]. (2007-05-11) [2009-01-19]. http://www.cl.cam.ac.uk/~tt291/publications/TuSG07.pdf.

[23] PNUELI A, ZAKS A. PSL model checking and run-time verification via testers[C]//Proc of the 14th International Symposium on Formal Methods. Berlin: Springer-Verlag, 2006: 573-586.

[24] 虞蕾, 赵宗涛. PSL 的有界模型检验[J]. 电子学报, 2009, 37(3): 614-621.

[25] EISNER C, SHITSEVALOV I, HOOVER R, *et al*. A methodology for formal design of hardware control with application to cache coherence protocols [C]//Proc of the 37th Annual Design Automation Conference. New York: ACM Press, 2000: 724-729.

[26] BUSTAN D, FISMAN D, HAVLICEK J. Automata construction for PSL [EB/OL]. (2005-05-10) [2009-01]. http://www.wisdom.weizmann.ac.il/~dana/publicat/automata_constructionTR.pdf.

[27] DAVID S B, BLOEM R, FISMAN D, *et al*. Automata construction algorithms optimized for PSL[EB/OL]. (2005-07-10) [2009-03]. http://www.prosyd.org/twiki/pub/Public/DeliverablePageWP3/Deliverable3.2_4.pdf.

[28] MIYANO S, HAYASHI T. Alternating finite automata on omega-words [J]. Theoretical Computer Science, 1984, 32(3): 321-330.

[29] HELJANKO K, JUNTTILA T, KEINÄNEN M, *et al*. Bounded model checking for weak alternating Büchi automata[C]//Proc of the 18th International Conference on Computer Aided Verification. Berlin: Springer-Verlag, 2006: 95-108.

[30] BLOEM R, CIMATTI A, PILL I, *et al*. Symbolic implementation of alternating automata[C]//Proc of the 11th Internationall Conference on Implementation and Application of Automata. Berlin: Springer-Verlag. 2006: 208-218.

[31] CIMATTI A, ROVERI M, SEMPRINI S, *et al*. From PSL to NBA: a modular symbolic encoding[C]//Proc of Formal Methods in Computer. Berlin: Aided Design, 2006: 125-133.

[32] RUAH S, FISMAN D, DAVID S B. Automata construction for on-the-fly model checking PSL safety simpleSubset[R]. Haifa: IBM Haifa Research Lab, 2005.

[33] TZOREF R, BRINKMANN R, NEVO Z. Research report on improved symbolic search strategies and model reduction for static property checking, PROSYD D3.2/2[R/OL]. (2005-03-15)[2009-03]. http://www.prosyd.org/twiki/pub/Public/Public Deliverableold/Prosyd 3.2_2publicversion.pdf.

[34] BLOEM R, JOBSTMANN B, PNUELI A. Property-based logic synthesis for rapid design prototyping, PROSYD D2.2/1[R/OL]. (2005-09-01)[2009-03]. http://www.prosyd.org/twiki/pub/Public/Public Deliverableold/Prosyd2.2_1.pdf.

[35] BLOEM R, GALLER S, JOBSTMANN B, *et al*. Specify, compile, run: hardware from PSL[J]. Electronic Notes in Theoretical Computer Science, 2007, 190(4): 3-16.

[36] BOULE M, ZILIC Z. Efficient automata-based assertion-checker synthesis of PSL properties[J]. ACM Trans on Design Automation of Electronic Systems, 2008, 13(4): 4-1-4-21.

[37] ESPARZA J, HANSEL D, ROSSMANNITH P, *et al*. Efficient algorithms for model checking pushdown systems[C]//Proc of the 12th International Conference on Computer Aided Verification. Berlin: Springer-Verlag, 2000: 299-310.

[38] LANGE M. Linear time logics around PSL: complexity, expressiveness, and a little bit of succinctness[C]//Proc of the 18th International Conference on Concurrency Theory. Berlin: Springer-Verlag, 2007: 90-104.

(上接第 2413 页)

c)会话创建和会话。在会话的创建过程中,调用 getLifeTimeSequenceBase()服务,防止再次可能的重放攻击;同时设置安全会话密钥,对会话内容进行调用,对服务的调用消息进行加密、解密和执行。中间过程只能得到加密过的消息,没有密码无法解密。在安全互连描述中,对频繁进行请求并认证失败的设备不予响应,可以有效防止拒绝服务的攻击。

d)结束工作。调用 expiredSessionKeys()函数删除原有的密钥等一些结尾工作,使得密钥过期,不能够在新的会话中再次使用原来的密钥,进一步增强了密钥的安全性。

5 结束语

在前人关注 IGRS 和 UPnP 设备简单非安全互连的基础上,本文依照 IGRS 和 UPnP 的安全工作原理,参考开源的 UPnP 库对 UPnP 进行改进,实现 IGRS 与 UPnP 的安全互连。原来非安全的互连上存在的设备冒充、重放攻击,互联网络中的设备、用户受到网络干扰等问题,在此方案中得到了十分有效的解决。在泛在设备的互连技术项目中,在已经实现了 IGRS 与 UPnP 互通协议栈的基础上进行了安全扩展,实现了预期的认证、完整性、防止重放、访问控制和保密五大目标。

本系统也存在需要改进的地方,如公钥的维护和更新问题;再者,由于 IGRS 和 UPnP 都存在组播特性,网络上的其他计算机可以"听到",并发现网络中无安全特性的设备,如果这个设备被其他安全设备所信任,那么黑客有可能利用此设备作为跳板来实现对其他设备和服务的攻击。

参考文献:

[1] 闪联工作组. 闪联应用白皮书[R]. 北京: 闪联工作组, 2003.

[2] UPnP Forum. UPnP device architecture 1.0[EB/OL]. (2008-10-15)[2009-11-10]. http://www.UPnP.org/resources/documents.asp.

[3] UPnP Forum. Security console: 1 service template[EB/OL]. (2003-11)[2009-11-10]. http://www.UPnP.org/resources/documents.asp.

[4] UPnP Forum. Device security: 1 service template[EB/OL]. (2003-11)[2009-11-10]. http://www.UPnP.org/resources/documents.asp.

[5] 中华人民共和国信息产业部. SJ/T 11310-2005, 信息设备资源共享协同服务第一部分: 基础协议[S]. 北京: 闪联工作组, 2005.

[6] UPnP Forum. UPnP security ceremonies design document v1.0[EB/OL]. (2003-10)[2009-11-10]. http://www.UPnP.org/resources/documents.asp.

[7] 周雪凤. 数字家庭 UPnP 标准安全研究[J]. 科技情况开发与经济, 2007, 17(25): 1-2.

[8] 廖国威, 杨军, 邓中亮. IGRS 基础协议中的安全机制[J]. 计算机安全, 2006(3): 1-3.

[9] 王佳慧, 贺墚. UPnP 中的 DoS 攻击防御方案[J]. 计算机系统应用, 2008(8): 1-4.