三网融合下的信息安全问题*

武传坤

(中国科学院软件研究所信息安全国家重点实验室 北京 100190)

摘要 三网融合,是指广播电视网、电信网与互联网的融合,其中互联网是核心。尽管现阶段的三网融合主要指高层业务应用的融合,而不意味着电信网、计算机网和有线电视网三大网络的物理合一,但表现在技术上将是趋于一致,如在网络层可以实现互联互通,形成无缝覆盖、业务层上互相渗透和交叉、应用层上趋向使用统一的IP协议等,这将导致在经营上的互相竞争、互相合作,并更好地向用户提供多样化、多媒体化、个性化和高质量的服务,同时行业管制和政策方面也将趋于更加规范和统一。但是,这种新业务模式的改变和转型必将面临诸多新的信息安全问题的挑战,一些在三网融合之前曾遇到的网络安全问题可能会在三网融合之后变得特别敏感。因此,研究分析三网融合下的信息安全问题,将有助于三网融合的健康发展,使用户在享受更好网络通信服务的同时,提供对信息安全的必要保障。本文分析了三网融合下信息安全方面的挑战和可能的解决方案,为三网融合信息安全的认识和解决提供一些指导性思想和技术方法,特别对三网融合下内容保护和安全监管提出了不同于传统理解方法的技术解决思路。

关键词 三网融合,信息安全,内容监管

DOI:10.3969/j.issn.1000-3045.2011.03.010

武传坤研究员

1 引言

2001年3月15日通过的国家“十五”规划纲要中,第一次明确提出三网融合:“促进电信、电视、计算机三网融合”。2010年1月13日,温家宝总理主持召开国务院常务会议,决定加快推进电信网、广播电视网和互联网三网融合。根据网络提供的信息,截至2010年8月16日,12个三网融合试点城市已全部上报试点方案,试点即将正式开始。据了解,有更多的城市对三网融合试点持非常积极的态度,这些都体现了国家近期在三网融合方面得到的积极响应和飞速发展。

现阶段三网融合主要指高层业务应用的融合,而不意味着三大网络的物理整合,

* 收稿日期:2011年4月18日

但表现在技术上将是趋于一致，如在网络层可以实现互联互通，形成无缝覆盖、业务层上互相渗透和交叉、应用层上趋向使用统一的 IP 协议等，这将导致在经营上的互相竞争、互相合作，并更好地向用户提供多样化、多媒体化、个性化和高质量的服务，同时行业管制和政策方面也将更加规范和统一。三网融合还能实现网络资源共享，避免重复建设，形成适应性广、易维护、低费用的高速宽带多媒体基础平台。

从服务形式上看，三网融合无疑会给用户带来很大方便，丰富人们对信息的获取和共享方式，如可以在电视机前拨打可视电话，点播自己喜欢看的电视节目，在手机上看电视，甚至将自己录制的视频共享给亲友甚至更大的用户群体等。但是，这种新业务模式的改造和转型必将面临诸多新的信息安全挑战，也有一些在三网融合之前曾遇到的网络安全问题可能会在三网融合之后变得更加敏感。因此研究分析三网融合下的信息安全问题，将有助于三网融合的健康发展，使用户在享受更好网络通信服务的同时，提供对信息安全的必要保障，也可对保障国家安全和推进和谐社会发展的起到积极的作用。

2 三网融合的特征

为了研究三网融合下的信息安全问题，并进一步提出针对三网融合特征的信息安全解决方案，必须认清以下两个问题：三网融合相对传统的网络有什么特征？现在已有的网络安全解决方案在三网融合环境下有哪些局限性？

三网融合意味着将电信网、广播电视网和互联网通过技术改造，使其成为能够提供包括语音、数据、图像等综合多媒体的综合通信业务平台。其中互联网将成为网络载体的核心，而电信网和广播电视网将更多地侧重于互联网平台上的业务服务。为实现这一目标，要求多方面的标准化和统一性，包括：(1)数据格式的统一(信源)：如电话、数据和图像信号都可以通过统一的编码进行传输和交换，所有业务在网络中都将成为统一的“0”和“1”的比特流；而且许多多媒体数据需经过统一的压缩处理，以适应不同终端的需求；(2)通信协议的统一(信道)：如统一的 TCP/IP 协议，或无论传输使用无线网络(移动通信、卫星通信、光通信等)还是有线网(金属线或光纤)，都能安全可靠地传递数据；(3)通信终端接口的统一(信宿)：即无论接收终端是掌上电脑、台式计算机，还是大屏幕电视，都可以正确识别数据类型并能正确接收。不过，这里所说的统一是一个广泛的概念，指那些被通信单元广泛识别和处理的技术手段，如国际标准和工业标准等，因此统一不等于唯一。从信息安全的角度看，三网融合需要有统一的认证鉴权技术，打破不同行业间的技术壁垒，实现跨平台、跨系统的统一认证鉴权步骤和管理规范。

在工作模式上，三网融合后的网络服务平台为人们提供的将不再是如早期广播电视网一样的信息发布与被动接收，而是用户可以在某种程度上与服务平台实现互动，如选择节目、在线投票、甚至将自己制作的多媒体内容在一定范围内共享和分发等。目前在互联网上虽然可以实现类似的数据共享业务，但共享群体规模比三网融合所提供的平台将小得多。而规模的大小直接影响到某些信息安全指标的重要程度。比如一个共享的多媒体数据，如果涉及到非法宣传的内容，当共享用户规模较小时，可以通过网络监管的方式进行过滤监督，但当共享人群很大(如相当于一个广播电视频道的收视群体时)，通过网络监管的方式是不合适的，即便发现后立即进行制止，很可能已经为时已

晚。特别是当所提供共享数据的来源不可控制时,更可能带来一些社会问题。因此针对三网融合平台,对网络传输的数据,特别是某些广播或组播的大规模共享数据,需要寻求特定有效的管控手段,这是相比传统网络安全而言比较特殊的安全需求,即三网融合下的内容安全问题。三网融合下的信息安全关键技术主要包括如下几个方面:认证机制、网络安全、系统安全和内容安全。

3 三网融合下的信息安全问题

3.1 三网融合下的认证机制、网络安全、系统安全问题

虽然在现有网络环境下,互联网和移动网各自在认证机制、网络安全和系统安全方面都有多种解决方案,但是在三网融合环境下,需要有统一的认证机制,因此需要对现有认证机制进行改造融合,充分发挥已有认证机制的特点为三网融合下的认证机制服务。比如在互联网上的认证一般需要有公钥证书的支持,而移动网上的认证只需要基于预置密钥的对称密码挑战应答方式。如果将两者结合,即三网融合下一些与移动网平台紧密相关业务的认证可以使用两者结合的认证方式,比如让移动网络部分继续使用预置密钥的认证方式,而在互联网阶段,只需要对移动网运营商进行认证即可,这样可以只需要移动运营商(或某些运营商节点)的公钥证书,而不需要每个用户都有自己的公钥证书,这样会在实际操作中减少公钥证书的管理代价(包括计算代价、通信代价、管理成本等)。因此三网融合环境下的认证机制应该跟具体应用类别相关,单一的认证模式是不现实的。

三网融合环境下的网络安全问题将更突出。因为在现有网络中,从互联网接入无线移动网受到很大限制,而在三网融合环境下,由于业务的需求,将有更多的从互联网到无线移动网的接入访问,这样就给无线移动网络的安全带来更大的挑战。传统的移动互联网的信息安全防护措施很可能并不能很好地应对新形势下的安全威胁,需要结合一些针对互联网的安全防护技术,而且需要专门设计一些兼容两种安全防护于一体的网络安全防护技术。

三网融合对系统的安全将带来更大的挑战,其中终端安全就是一个重要且现实的问题。三网融合后许多终端设备,包括移动终端设备,将直接连接到互联网,而互联网对终端系统的攻击方式层出不穷,防不胜防。这些由于体积有限导致功能受限的终端设备可能需要加强和优化信息安全方面的保护,才能有效应对种类繁多的网络攻击。因此三网融合下的系统安全将是一个重要的技术挑战。

3.2 三网融合下的内容安全问题

3.2.1 内容安全问题的重要性

三网融合环境下除了认证机制、网络安全和系统安全将遇到的新挑战,还有一些问题值得我们的重视,这类问题多与上述安全问题有密切联系。如密钥管理问题与安全认证就有着直接的联系,密钥管理一般与认证是分不开的,而认证的目的通常会伴随着密钥管理(如密钥协商等)过程。

三网融合下的另一个特殊问题是内容安全,这在传统网络中未得到足够重视,原因是其安全威胁尚不够可怕。但在三网融合环境下,内容安全问题将会更严重地关系到社会的安全。由一个典型的案例假设即可看出端倪:假如某非法组织在三网融合环境借助某个电视频道向外发布消息,由于该消息的接收群体将远大于传统互联网环境,即使能及时发现,一个短消息的发布可能也已经完成。因此三网融合环境下所传输数据的内容安全是一个特别值得重视的问题。

实际上，在互联网环境下，内容安全已经得到有关部门的重视，一些提供互联网业务的服务平台就根据国家需求对互联网上传输的内容进行一定程度的监管。最近，美国也启动了深度包检测计划(DPI[1])，旨在进一步加强内容安全方面的监管力度。可见，内容安全已经越来越受到重视，在三网融合环境下，内容安全无疑是一项重要的安全防护目标。

内容安全的防护从直观上应该是对内容进行监督分析，使其在发布的同时甚至发布之前就能识别并对非法内容进行阻止。但是经验告诉我们，对网络数据内容的分析监督是何等的困难。垃圾邮件是一种被众人厌恶的网络骚扰，但多年积累的技术对垃圾邮件的治理效果仍然十分有限，一些精心设计的垃圾邮件还是能顺利通过许多垃圾过滤软件的监管。目前对垃圾邮件的过滤多是通过学习过程，即用户收到垃圾邮件，可向网络端进行汇报，网络端经过特征分析，可望在后来截获类似特征的邮件时将其过滤掉。但这是事后行为，只适合垃圾邮件的过滤，因为用户不是同时收到相同的垃圾邮件。这种技术不适合三网融合环境下的数据过滤，因为如果许多用户几乎在同一时间收到垃圾邮件或其他类型的数据，再让系统进行学习并记录特征则为时已晚。

但是，对内容的分析也不是没有效果，许多特殊类别的内容过滤还是能取得很好的效果。比如对黄色内容的过滤就可以根据黄色内容的颜色特征进行分析和匹配的方法进行，但如果发布者将黄色内容变成黑白两色，则上述方法的效果会明显降低，当然变色后的内容在宣传效果上也会降低。针对这一特殊类型的内容防护，可以设计不同等级的内容防护。当遇到内容特征不是很容易提取甚至容易隐藏的数据类型时，如音频，甚至普通多媒体的水印图像，则很难通过内容特征匹配方面的技术进行过滤。更具挑战的是，对内容保护的技术在攻击者看来是公开的，而攻击者的手段是秘密的，至少在攻击之前是这样。因此让公开的技术防护未知的攻击是很困难的，特别当一些攻击手段专门针对已有防护技术进行攻击时更是如此，因此要做到提前防护的确是很大的技术挑战。

3.2.2 内容安全的监管

上述讨论似乎给出这样的论断，即内容防护很困难。根据我们的经验和现有网络环境下的一些实例，内容防护仅从内容特征分析的确很困难，这与三网融合环境没有太大的关系。但这并不意味着内容防护没有好的办法。这里我们试图探讨另一种途径，即通过技术手段和行政管理相结合的方式，使其在实际中达到内容监管的效果。

首先在行政管理方面，对连接到网络的用户进行分类，如(A)广播通信类，目标用户主要是授权的广播电视发布机构；(B)组播通信类，目标用户主要是授权的网络服务平台的管理者；(C)普通用户类，包括所有不属于上述两种类型的用户。另外，对广播通信平台进行授权管理，即哪些网络平台是合法的广播电视多媒体的服务平台。在这种行政管理准备前提下，网络内容的安全监控可以通过如下步骤进行：

(1) 广播通信和组播通信业务都需要对用户进行安全认证，确认数据来源是授权的合法用户，并且用户要对广播或组播的内容进行承诺；该认证由授权的广播通信平台负责。如果通过某种途径(事前或事后)证明某个广播或组播内容是应该被禁止的，则来源用户将对其所造成的后果负有不可推卸的责任，除非该用户可以将责任追溯到他人。在实际应用中，广播通信用户还需要对

广播通信平台进行认证,否则可能会造成经济损失,但这不是内容监管所考虑的问题。

(2) 监管部门对除授权的广播通信平台之外的平台进行定期检查,看这些平台是否发布广播通信类业务。一旦发现,无论这些通信类业务本身的内容是否有问题,都将根据有关法律法规对运营者进行惩罚。检查业务类型比检查业务数据内容要容易得多,因此具有操作的可行性。

容易看出,上述规定并没有影响三网融合对服务便利性的影响。三网融合的影响是广播通信类业务发布信息的途径发生了根本性变化,但普通用户发布信息的途径与当前通过互联网的情况基本一致,当然普通用户可能会有更多的终端设备使用,如多媒体数字电视。

需要说明的是,上述对数据内容安全监管的方法简单地说就是谁发布谁负责。是否会存在"勇敢者"敢冒天下之大不韪,明知内容非法却仍进行广播或组播呢?这种可能性与目前情况下某个广播电视台从当前的广播电视网发布这些信息的可能性是一样的,而且成功的可能性还要低,因为通过多媒体网络服务平台进行发布时,该平台要使用技术和人工相结合的手段对内容进行检测过滤,即使检测手段有许多漏报情况,也比现在完全依赖广播电视台的情况要好。

但是,对内容安全的监管还没有可靠的具体方案实施,因为这不仅仅是管理方面的问题, 更重要的是为管理所提供的技术支持,这些相关技术包括如下几方面的问题:

(1)如何为用户进行授权? 如何为网络平台进行授权?虽在技术上已有许多成熟的手段, 但对三网融合这一具体产业架构,需要在管理层面解决这一问题。

(2)对不同类别的用户应分别使用什么认证方案?使用哪种数字签名方法和哪种协议来提供认证服务?这些则是需要根据需求进一步分析和研究的。

(3)存在哪些可能的攻击(假冒、重放、拒绝服务等)和使用什么预防、灾难恢复等方案? 这些问题不仅需要严谨的科学分析,还需要持续的研究和更新。尽管目前有许多种密码算法可选, 有许多种认证协议可用,有许多种网络安全方法可采纳,但是,一个安全可靠的系统的建立不是将这些方法的简单组合。因此科学的分析和论证,特别是对整体安全解决方案的有机整合是解决三网融合信息安全问题的必要途径。

除了技术上有许多问题需要解决和不断发展外,在管理方面也有一些问题尚待解决,比如,如何为用户进行分类?如何对授权网络平台进行审核审批?谁来负责授权?这些问题都将对规范三网融合后的网络管理和使用,特别是保障三网融合安全健康地发展具有重要意义。

总之,内容安全很难通过某种尖端设备来过滤,但可以通过一个安全系统来实现。

3.3 三网融合下对电子财产和电子财产知识产权的保护

我们都知道要保护国家财产、企业财产、个人财产等,通常我们对这些财产的理解都是有形的,即看得见摸得着的。近年来,国家也逐渐重视对无形财产的保护,如对民俗文化遗产的保护。但是,对电子财产的保护还很不够。所谓电子财产,即所有以电子形式存在 (如可存储于计算机或其他介质)且有价值的数据,如图片和多媒体就是典型的电子财产。我们除了要对电子财产本身进行保护外,在一定条件下还需要对其知识产权进行保护,即电子财产的内容虽然可以被使用(或消费),但使用者必须遵守一定的规则,而不能非法盈利或非法使用(如非法篡改)。如何保护电子财产和电子财产的知识

产权一直是一个重要研究课题，而三网融合更强化了这些问题的重要现实意义。

目前对图片、多媒体等类型的电子财产已有一些保护方法，通常的认证和机密性就可以用来提供对这类财产的保护，因为它们可以压缩后被当作普通数据来处理。对这类电子财产知识产权的保护也有一些技术方法，如水印技术、指纹技术等。但计算机软件作为一类特殊而且重要的电子财产，在本身的保护和其知识产权保护方面的研究都不够，一些企业解决方案缺乏理论支持，不具有规模化和可发展性。三网融合环境下给人们提供了更多合法和非法获取这些电子财产的机会，因此加强电子财产的保护和知识产权保护是三网融合时代面临的另一项重要的挑战。

4 发展建议

当前我国各职能部门正各自为三网融合的发展作着积极的准备，各相关企业也异常活跃，特别是网络运营商更是为三网融合的发展进行着多方面的积极筹备。同时，相关的标准规范也在制定中。但是从长期可持续发展方面看，三网融合的终极目标除了需保证其功能外，更应重视其性能，其中信息安全保障就是重要的性能指标。

2009 年美国提出了对深度包检查(deep packet inspection, DPI)的发展战略，以加强对互联网上传输数据的检控能力。三网融合将拓宽互联网的功能，无疑会增加互联网上传输的数据类型和来源，因此对数据包深度检测更为重要。但是，对数据包深度检测不能仅从字面上理解，应该从其根本目标上理解。正如上述分析所表明的，如果仅仅从数据包本身进行深度检测，则效果非常有限，而且很容易被恶意攻击者逃脱。为了更好地实现对网络数据的监管和管控，需要安全监管的整体方案，并且需要对数据包进行深度检测的技术手段。前者是解决问题的根本，后者则起到辅助作用，为前者提供一些技术帮助，目的在节省人力成本。

然而，根据笔者所了解的情况，目前国家对三网融合安全方面的投入除了加强传统的互联网和移动网安全外，新增投入主要是对数据包本身的检测方面，缺乏对网络监管整体系统的研发投入。在当前的网络监管能力很有限的情况下，需要将当前的行政管理手段同密码技术相结合，特别是认证技术和电子证据技术方面的结合，才能更好地服务于三网融合下的安全监管。

总之，三网融合所带来的信息安全挑战，除了目前网络和系统所面临的安全挑战外，更突出的是安全监控和知识产权问题。如何解决好这些问题关系到三网融合的健康发展。解决这些问题不能单一依赖技术手段、管理手段或政策措施，而应该将这些手段有机地结合，才能更有效地提供三网融合所期望的服务。因此，希望国家有关部门加强将三网融合作为一个整体系统来解决安全监管的研究方面的投入力度，以及电子财产安全和电子财产知识产权保护方面的投入力度。

最后要强调的是，对一个系统的信息安全保护不是单凭一个插件或设备就可以实现的，必须要有一套完整的安全体系和配套的安全解决方案。

主要参考文献

1 http://epic.org/privacy/dpi/

The Security Issues in Triple-play

Wu Chuankun

(State Key Laboratory of Information Security, Institute of Software, CAS 100190 Beijing)

Abstract Triple-play in China is to integrate the broadcast and TV networks, the China Telecom Networks, and the Internet together, where the Internet will play a key role. Although at the preliminary stage, the triple-play in China mainly means to integrate application services in the high layer of networks, and does not mean to physically combine the three networks together, the technology will tend to be the same, for example, in the network point of view, interconnection can be established which can provide thorough coverage, and in the service point of view, there will be interpenetration and overlap, and in the application point of view, it tends to use the standard IP communication protocol. These features will lead to competation and collaboration in business operation, hence to provide users higher quality of services which are more dynamic, multimedia-driven, and more personalized. In the mean time, administrative control and policy making will also become more formal and consistant. However, the change and evolution of this new model of business operation will also face many new information security challenges that have not been encourtered before, while some other security challenges occured before may become more sensitive and servere in the triple-play environment. Therefore, in-depth study on the issues of information security in the triple-play environment is a necessity to ensure the healthy development of the triple-play, to provide necessary ensurance about the information security for users when users enjoy better network communication services.

This paper gives some preliminary information security challenges and possible ways of finding solutions in the triple-play environment, tend to provide some methodological and technical approaches toward understanding and solving the information security issues in triple-play environment, and in particular, a technological approach to ensure the content security and security surveillance is provided that is different from traditional methods.

Keywords triple-play, information security, content security

武传坤 中国科学院软件所研究员、博士生导师。1985 年获理学学士学位,1988 年获理学硕士学位,1994 年获工学博士学位。1992 年破格晋升为副教授,1995 年破格晋升为教授。2002 年入选中科院“百人计划”,曾获得包括国家教委科技进步二等奖和三等奖等多项科技和荣誉奖励,1991 年度机械电子部优秀科技青年,1993 年起享受国务院政府特殊津贴。现为 IEEE 高级会员,国际密码学会(IACR)会员。先后任 2001,2002 和 2003 年度密码学和网络安全国际学术会议程序委员会主席。目前主要研究方向为密码学和网络安全和物联网中的安全。E-mail:chuankun.wu@gmail.com