学校编码：10384　　分类号_____密级_____

学号：X2013232081　　UDC _____

厦门大学

工　程　硕　士　学　位　论　文

面向广电互动电视安全系统的设计与实现

Design and Implementation of Interactive TV Security System of Broadcast and TV Network Group

林动

指　导　教　师：　林　坤　辉　教　授

专　业　名　称：　软　件　工　程

论文提交日期：　2016　年　09　月

论文答辩日期：　2016　年　11　月

学位授予日期：　　年　　月

指　导　教　师：_____

答辩委员会主席：_____

2016 年 9 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或排课的资助，在（　　）排课完成。（请在以上括号内填写课题或课题组负责人或排课名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（ √ ）2.不保密，适用上述授权。

（请在以上相应括号内打。√。或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

广电互动电视业务随着“多业务”运营的深入不断发展，互动电视业务系统的建设需要考虑业务发展的多样性，还需要考虑不断用户增长的扩展性。作为“可运营、可管理”不可分割的一部分，互动电视业务系统的安全性至关重要。随着网络的快速发展和应用技术的飞速进步，系统安全越来越重要，针对互联网的黑客破坏攻击逐渐由网络层迁移到系统层以及应用层。各种新颖类型的黑客、病毒、漏洞攻击和常见的不规范操作都很都很大概率严重威胁到互动点播平台。有线电视用户在享受稳定服务的过程中，也存在着遇到各种安全风险的可能，为了提供互动电视系统的安全能力，需要对互动电视安全系统进行统一规划及加固建设。

互动电视系统安全加固建设从多层次出发考虑，借助已有的安全防范技术与手段并将其实践于现实网络环境当中，让互动电视系统作为一个安全防御系统能够支持同用户群的使用，在确保互动电视系统安全可靠的前提下，还保障了用户能够正常使用业务安全。

本研究旨在设计出互动电视系统的网络层、应用层、系统层的安全方案，且追求方案的详细性，研究中详细论述了触及到的关键技术，为广电网络互动电视系统的安全化提供一个参考。

关键词：系统安全；系统加固；服务管理

Abstract

Radio and television interactive TV service with "business operation" in-depth development, the construction of interactive television service system needs to consider the diversity of business development, also need to consider the extension of continuous user growth, as part of "operation and management" inseparable, safety critical interactive TV system. With the rapid development of network and the rapid progress of application technology, the system security is becoming more and more important. The hacker attacks against the Internet gradually moved from the network layer to the system layer and application layer. A variety of novel types of hackers, viruses, vulnerabilities and common non-standard operations are very large probability of a serious threat to interactive VOD platform. In the process of cable TV users enjoy a stable service, there are also encountered various security risks, in order to provide safety capability of interactive TV system, the need for interactive television security system for unified planning and reinforcement construction.

Interactive TV system security reinforcement construction from the multi-level view, with the existing security technology and means and practiced in the real network environment, make the interactive TV system as a security defense system can support the use of user groups, in order to ensure the interactive television system is safe and reliable under the premise, but also to protect the user can the normal use of the business safety.

The purpose of this study is to design the interactive TV system network layer, application layer, system layer security scheme, and the scheme with the pursuit of research, elaborated the key technology involved, which provides a reference for the safety of radio and television network interactive TV system.

Key words: System Security; System Reinforcement; Service Management

目 录

Contents

第一章 绪论

1.1 研究背景和意义

随着三网整合政策和深化文化体制改革的部署和要求在全国各地全面铺开，传统电信运营商 IPTV 营销走向阳光，其大力拓展 IPTV 用户，严峻的政策和竞争压力迫使广电运营商加速全面转型。IPTV 和互联网新型电视媒体服务近年来发展迅速，个性化视频内容和传统媒资并存，但由于政策的倾向，广电运营商作为传统视频服务提供商的优势就是因为其有可管可控的内部网络和大规模稳定的用户群体。

广电运营商靠着丰富的有线电视视频多业务运营经验，以宣传党的方针政策和大众文化为主要责任，一直在为广电用户提供稳定可靠、安全高效、优质优量的广播电视服务，为社会公益事业做出自己的贡献。“广电互动电视系统”是基于广电业务的全媒体互动平台，提供直播、点播、时移、回看、公共信息、八闽集萃、智慧家庭等多项服务，提供各类公共信息查询、缴费支付、政务发布、预约挂号、游戏、电视商城等增值应用。该系统的投入使用，标志着广电正式跨入“互联网+电视”新时代，真正让用户从“看”电视进行到“用”电视的时代。

1.2 现状和存在问题

互动电视系统建设之初因为建设周期紧只考虑方便和业务快速上线，随着网络拓扑不断变大和复杂，用户接入途径多元化，移动办公、远程接入成为日常副产品作模式不可或缺的部分[1]，由于未经认证的非常接入，把潜在的病毒、木马、恶意代码等带入内部网络，造成重要信息泄密，危害内部安全[2]。

目前互动电视系统分为三个区域如图 1.1 所示。互动平台区域、媒资平台区域、增值平台区域，三个区域通过核心防火墙相连接，互动平台区域和增值平台区域通过核心防火墙对终端提供服务，增值平台区域和互动平台区域、媒资平台区域之间无法互相访问，互动平台区域和媒资平台区域之间可以互相访问。互动电视系统与 BOSS 互联接口、内容提供商互联接口、媒资平台互联网接口、增值平台互联网接口等部署有防火墙，增值专线业务未部署防火墙。

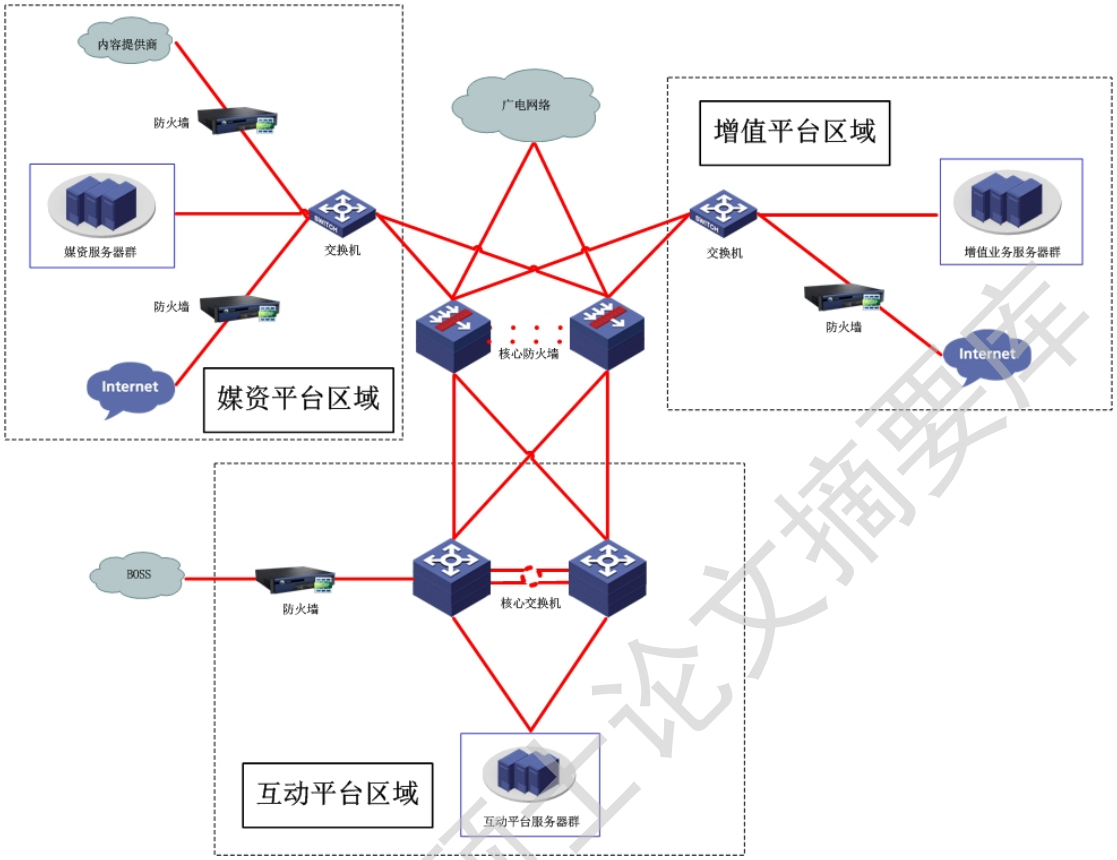

图 1.1　互动电视系统结构

互动电视系统存在以下问题：

1. 缺乏对入侵行为的实时检测、监控和响应。

2. 缺乏对攻击行为的联防措施，无实时检测、监控和响应。

3. 对 IP 访问没有进行有效的访问控制。

4. 对来自于内网的安全威胁，包括内部攻击、蠕虫病毒等，没有有效的监控和防护措施。

5. 未建立日志统一收集及管理机制，将关键设备、服务器、操作系统等日志进行统一收集存储，并且对日志进行分析，导致日志零散存储，部分告警日志被忽略。

6. 未建立统一实时告警平台，设备、业务系统等出现异常或故障告警信息未进行统一管理并发送给相关管理人员，导致不仅无法第一时间通知先关人员解决，事后也查询不到任何历史告警数据。

7. 未能对系统网页篡改、应用系统漏洞攻击等进行防护。

8. 攻击行为或者威胁行为发生后，无法确定威胁来源，不清楚威胁是来自于内部还是来自外部。

9. 内部人员的误操作造成的安全隐患无法定位相关责任人员。

1.3 论文研究内容

本文将探讨互动电视系统的网络层、应用层、系统层的安全方案，且追求方案的详细性，此外还将详细论述触及到的关键技术。

互动电视系统在安全防护工作当中的核心即为，保障涉及到的播出系统的安全防护强度。针对安全防护有三个安全层面的要求：物理安全层面、技术安全层面以及管理安全层面。从网络、主机、应用这三个方面提出了有关安全要求。

追究互动电视系统安全加固建设的深层内涵，借助各种各样的安全加固方法与技术，分析现实网络真实环境，将互动电视安全系统建设成一个不同用户群的安全体系，在保证业务系统高可靠使用的同时，保证业务正常开展。

1. 加强对现有网络的控制，做到网络边界可管可控；

2. 消除各种系统、各种应用服务自身存在的大量漏洞和认为操作或与安全策略相违背的系统配置；

3. 强化病毒感染测试，增强抵御病毒入侵能力，高校抗击网络外部的多类型攻击行为，与此同时也要抑制内部不合规定的各种操作行为；

4. 通过安全加固手段明显提高系统的安全等级级别；

5. 针对应用服务的安全风险有针对性的进行安全加固，防止应用服务的安全威胁危害整个系统的安全；

6. 增强系统防御水平，使得业务系统内部的各种敏感信息在网络协议中传输，为系统本身制定严格的不同策略，防止黑客绕过防御体系进行破坏的行为；

7. 加强系统页面被非法篡改的能力。

1.4 论文组织结构

本文重点探讨面向广电互动电视系统安全体系升级改造项目的分析与设计，总共分为六章，组织结构如下：

第一章 绪论。阐述面向广电互动电视系统安全体系升级改造工程项目的发行方案的分析与设计的背景和意义，现状和存在的问题以及本研究的创新点。

第二章 网络安全相关理论与技术。通过大量查阅国内外相关技术资料的方式，总结并简介网络安全相关概念与技术及互动电视网络的体系结构。

第三章 系统分析。通过将分层分析的方法，在多个层面上进行细致的风险分析，指出该安全体系存在的问题。

第四章 系统设计。结合实际情况和业务要求，列出设计目标、设计原则与设计方案。

第五章 系统实现。结合 IT 服务管理的理念，在整个项目实施过程中穿插使用，并阐述实施方案。

第六章总结与展望。针对该项目做出总结并展望下一步的发展方向。

第二章 网络安全相关理论与技术

强大而有力的理论支持是软件工程项目实施的关键和基础，理论与实践的完美结合是放大理论价值、实施项目的重要前提。本章主要对安全相关方面的理论知识进行介绍，并结合广电互动平台实际情况提出所涉及到的安全相关技术。

2.1 网络安全概念

所谓计算机病毒，指的是编制或者插入在程序当中的，能够损坏计算机内部数据或阻碍计算机的正常使用的，并且可以实现自身复制的指令或代码[3]。病毒成功入侵后的计算机往往在一定程度上失去了全部或者一部分正常的工作运转能力，如运算速度下滑、文件丢失、数据损坏。作为病毒的子类，蠕虫在传播过程中不需要借助用户的任何操作，蠕虫能够仅凭网络就可以传播分发出自身的复制副本，且副本具有高度完整性[4]。一旦计算机被蠕虫侵入，那么计算机的内存将被快速消耗、网络宽带也会受到严重影响，最终计算机沦为崩溃状态。人们常说的木马指的是一种计算机程序，这种程序从表面来看具有使用价值，但事实上起到的却是破坏作用。

计算机系统的脆弱性是产生计算机病毒的根本原因，冯诺依曼体系提供了病毒存在的可能，另外从理论上也可以证实，没有信息共享，就不会存在计算机病毒。而信息共享是当前计算机网络的基础，并且冯诺依曼体系已经被广泛应用，所以计算机病毒必将长期存在，人们只能在计算机病毒存在的前提下，研究对付计算机病毒的策略[5]。

计算机网络的发展就是计算机病毒的发展历史，新的病毒往往会伴随着新技术的发展而出现。

现在的Intelnet网络是在1968年美国国防部高级研究计划管理局组建的阿帕网的基础上建立起来的，阿帕网为 Internet 的产生和进步起到了奠基性的作用，阿帕网在解决不用类型计算机之间网络互联的一系统理论和技术问题方面表现出了很强的优越性[6]。阿帕网作为一个网络系统，它的建立是以“包交换理论”为基础的，具有去中心化或分布式特点。这里提到的“包交换理论”指的是将每

份信息都切分成一定大小的块并对其“打包”，然后对这些包进行逐个标注，标注的内容即是从哪来，到哪去。该原理是 1964 年由保罗·巴伦给出的。保罗·巴伦提出设想，假设将某种接口建立于电脑或互联网之间，实现互联网之间的可连接性。而且，该种可连接性具有直接相连性，可以不用中央控制，借助互联网间的接口便可实现连接。此种模式下的网络通信不由中央控制，数据的传送也不再简单，这种方式下的数据传送是通过不同网络站点之间的连接实现传送的。1983 年，ARPA 指出了阿帕网的标准协议，即 TCP/IP 协议集，且该协议集是用于异构网络的[7]。该网际互联网的主干网为阿帕网，人们将其称之 Internet。

OSI 网络结构模型共有七层，而 TCP/IP 协议覆盖了其中六层，而且从第二层到应用程序的各项功能。其中，寻找地址是核心功能之一，除此之外，还有路由选择和传输控制也是其中的核心功能[8]。

IP 协议是 TCP/IP 协议网络层的主要协议，IP 协议提供的数据报传送机制是无连接的。IP 协议实现上非常简单，它对数据提供“尽力而为服务（Best-effort Service）”，即它不能保证传输的可靠性，对 IP 协议只负责将分组送到目标节点，至于能否成功进行传输，不进行检验，不通知确认，也不能保障分组过程中的顺序是否正确，而将可靠性工作交给运输层处理[9]。

传输控制协议（TCP）作为一种传输协议不仅是面向连接的、端到端的，而且是基于字节流的，同时还具有高度的可靠性。用户数据协议（User DataProtocol，UDP）则是端到端的传输协议，而且是无连接的[10]。

从互联网络 TCP/IP 设计之初衷可以看出，当时仅仅只考虑了方便性、开放性，这种天生的“善良”有损互联网的坚强程度，加大了黑客成功攻击互联网的可能性以及有组织群体成功侵入互联网的概率。伴随着增长的网络规模，新的网络技术正越来越多，日益复杂的网络组织，网络越来越高度合作，在现有的网络安全系统形成了新的挑战，如何保证网络安全在我们面前成为了一个重要问题。

2.2 网络安全技术

网络安全保护的重要在于一种访问过程，且是主体对客体的访问。首先，不仅需要认证主体的身份，同时还要认证客体的身份；其次，要注意加密全部访问过程，同时做好访问过程中的防止恶意程序代码以等工作；最后，要核查追踪并