Contents

Preface xv
About the Author xvii

1 Introduction to IPTV 1
1.1 Introduction 1
1.2 General Threats to IPTV Deployments 3
  1.2.1 Access Fraud 4
  1.2.2 Unauthorized Broadcasting 5
  1.2.3 Access Interruption 5
  1.2.4 Content Corruption 6

2 Principles Supporting IPTV 9
2.1 History of Video and Television 9
  2.1.1 Television 10
2.2 Viewing Experience of Video 15
  2.2.1 Line Scanning 15
  2.2.2 Video Resolution 15
  2.2.3 Number of Pictures per Second 16
  2.2.4 Aspect Ratio 16
  2.2.5 Video Compression Method 16
2.3 Video Compression 16
  2.3.1 MPEG-2 17
  2.3.2 H.263 18
  2.3.3 MPEG-4 18
2.4 TCP/IP Principles 19
  2.4.1 Addresses 19
  2.4.2 Routing 20
    2.4.2.1 IP Packet 20
2.5 Summary 21
References 22
Bibliography 22
3 IPTV Architecture

3.1 High-level Architecture

3.1.1 Service Types

3.2 Functional Architecture for the IPTV Service

3.2.1 Content Provision
3.2.2 Content Delivery
3.2.3 IPTV Control
3.2.4 Subscriber Functions
3.2.5 Security

3.3 Detailed IPTV Architecture

3.3.1 Head End (IPTV Service Provider)

3.3.1.1 Critical Elements of the Head End
3.3.1.2 Content Input
3.3.1.3 MPEG Video Encoder
3.3.1.4 IP Encapsulator
3.3.1.5 Video Transcoder
3.3.1.6 Content Management Server
3.3.1.7 Video Repository
3.3.1.8 Digital Rights Management
3.3.1.9 Video Streaming Server
3.3.1.10 Subscriber Interaction

3.3.2 Transport and Aggregation Network (IPTV Network Provider)

3.3.2.1 RP and RTSP
3.3.2.2 RTSP
3.3.2.3 Ismacryp
3.3.2.4 PIM
3.3.2.5 MSDP
3.3.2.6 DSM-CC
3.3.2.7 Internet Service Provider
3.3.2.8 DSLAM

3.3.3 Home End (Subscriber)

3.3.3.1 Set Top Box

3.4 Summary

References

4 Intellectual Property

4.1 Introduction

4.2 Supporting Technology

4.2.1 Symmetric Key Cryptography
4.2.2 Asymmetric Key Cryptography
4.2.3 Hybrid Encryption
4.2.4 Hash – Digest
4.2.5 Commonly Used Algorithms
4.2.6 Public Key Infrastructure and ITU-T Recommendation X.509
4.2.7 Operation of PKI
4.2.8 Secure Socket Layer and Transport Layer Security

4.3 General Mechanisms for Content Protection

4.3.1 CPS
4.3.2 CAS
4.3.3 DRM
4.4 Operation of DRM on IPTV

4.4.1 DRM Applied to VOD

4.4.2 DRM Applied to Broadcast TV

4.4.3 Smart Cards and DRM

4.4.4 Storage Protection

4.4.4.1 VCPS

4.4.4.2 CPRM/CPPM (CPSA)

4.4.5 Open DRMs

4.4.5.1 SDMI

4.4.5.2 OMA DRM

4.4.5.3 DMP

4.4.5.4 MPEG21

4.4.5.5 MPEG21 REL Data Model

4.4.5.6 DVB-CPCM

4.4.5.7 DVB-CBMS

4.4.5.8 PERM

4.4.5.9 DCAS

4.4.5.10 DReaM

4.4.5.11 OpenIPMP

4.4.5.12 OpenCA

4.4.5.13 PachyDRM

4.4.6 Interoperability Proposals

4.4.6.1 Coral

4.4.6.2 DMP

4.4.6.3 SmartRight

4.4.6.4 SVP

4.4.6.5 OpenCP

4.4.6.6 OMArlin

4.5 Watermarking and Fingerprinting

4.5.1 History

4.5.2 Steganography Techniques

4.5.3 Watermarking and Fingerprinting Principles

4.5.4 Typical Attacks

4.5.5 Forensic Use of Digital Fingerprints

4.6 WWW? (What Went Wrong?)

4.6.1 Introduction

4.6.2 Satellite Television

4.6.3 DVD Protection

4.6.4 AACS on Blue-Ray and HD-DVD

4.6.5 Videos Over the Web

4.7 Authentication

4.8 Summary

References

Bibliography

5 Existing Threats to IPTV Implementations

Co-authored by Andrew R. McGee, Frank A. Bastry and David Ramirez

5.1 Introduction to IPTV Threats

5.1.1 Specific Threats to IPTV Environments

5.2 IPTV Service Provider – Head End

5.2.1 Video Feeds – Live or Prerecorded (Physical Media, OTA, etc.)
5.2.2 Video Switch 126
5.2.3 Ingest Gateway (Video Capture) 127
5.2.4 Platform SW/OS – Stored/Running 127
5.2.5 Content Management System 127
5.2.6 Content Metadata from Video Repository 128
5.2.7 MPEG-2 Content from Video Repository 128
5.2.8 MPEG-4 Content 128
5.2.9 Load Balancer Software 129
5.2.10 Master Video Streaming Software 129
5.2.11 CA/DRM Service 129
5.2.12 SRTP Keys 129
5.2.13 Ismacryp Key 130
5.2.14 Key Management Protocol 130
5.2.15 CA/DRM Service Administration 131
5.2.16 VOD Application – Cached Video Content Metadata 131
5.2.17 Cached MPEG-2/MPEG-4 Content (Primary and Secondary Storage) 131
5.2.18 Video Streaming Software 132
5.2.19 Local Ad Insertion Authentication Information (e.g. User ID(s) and Password(s)) 132
5.2.20 Local Ad Metadata 132
5.2.21 Local Ad MPEG-2/MPEG-4 Content 133
5.2.22 Local Ad Insertion Tracking Information 133
5.2.23 nPVR Application Recorded/Stored Content Metadata 133
5.2.24 Recorded/Stored MPEG-2/MPEG-4 Content 134
5.2.25 nPVR/Video Recording Software 134

5.3 IPTV Network Provider – Transport and Aggregation Network 134
5.3.1 Protocol Vulnerabilities 134
5.3.2 Content Distribution Service: Unicast Content Propagation – FTP or Other Transport Protocol 137
5.3.3 Multicast Content Propagation 137
5.3.3.1 IGMPv2/v3 (Snooping) 137
5.3.3.2 PIM (SM, SSM, Snooping) 138
5.3.3.3 MBGP 139
5.3.3.4 MSDP 139
5.3.3.5 MFTP 140
5.3.3.6 RTP 141
5.3.4 QoS Signaling (RSVP, DiffServ) 141
5.3.5 Management of Content Distribution Service 142
5.3.6 Connection Management Service 142
5.3.6.1 DSM-CC Protocol 143
5.3.6.2 RTSP Protocol 143
5.3.6.3 MPEG-2 Video Stream 143
5.3.6.4 MPEG-4 Video Stream 144
5.3.6.5 DSM-CC 144
5.3.6.6 RTSP 145

5.4 IPTV Subscriber – Home End 145
5.4.1 Set Top Box 145
5.4.2 STB Executing Software 147
5.4.2.1 DRM Software 147
5.4.2.2 Middleware Client SW 147
6.2.2.1 Satellite Feed 177
6.2.2.2 Premium and Direct-feed Content, Pre-encoded Content Ready to be Encapsulated 178
6.2.2.3 Physical Media 179
6.2.3 MPEG Video Encoder and Video Transcoder Functions 179
6.2.4 IP Encapsulator 180
6.2.5 Content Management Server 182
6.2.6 Video Repository 182
6.2.7 Digital Rights Management 184
6.2.8 Video Streaming Server 187
   6.2.8.1 IGMPv2/v3 188
   6.2.8.2 MBGP 188
   6.2.8.3 MSDP 188
   6.2.8.4 RTP 188
   6.2.8.5 RTSP Packets 189
   6.2.8.6 RSVP 189
6.2.9 Middleware Server 189
6.3 Aggregation and Transport Network 190
   6.3.1 DSLAM 190
      6.3.1.1 Access and Session Control 191
      6.3.1.2 Routing 193
      6.3.1.3 User Segregation 193
      6.3.1.4 Quality of Service 194
      6.3.1.5 Virtual Networks and Virtual Circuits 194
      6.3.1.6 802.1X Authentication 195
   6.3.2 Firewalls 196
6.4 Home End 197
   6.4.1 Residential Gateway 197
      6.4.1.1 Filtering 197
      6.4.1.2 Quality of Service 198
   6.4.2 Set Top Box 198
      6.4.2.1 Secure Processor 198
      6.4.2.2 DRM 200
      6.4.2.3 Output Protection 200
6.5 Secure IPTV a Reality 201
References 202

Appendix 1 Converged Video Security 205
A1.1 Introduction 205
A1.2 Threats to IPTV Deployments 205
A1.3 Protecting Intellectual Property 206
A1.4 VOD and Broadcast 207
A1.5 Smart Cards and DRM 208
A1.6 Countering the Threats 208
   A1.6.1 Threat References 210
   A1.6.2 Threat Models 211

Appendix 2 Federated Identity in IPTV Environments 217
A2.1 Introduction 217
A2.2 IPTV Federated Identity Solutions 217
   A2.2.1 SAML for Security 218