Foundstone
Professional Services
A DIVISION OF McAFEE

PAC SEC

» Triple Play; Triple Threats? IPTV Security

Yen-Ming Chen
Senior Principal Consultant
Foundstone, A division of McAfee

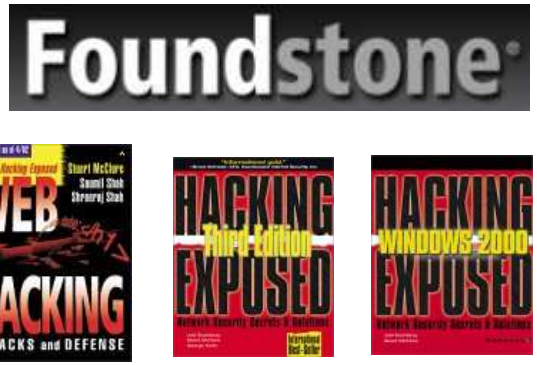
Agenda

- "Triple Play" Strategy
  - The Business Case
- IPTV Introduction
- IPTV Security
- Countermeasures
- Conclusion

Introduction

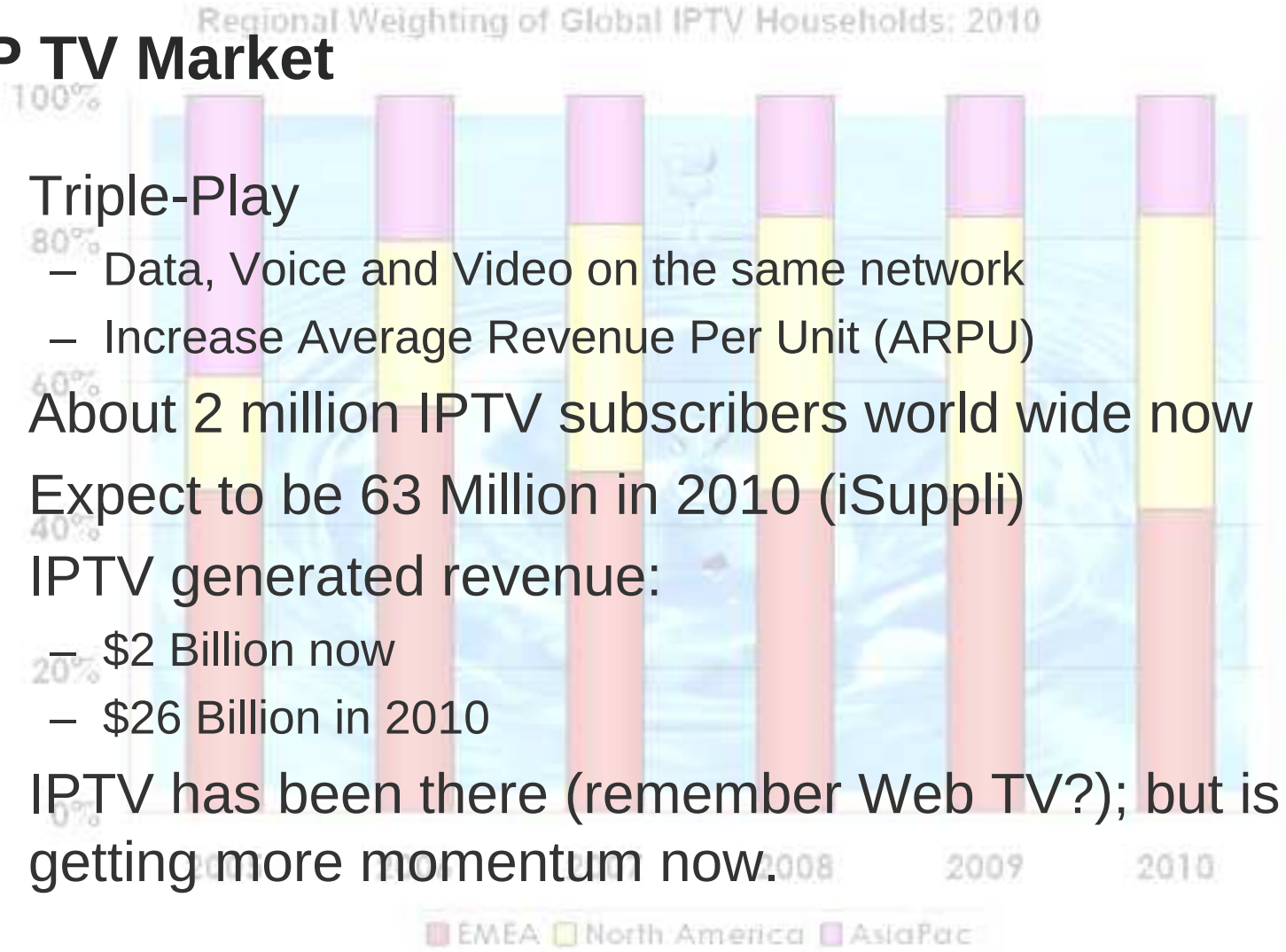
Yen-Ming Chen

- Sr. Principal Consultant
- Joined Foundstone since 2000
- Contributing author of four security books and numerous published articles.
- Master of Science in Information Networking from C.M.U.
- Provide security risk assessment from web applications to emerging technologies
- Invited speaker for HACK.LU, HITB, HIT, Pacsec.JP and others

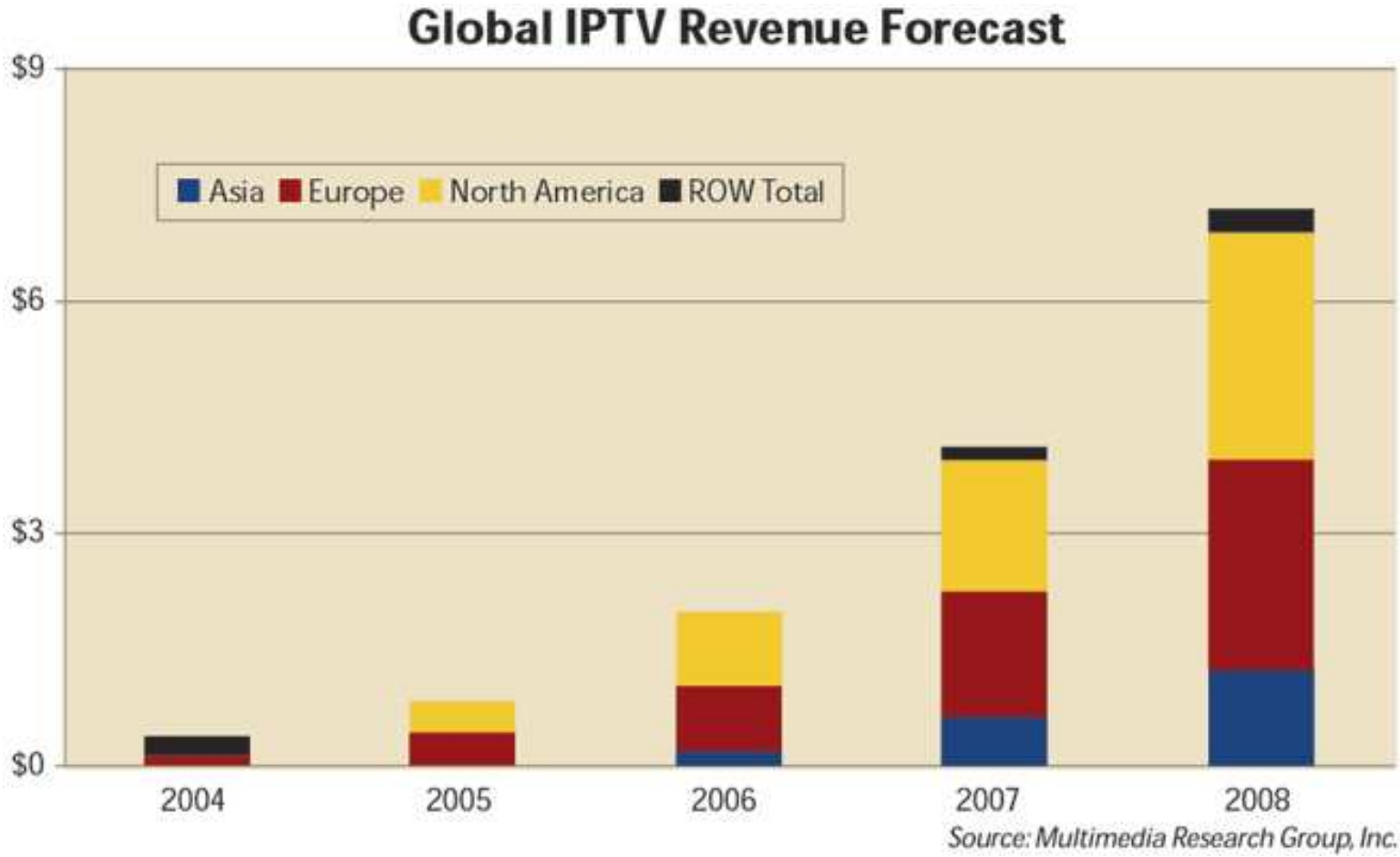


IP TV Market

- Triple-Play
  - Data, Voice and Video on the same network
  - Increase Average Revenue Per Unit (ARPU)
- About 2 million IPTV subscribers world wide now
- Expect to be 63 Million in 2010 (iSuppli)
- IPTV generated revenue:
  - $2 Billion now
  - $26 Billion in 2010
- IPTV has been there (remember Web TV?); but is getting more momentum now.



IPTV Revenue Forecast



IPTV

- Part of the “Triple-Play” strategy
  - Service provided on Telecoms’ own network
    - Easy to control quality
- Standalone service provider
  - Use the Internet as their own backbone
  - Watching TV from China in your home at London
  - P2P streaming, Web TV or RTP
- Others (short videos, lower resolution)
  - YouTube, Google Video and other vBlogs
- There are over 350 IPTV Service Providers
- 60+ different vendors
- We will focus on the first type of IPTV

Known Security Problems

- Data Service
  - Home computers are turned into Zombies
  - Phishing, Spamming and DoS
- Voice over IP
  - Conversation eavesdropping
  - Phreaking, free phone calls
  - Device insecurity
  - Denial-of-Service

IP TV Overview

- Video content offered on your broadband network
  - Subscription
  - Video-On-Demand
  - Interactive applications (web browsing, e-mail, games and others)
- Architecture
  - Content Source
  - Delivery and Management Network
  - Home Network

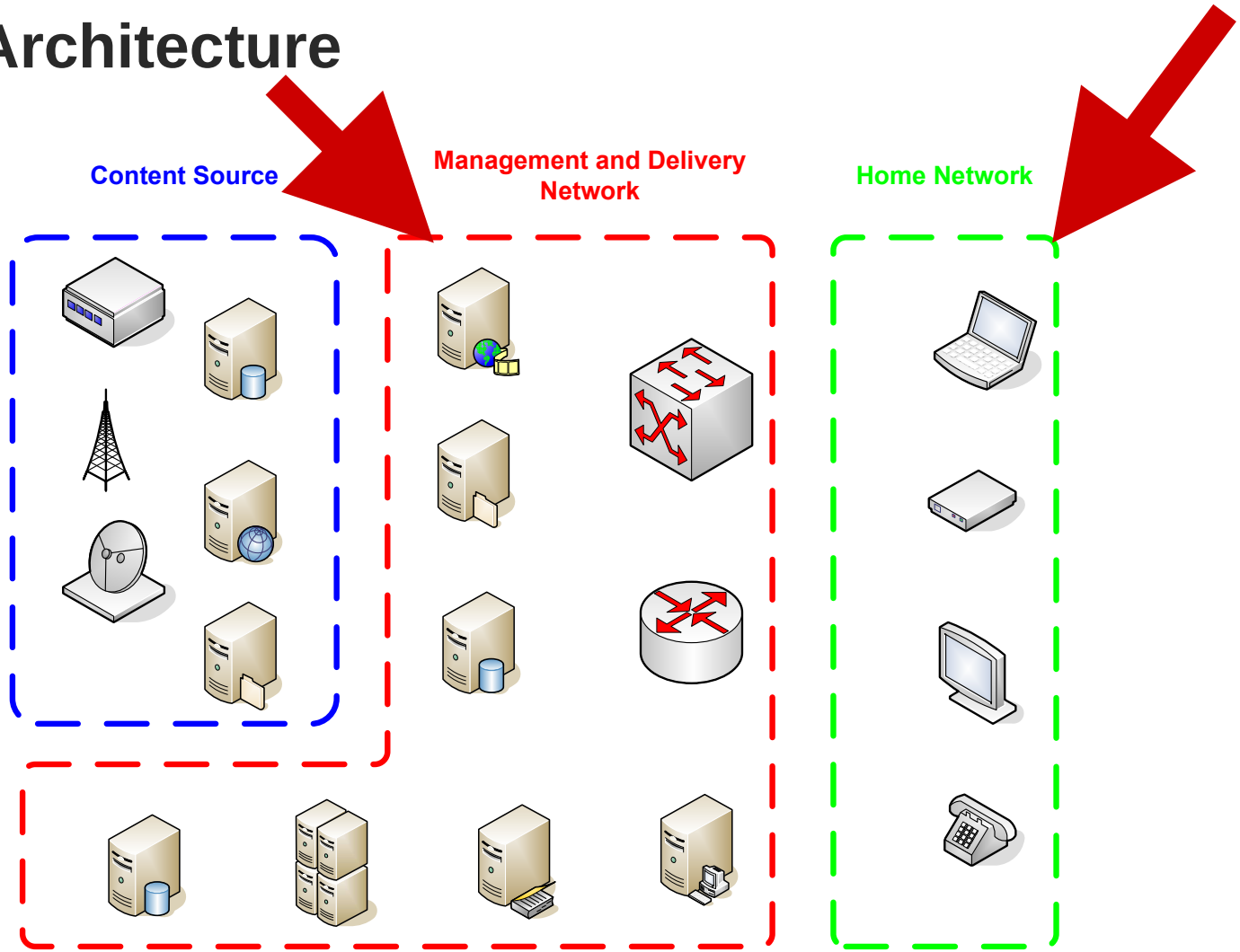
IPTV Security Testing

- A combination of:
  - Network penetration testing
  - Web application security testing
  - Device security testing
  - Software vulnerability testing
- May also include
  - Policy and procedure review

IPTV Walkthrough (Home Users)

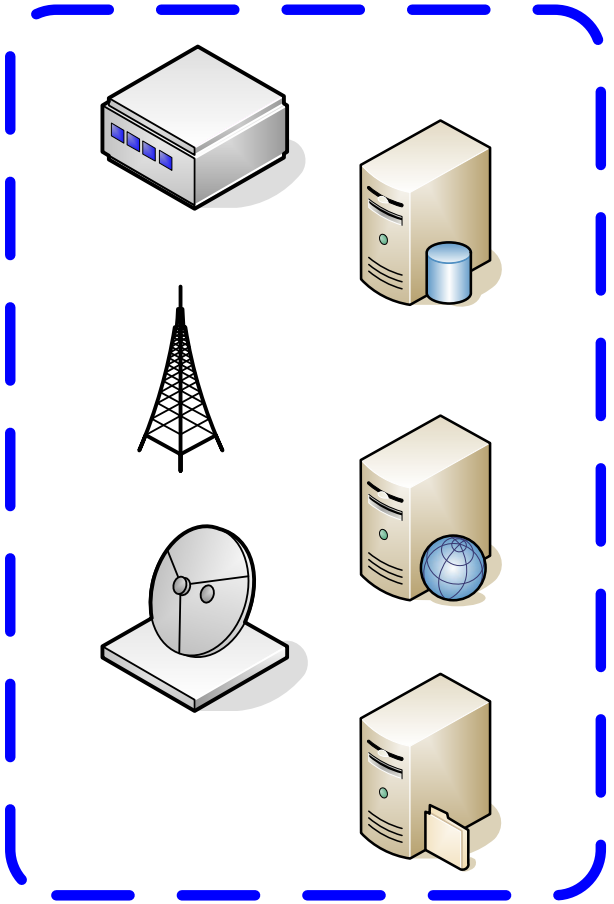
- Home gateway (if any) boots up and authenticates
- Set-Top Box boots up and authenticates
  - DHCP, TFTP or NFS to get the latest boot images
  - Authenticate with MAC, random nonce or public/private key
- Choose and watch your channel
  - IP Multicast at work (unicast sometimes to reduce delay)
  - IGMP join/leave group to change channel
- Purchase your VoD
  - Choose and purchase
- Use other interactive applications
  - If available

IPTV Architecture



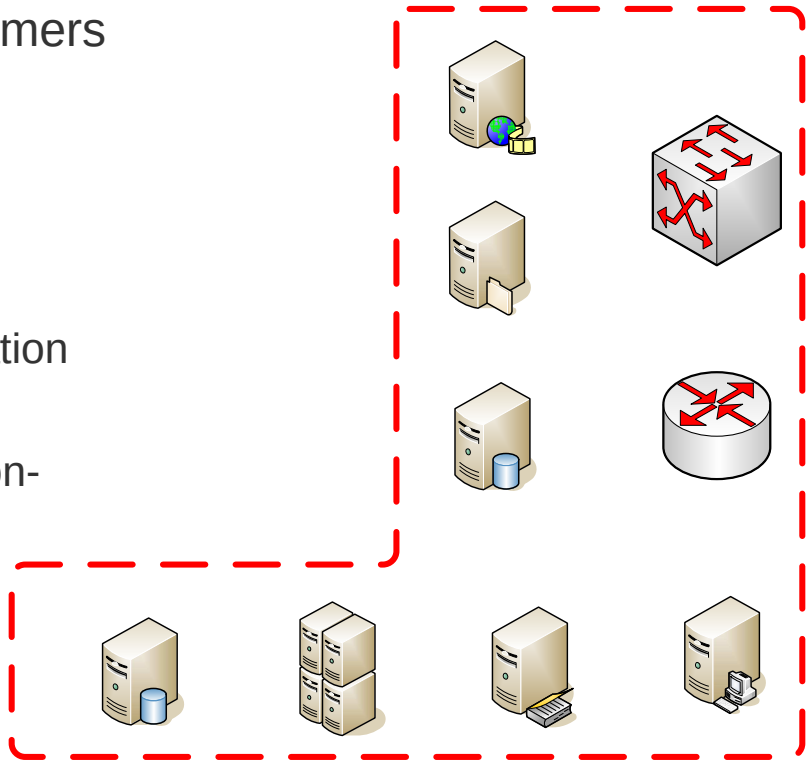
Content Source

- All devices, processes and networks that import and store video contents
- Different sources
  - Satellite
  - RF
  - Pre-recorded tapes
  - Cable
  - Others



Delivery and Management Network

- All devices and network used to deliver video through the network to customers
  - Encoding and Streaming servers
  - On-Demand servers
  - Network backbone
- Major functionalities
  - Customer authentication/authorization
  - Customer service
  - Provide video content (normal or on-demand) via
    - Multicast
    - Unicast



Home Network

- Customer Premise Equipment
  - Anything that connects to a consumer's home network
    - Computer
    - Set-Top Box
    - Home Gateway
    - Game Console
    - Phone
    - Others

Attacker's Goals

- Take control of a large amount of home networks
  - Service disruption
  - Spreading worms, trojans, virus
  - Broadcast own material (for political or other reasons)
- Steal the content
  - For piracy or as simple as P2P TV source
  - For free TV/Video

IPTV Security Problems

- Home Network
- Deliver and Management Network
- Content Source

Home Network

- Understand how authentication and authorization are done
  - As easy as spoofing MAC Address
- Security vulnerability on home network devices
  - Device management
  - Device weakness

Set-Top Box Communication

- Set-Top Box downloaded boot image from a TFTP server
- Set-Top Box register itself to a middleware server
- Set-Top Box receives channel listing, application directories (other than TV)
- IGMP Membership report
  - To indicate the current channel or join a new channel
- IGMP LeaveGroup
  - To leave a channel
- Poweroff packet

IGMP Membership Report

- Every channel takes a multicast address
- IGMP packet to stay in a channel or leave the current channel
- Set-top box has listening service to receive channel content

Device Management

- Most of the devices can be managed by SNMP or TELNET
  - telnet <set-top-box-ip> <telnet-port>
    - DSLFactoryTest> LeaveMGroup (Leave's the current multicast group)
    - DSLFactoryTest> JoinMGroup <multicast-group-address>:<mgroup-port> (Join the multicast group for another channel)
- Information transmitted in the clear
  - PIN (for parental control or VoD purchase)
  - Account number

Local Access to Device

- Plug in USB keyboard/mouse
  - Command shell access
  - Tools on the STB
  - Modify EEPROM
    - Works if the authentication uses STB MAC Address
  - Access to other information
    - DRM-related

Weak TCP/IP Stack

- Set-Top Boxes have limited memory and CPU resource.
- Using isic to test:
  - Every set-top box starts a listener service to take video traffic
  - udpsic –s <streaming_server_ip> –d <stb_ip>,<listener_port> –r 1234
  - For some set-top boxes, this is Denial-of-Service
  - Useful if you want to perform DoS on each home network from your zombies.

Other Vulnerability

- Web management interface
  - Data validation problem
  - Other standard web application issues
- Weak/default account and passwords
  - Might apply for
    - Web management interface
    - Telnet/SSH
    - SNMP

Delivery and Management Network

- Access to other servers
  - Middleware problem
  - Streaming/Encoding server problem
  - Other servers

Access to Other Servers

- Change your IP address to set-top box's IP address range, then you're on!
- Scan the network range and you may find:
  - Middleware Server
  - Database Server
  - Other Servers

What Can You Find?

- Passwords in spreadsheet or configuration files
- Web management interface for middleware server
- Database servers
- Movies for test
- And ……

Streaming and Encoding Servers

- RTSP Buffer Overflow
- Weak TCP/IP Stack

Real-Time Streaming Protocol

- RFC 2326 (www.rtsp.org)
- Used for video-on-demand server to deliver videos.
- Sample:
  - DESCRIBE
  - SETUP
  - PLAY
  - GET_PARAMETER

Buffer Overflow

- DESCRIBE rtsp://vodserver:554/mediacluster?ProviderId=company&ProviderAssetId=company00123 RTSP/1.0

- Change the URI for the DESCRIBE method to a large chunk of data, you get buffer overflow on the VoD server.
- Other location of the implementation might have the same problem
  - PROTOS for RTSP?

Weak TCP/IP Stack

- Streaming or encoding servers are good at sending data out
- They are not good at handling incoming traffic
- A nmap full-port scan could degrade the server response from 10ms to 3000ms for example.
- An aggressive scan could cause denial-of-service

Content Source

- Finding the backup
- Finding the source
- VOD Manager
  - Web management interface

IPTV Security Summary

- Privacy
- Confidentiality
- Integrity
- Availability
- Interoperability

Privacy

- How do Telecoms handle customer information?
  - Does any personal identifiable information (PII) goes through the network when you order a movie?
  - Any vulnerability on back-end billing system?
- How do Telecoms manage CPEs?
  - Customer Premise Equipments, does it belong to the customer or the service provider?
  - How about Set-Top Box and other related equipments?
  - What's the Acceptable Usage Policy?

Confidentiality

- Video Content
  - Is Digital Right Management (DRM) being used?
  - How about people stealing content directly from content source?
    - Remember all the backup tapes, laptops losses in 2005?
  - How are recorded contents protected?
    - Set-Top box as a DVR
- Authentication and Authorization
  - How does the system perform authentication and authorization?
- Other interactive applications

Integrity

- Can Content be modified?
  - Multicast and unicast security
  - Content source security
- Billing system integrity
  - Who should have access to billing system and how is internal fraud being prevented?
- Other systems on the network
  - How about their security?

Availability

- Can someone disrupt your IPTV service?
  - To what scale?
- Any of the IPTV device could be vulnerable to Denial-of-Service attack?
  - Buffer overflow
  - Weak TCP/IP or protocol stack implementation
- If other service is down (Voice and Data) would it take down IPTV too?
  - System dependencies

Interoperability

- There is currently no common standard on IPTV
  - Other than the use of multicast/unicast
  - May help security as a ‘diversity factor’
    - One vulnerability for one telecom may not work for another
- Standards on the work
  - ITU (ISO)
  - ISMA.tv
  - Others

Countermeasures

- Organization
- Policies and Processes
- Technology

Organization

- Security team from the beginning
  - Integrate with current security teams
  - Responsible for security program management
    - From planning to deployment to incident response
  - Secure deployment lifecycle
    - Evaluate, Test and Response
- Gap analysis
  - Understand security baseline at the beginning
  - Update status as new technologies are involved

Program and Procedure

- Change management procedure
  - Access control list
- Incident response program
  - Recognize
  - Response
  - Evolve
- Security evaluation program and procedure
  - Evaluate security in technology and deployment

Technology

- Product security
  - Secure SDLC
  - Security evaluation
- Deployment best practice
- Measure security impact to performance
- Monitor and management
  - How do you recognize an IPTV fraud?
- Bring security into standards

Conclusion

- IPTV has been adopted as one of the “Triple Play” strategy by Telecoms
  - Evolved into “Multi Play” in the future
  - More interactive applications planned in the future
- Risk still exist due to
  - Vulnerabilities in technology
  - Weakness in deployment
  - Incomplete or insecure processes
- Countermeasure
  - Organization, process and procedures
  - Secure deployment (mitigating technology risk)

Foundstone
Professional Services
A DIVISION OF McAFEE

PAC SEC

» Thank You

Yen-Ming Chen
Senior Principal Consultant
Yenming.Chen@Foundstone.Com