DOCKET FILE COPY ORIGINAL

WILLKIE FARR & GALLAGHER

EX PARTE OR LATE FILED

Washington, DC
New York
London
Paris

RECEIVED
MAY 22 1998
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

May 22, 1998

VIA HAND DELIVERY

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
1919 M Street, N.W., Room 222
Washington, D.C. 20554

Re: Ex Parte Notice, CS Docket No. 97-80
(Commercial Availability of MVPD Navigation Devices)

Dear Ms. Salas:

This letter provides notice that on May 21, 1998, the following people met in connection with the above-captioned proceeding:

Quincy Rodgers, Vice President, Government Affairs, General Instrument Corporation ("GI")
Chris Crafton, Director, Industry Affairs, GI
Dave Robinson, Senior Vice President & General Manager, Digital Network Systems, GI
Mark DePietro, Director Systems Engineering Digital Network Systems, GI
Jeff Krauss, Consultant to GI
The undersigned

Anita Walgren, Legal Advisor, Commissioner Ness
Dale Hatfield, Chief, Office of Engineering and Technology
Bill Johnson, Deputy Bureau Chief, Cable Services Bureau,
Karen Kornbluh, Deputy Chief, Mass Media Bureau
Michael Lance, Deputy Division Chief, Cable Services Bureau

Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20036-3384
202 328 8000

Telex: RCA 229800
WU 89-2762
Fax: 202 887 8979

0062651.01

No. of Copies rec'd 0+2
List A B C D E

Jonathan D. Levy, Senior Economist, Office of Plans & Policy
Alan Stillwell, Industry Economist, Office of Engineering and Technology
Stan Trost, IEEE Fellow, Office of Plans & Policy

Miles M. Circo, Senior Vice President and Chief Technical Officer, Divx
David Goldschlag, Manager, Security Systems, Divx
Robert Schwartz, Attorney, McDermott, Will & Emery

The discussion focused on the superior nature of embedded security over separate security in MVPD navigation devices. The attached document was provided to Commission staff during the meeting and should be included in the record in the above-captioned proceeding.

Kindly direct any questions about this matter to the undersigned.

Thank you.

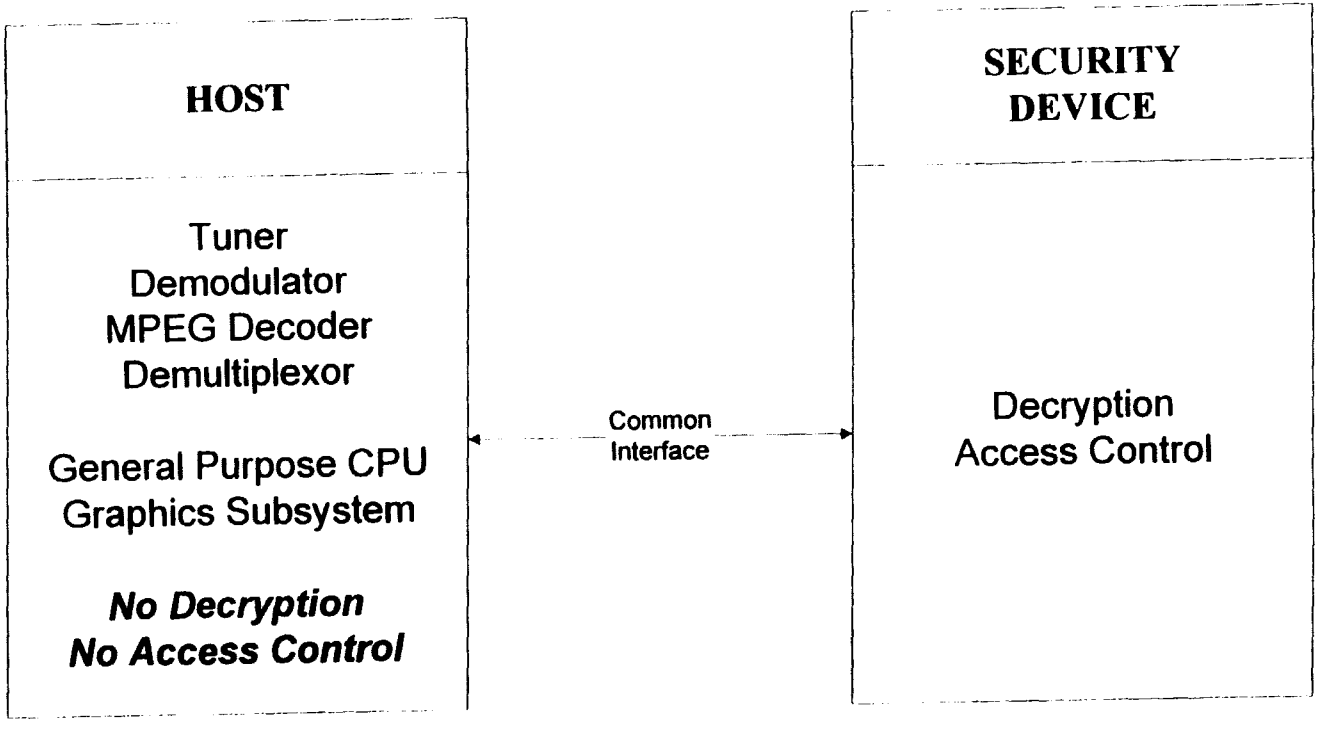
Sincerely,

Francis M. Buono

cc: Above-named parties

Attachment

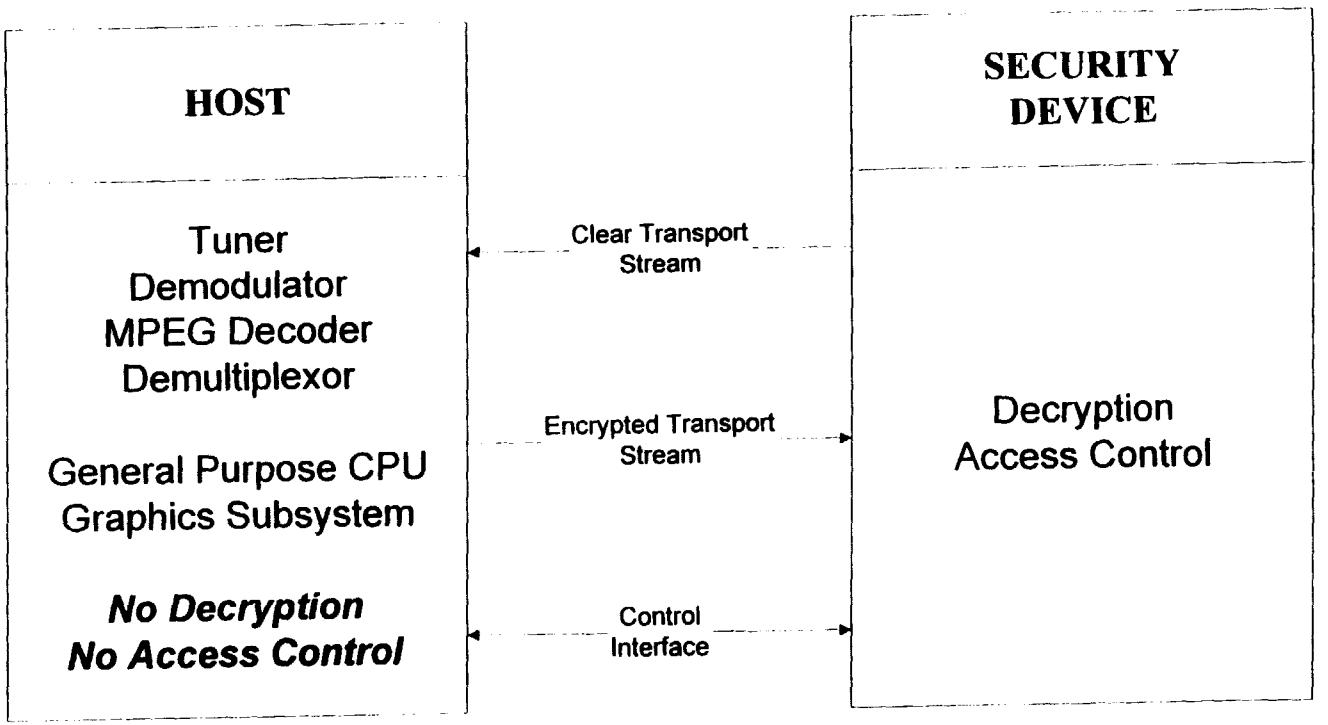
Pure Separation Model



980521-01

Pure Separation Model: Conceptual View

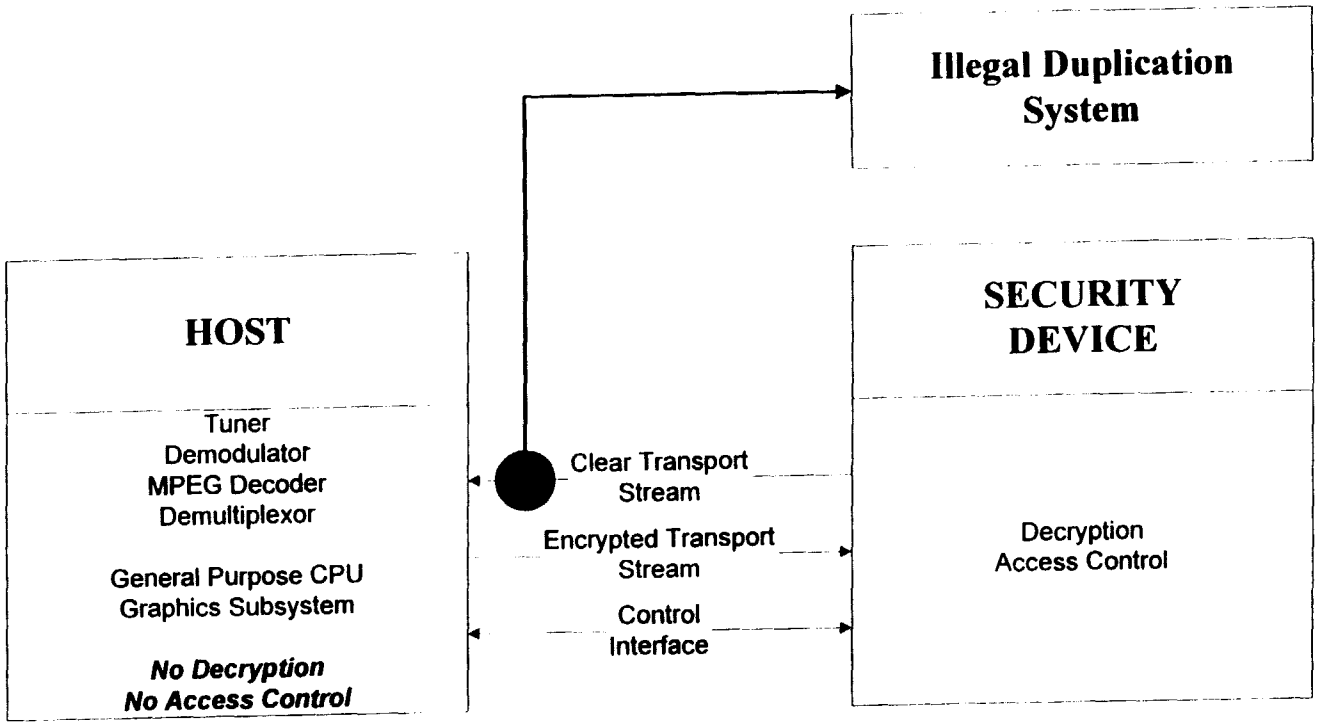
Pure Separation Model : Interfaces



Pure Separation Model: Common Interface Defined

980521-02

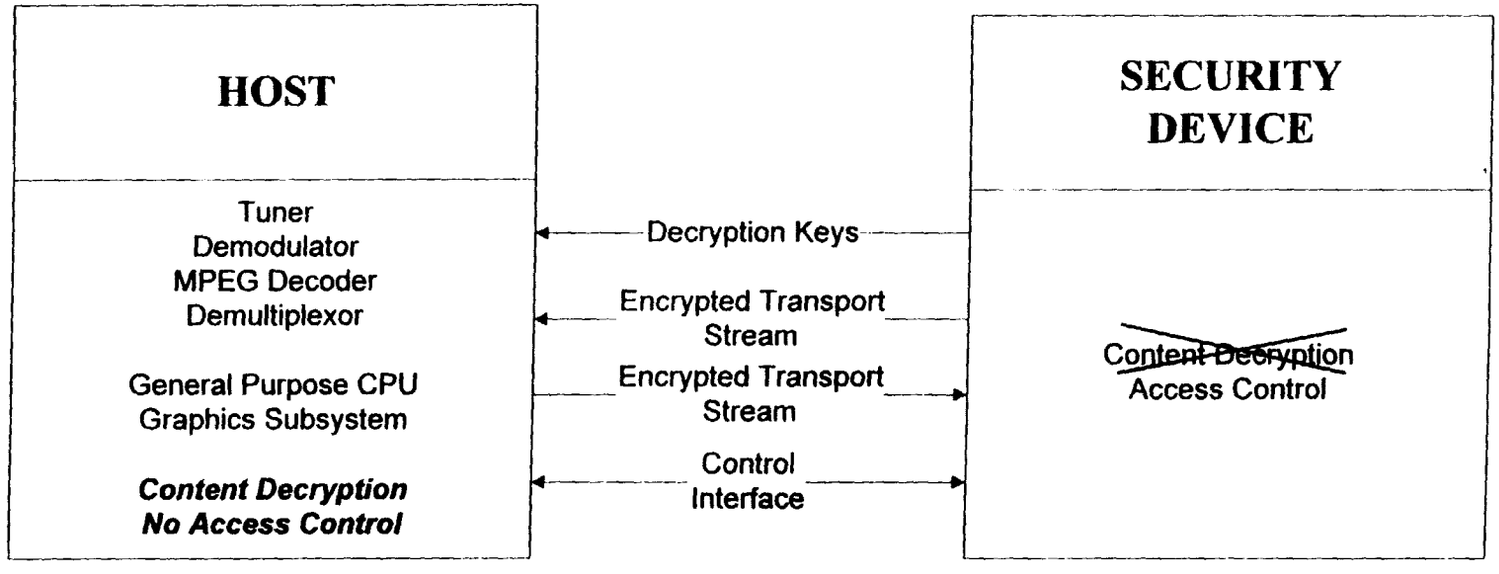
Attack For Pure Separation Model



980521 03

Pure Separation Model: Obvious Point of Attack

Modified Separation Model Makes Duplication Harder



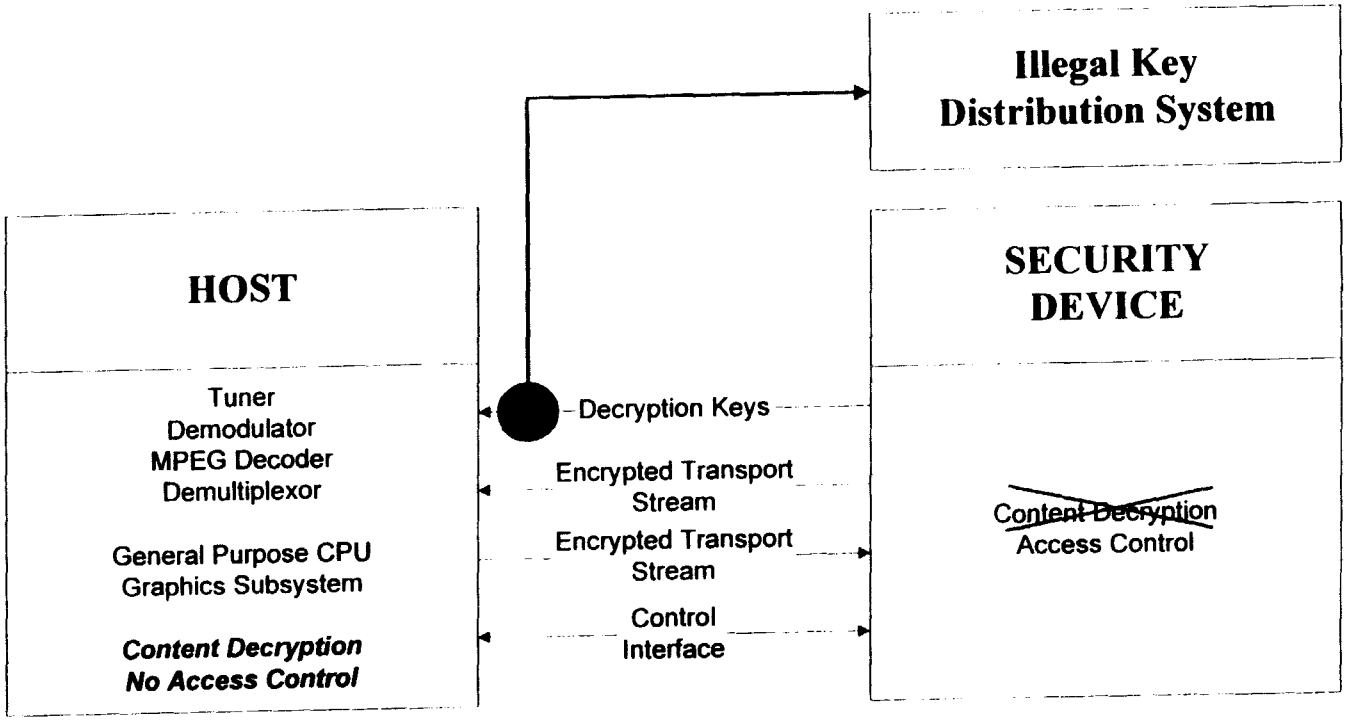
"Modified Separation" Model: Content Decryption in Host
This includes embedded security functions in Host !

980521-04

Immediate Conclusions

- Pure Separation Does Not Work
- Some Security Functions Must Be Embedded in Host

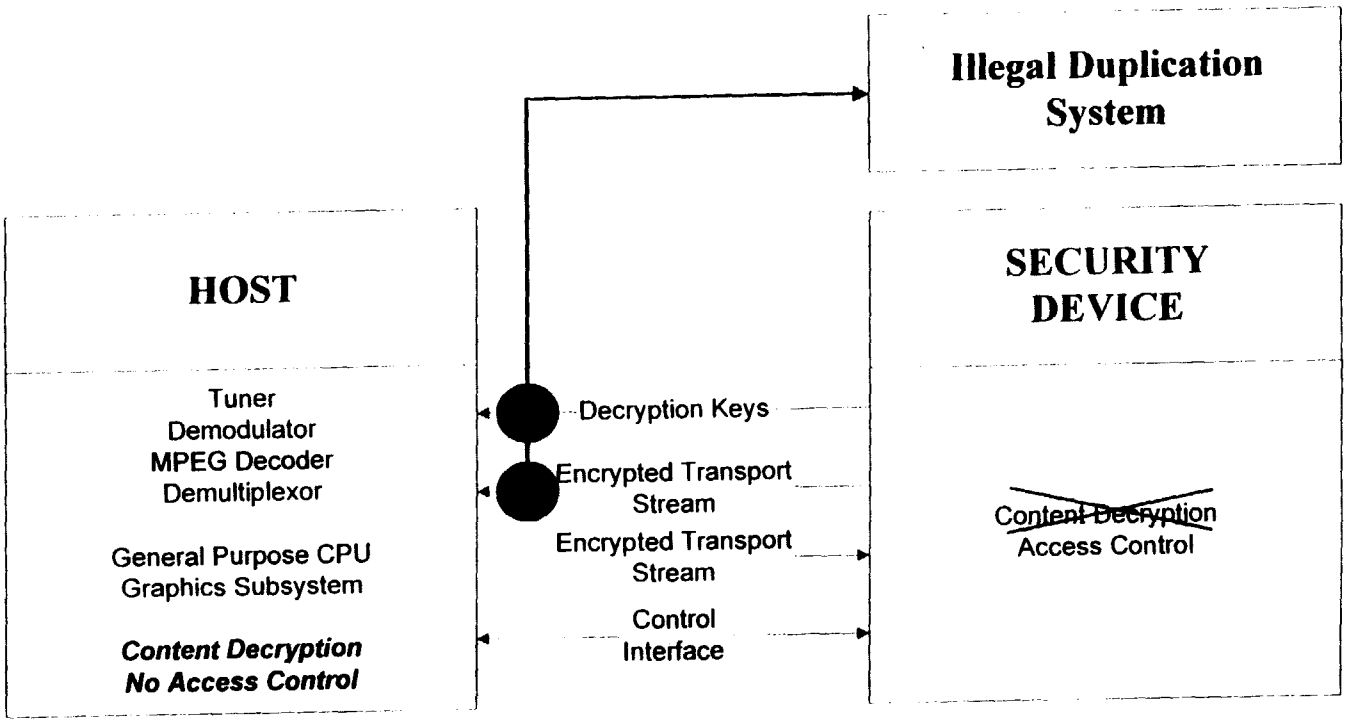
Modified Separation Model Attack Scenario 1



980521-05

"Modified Separation Model": One Possible Attack

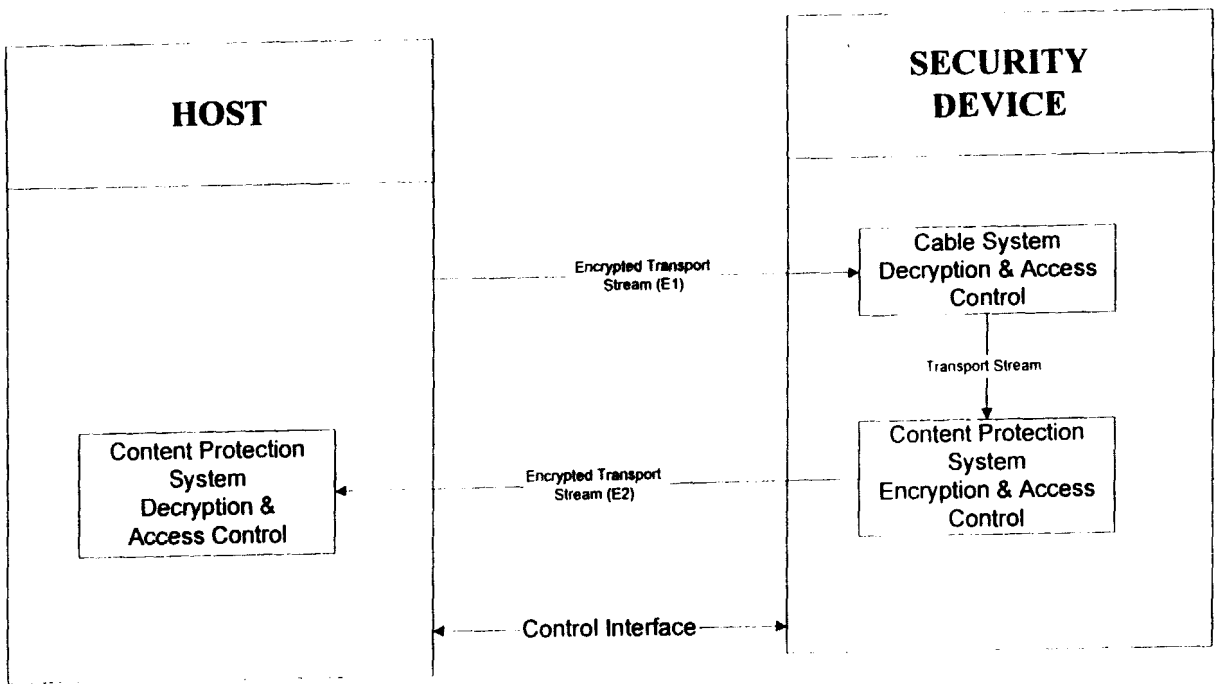
Modified Separation Model Attack Scenario 2



980521-06

"Modified Separation Model": Another Possible Attack

Final Separation Model



"Final Separation Model" : Two Encryption / Access Control Systems
Consistent With POD Model
Requires Embedded Security in Host &
Two Security Systems in Security Device

980521-07

Integration : More Is Better

- Trend: Continuously Increase Level of Integration
  - Lowers Cost for Maufacturer
  - Lowers Price for Ultimate Consumer

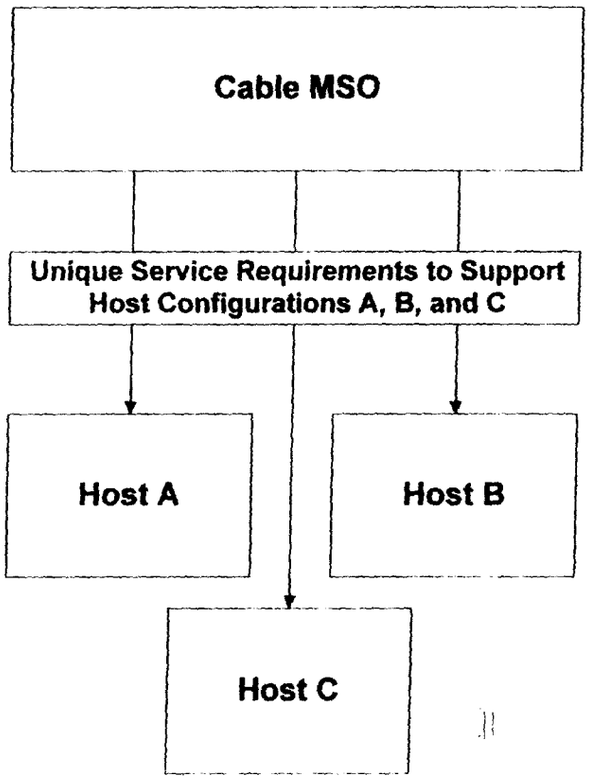
Conclusion For Final Separation Model

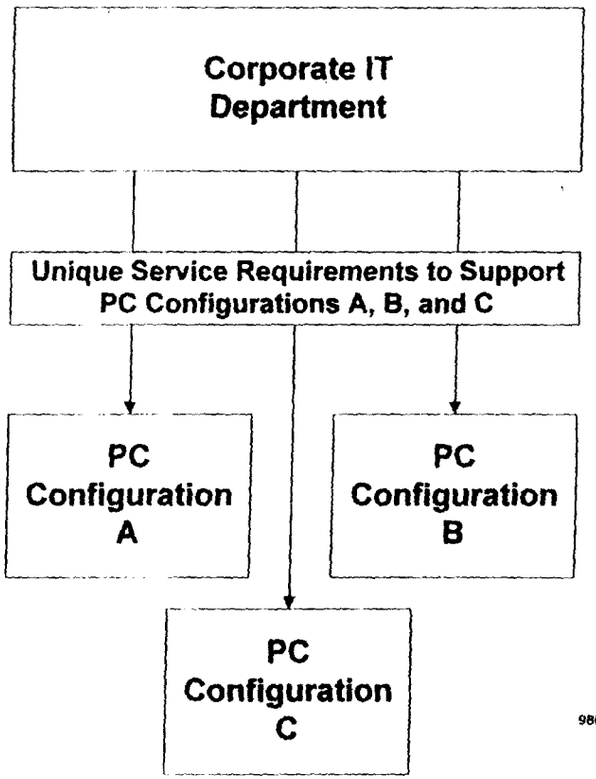
- Embedded Security is Needed in the Host
- Since it is needed
  - It can be used for the initial cable system security function
  - Use the security system standard interface to facilitate upgrades

Conclusions

- Any Adopted Rule Should Not:
  - Hurt MSO's ability to innovate & provide consistent quality of service
  - Make User-Experience Based Service Differentiation More Difficult
  - Outlaw Architecture Adopted by Opencable POD Initiative

MSO's Job : Comparable to a Corporate IT Department





980521-08

MSO Desire to Differentiate Based on the Entire User Experience

- User Experience
  - Look and Feel of Menus
  - Ease of Navigation
  - Features Supported in Program Guide & Native Application
- Translates into need to specify
  - Processor Horsepower
  - Graphics System Capabilities
  - Resident Application Capabilities

Authentication : Necessary But Insufficient

- For Copy Protection
  - Communicants Must Be Able To Autheticate Each other AND
  - Communication Must Be Able to Be Validated with Respect to Access Control List
- Access Control List
  - Defines Universe of Legal Communicants
  - Is Adminstered Outside of the Set Top domain

Typical Uses of OOB Channel

- Code Downloads
- EPG Data & Code Feeds
- VCR IR Code Database Downloads
- Cable System Channel Maps
- Control System Poll Requests
- Personal Text Messages
- Emergency Alert Messages
- Entitlement Management Messages
- Media Access Control
- Interactive Data Services
- System Time Delivery

OOB Channel Notes

- OOB Is Not Only Mechanism to Deliver Services
- Inband Systems Are Also Possible
  - Popular with Wireless Operators
- Tradeoff Between Inband & OOB System Design Based On
  - Existence of Analog Channels
    - OOB Design More Convenient Here
  - Number of Digital Channels
    - With Large Number, Aggregate Bandwidth of OOB Becomes More Economical