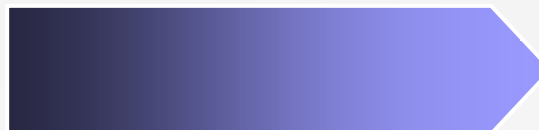
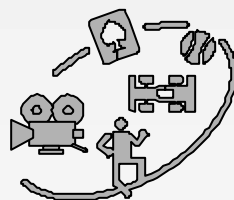


July 18th CPTWG Meeting

-

Securing IPTV

Arnaud Robert, PhD
NagraVision – Kudelski group
arnaud.robert@nagra.com



IPTV
Security requirements
Security solutions
NagraVision's solution
Conclusions

- **Businesses**

- PayTV
 - Physical access
 - Secured transactions

- **Staff**

- Kuldeski Group: 1000
 - NagraVision: 500

- **Deployments**

- Over 25 million STB equipped with NagraVision CA

- **Customer base**

- Over 30 operators
 - Echostar, NTL, ExpressVu, Telewest, Honk Kong cable, Via Digital

- **Success factors**

- Smart card technology
 - Security management
 - Open, flexible solution
 - Relation to partners (50+)

- **Slowing factors**

 - Quality: bandwidth, QoS

 - Untrusted end device

 - Operators struggle with business model

- **Success factors**

 - “one protocol, any network”

 - Inherent two-way communication

 - Successful streaming video on Internet: news, sports, adult

 - Existing IPTV trials

- **IPTV is around the corner**

 - **Content owners, CE vendors and operators must agree on content usage ruling, before it gets imposed by others... legislation, Kazaa**

IPTV – need for security ?

- **Digital content**

 - Easy to distribute [Napster, Kazaa]

 - MPEG-4 = smaller file sizes

 - Content type: premium, paying [adult],

- **Attacks**

 - Brute force

 - Usual system attacks

 - Tailored IP attacks: sniffing, spoofing, man-in-the-middle, etc

 - And many, many more

- **Protect revenues for content owners**

 - Wide distribution of content can be dramatic

 - Ex: DVD zones, Harry Potter, etc

- **Protect business for operators**

 - High value content requires security

 - Reliable, secured transaction reporting is essential

- **Trust of delivery chain ?**

 - Aggregators, Operators, Networks, end device, subscriber

 - Superdistribution

IPTV – what security level?

- **Network dependent**

Cable vs satellite vs xDSL vs FTTH
Protocol – DVB, ATSC, IP

- **CPE dependent**

Can not achieve same security on open / closed platforms
CPE has connection to a home network ?

- **Content value dependent**

Which content – premium, live events, scheduled
What release time – box office, PPV, PayTV, Blockbuster
What quality – MPEG-2, VHS

- **“DSL is a closed network ... it only requires authentication”**

Authentication can be achieved rather securely: TRUE

That is sufficient for secure content delivery: WRONG.

DSL is a point to point network, but PPP & IP are open protocols

It does not prevent IP stack attacks

It does not prevent non-repudiation and similar system attacks

It does not achieve copy protection

BTW, aren't cable or satellite (closed networks) hacked ?

- **What are the main building blocks ?**

- Authentication
- Encryption
- Copy protection
- Non repudiation

- **Checklist when selecting solution**

- Track record
- Flexible
- Persistent protection
- Upgradeable AND renewable

- **SSL**

- Used for securing small data [bank]
 - Link encryption only – no copy protection
 - Fits only small size data (requires large CPU, memory)
 - Based on RSA – asymmetrical, hence slow

- **IPsec**

- Link encryption only – no copy protection
 - Complex solution - combination of security bits & parts
 - AH protocol not secure.
 - Transport mode not secure.
 - Key management is ... up to the operator
 - Creates data expansion
 - Flaws yet unanswered (thus not a std)
 - Requires IPsec compliant devices (routers, etc)
 - Analysis by security experts – not a good grade ...

- **VPNs**

- Based on IPsec
 - Aimed at controlling authorization, more than persistent content protection

- **Comes from the Internet**

- Born for music (mp3, documents) in Internet world, 1992
 - Most vendors disappeared
 - Broadcast ≠ physical medium protection (DVD, etc)

- **DRM is a subset of conditional access**

- It's "CA" for file downloads

- **Security weaknesses**

- No track record, no deployed system
 - No rotating keys but static keys
 - No unique session encryption
 - Key management is undefined, thus depends on implementation ...

- **Legal issues**

- Most patents are battled for
 - Many could be discussed by CA vendors

- **It allows for superdistribution**

- DRM was designed for peer-to-peer distribution ...
 - Do you want this?

- **Limitations**

- Requires complete new head end architecture
- Requires interoperability between systems [failure today...]
- Not scalable
- No real time encryption [live, streaming]
- No multicast
- Limited to file downloads
- Never integrated with STBs

- **Superdistribution**

- Complex AND requires complete interoperability
- License servers are overloaded with requests
- No established trust between owners and back office
- Never deployed and tested in large scale

Although tempting, will subscribers really use it and pay for BW?
Owners, aggregators loose control of your content
Bypasses one of PayTV's fundamental business laws
"operators own their subscribers"

- **Security requirements**

 - Conditional access

 - + Copy protection

 - + tamper resistance

 - = persistent protection

- **STB**

 - Mainly analog copy protection

- **PVR**

 - Personalized ECMs

 - Updateable access rights

 - Secured path between S/C and descrambler

 - Tamper resistance + evidence

 - Fingerprinting, watermarking

- **Home gateway**

 - Combination of copy protection for PVR & STB

 - Every device must have conditional access

 - Interoperability

 - SmartRight

- **NagraVision carries on DVB/ATSC protection into IP**
- **References**
Track record, trusted solution, experience
- **Adapted solution – not IPsec reviewed**
Working with the right partners – Widevine, Wave
Conditional access for new networks / new attacks
Smart real time encryption
- **Security aspects**
Fundamentally cryptographically secured
Key management
Upgradeable + renewable
Persistent protection
Tamper resistance, evidence
Watermarking

- **Use of EMM, ECM**

- Proven key management model
 - In band delivery

- **End device**

- Adapted CA kernel

- Copy protection:

- Personalized ECMs

- Updateable access rights

- Tamper resistance [Widevine]

- Tamper evidence [Widevine]

- Secured saved content [Wave]

- **Pairing**

- Dynamic pairing between S/C and STB

- S/C locator [S/C, MAC address, IP address]

What security will guarantee the same business in the IPTV food chain?

A. untested, un-adapted, "promising", yet to be solutions that do not offer copy protection mechanisms, and that require rethinking the entire business + value chain?

B. Existing, trusted, adapted solution that serve persistent protection

C. No need for track record persistent protection. And risk "Kazaa" steals your business

- **IPTV facts**

IPTV is around the corner. Can't ignore it.
Owners, CE vendors must agree on scheme ... now!

- **Security**

Ensures the business – for owners and operators
Persistent protection is key
Closed networks are NOT secured as such
Real IPCAS is the only available solution ... today!

- **First shot may be only shot [Napster] ... do it now!**

- **Why rethink the entire business, and wait, when known solutions are available today ?**

Questions

- arnaud.robert@nagra.com
- www.nagra.com