DVB®

Protecting DVB broadcasts from hackers

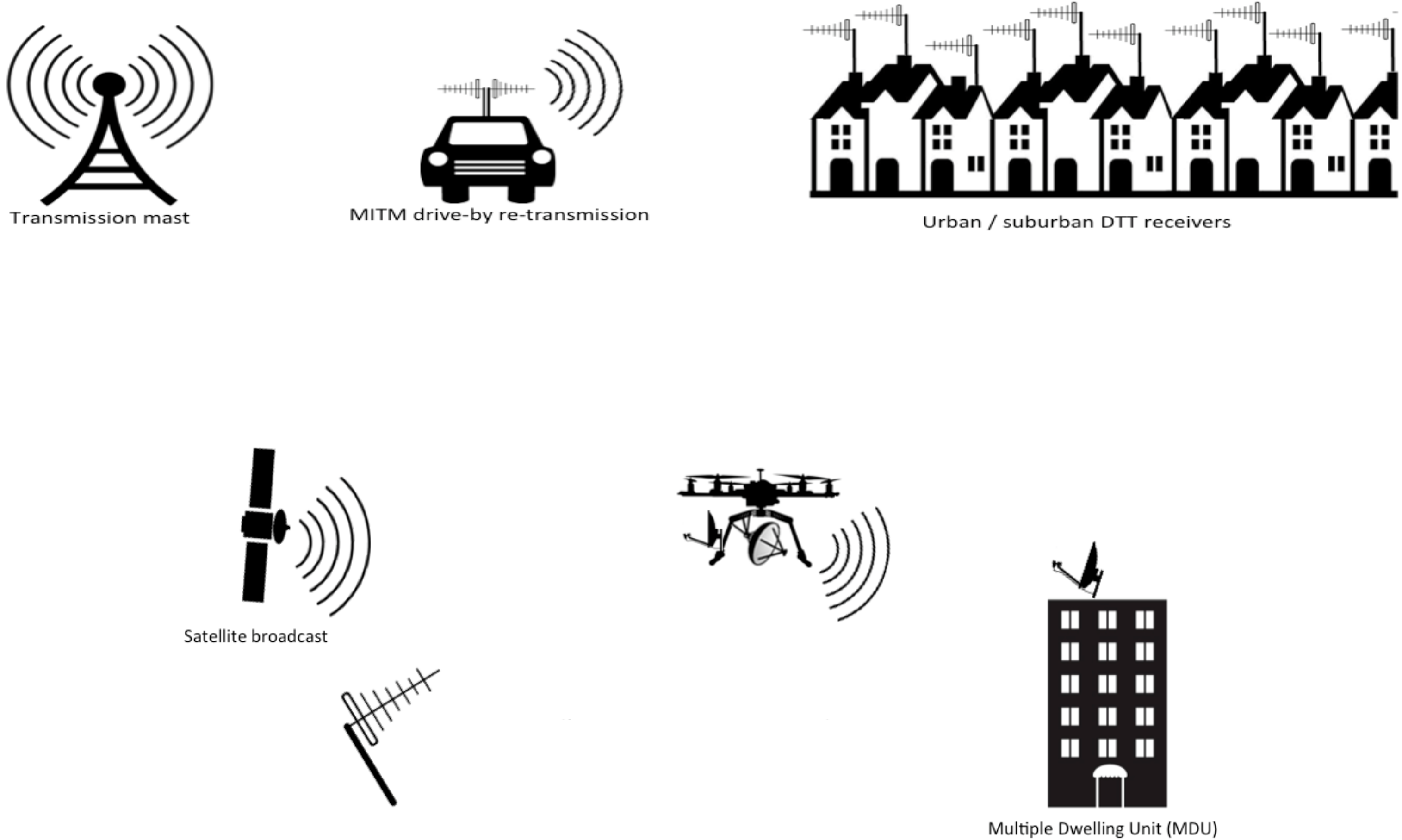
Using TS 102 809 1.3.1

Jon Piesing
Chair DVB TM-MIS and
Chairman-elect DVB Technical Module

What is the Problem?

- TV signals can include interactive components that cause applications to run automatically when a channel is selected.
- An attacker can modify a broadcast to introduce their own applications.
- If there is a vulnerability in the TV receiver then the attacker may be able to take control of the receiver.

Two Example TV Attack Scenarios



Transmission mast

MITM drive-by re-transmission

Urban / suburban DTT receivers

Satellite broadcast

Multiple Dwelling Unit (MDU)

Why is it Relevant Now?

- Attacks via broadcast have been discussed for at least 15 years
  - Initially called “man in a van attack”
- Security researchers have brought analysis of vulnerabilities to the attention of TV organisations
  - In particular Ben Michéle at TU-Berlin spent significant time with DVB and HbbTV and motivated the start of the DVB specification work
- Several things have changed in the last few years
  - Price and size of DVB-T modulators has fallen
    - E.g. UT-100C for US$170 - $230
  - Price & size of equipment to modify streams has fallen
    - Can now be done in software on a Raspberry Pi
  - TV sets now use commodity software
    - Exploits for bugs in open source software (e.g. libraries and/or browsers) can be aimed at TVs
  - TVs have become the centre of networked home entertainment and offer much more possibilities for attackers

How Many People Might an Attack Reach?

- Densely populated urban area might have up to 5900 people per square km
  - Mobile attack with 60m radius would therefore cover 67 people or 29 households
- Degree of success depends on proportion of TVs that are:
  - Both smart (i.e. connectable) and actually connected
  - In use at the time
  - Tuned to a channel on which the attack is happening
  - Vulnerable to the exploit(s) selected by the attacker
- Making assumptions and multiplying these out suggest 30 attacks might be needed to get a single victim

Source: DVB CM-SEG calculation based on publicly available statistics

Why is this a Problem?

- The stakeholders need to protect the consumer and consumer confidence
- Potential for reputational damage to receiver manufacturers
- Potential to make consumers afraid of buying/connecting advanced receivers:
  - Reduces perceived value of advanced receivers
  - Reduces audience for internet delivered services

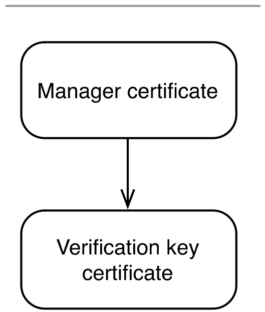
Basic Principle of Solution

- Each service carries all the information needed to authenticate its interactive components
  - Makes things easy for re-multiplexing
  - Avoids complex operational relationships between competing broadcasters
- No need to include root of trust in TV / STB
  - Trust is derived from the broadcast
  - Signalling becomes trusted based on either
    - Persistence in the broadcast over time or
    - Authentication by previously trusted signalling
- Works with a unidirectional TV broadcast
- Also optional “coordinating entity” mode with root of trust included in TV / STB

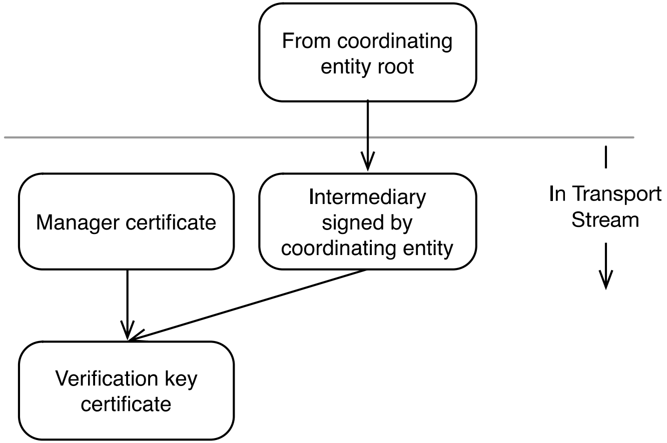
Establishing Trust: Two schemes

- Stand alone mode
  - Basic mode supported by all implementations
  - Relies on persistence of certificate signalling in the broadcast
- Coordinating entity mode (optional)
  - Uses a certificate pre-installed in the receiver
  - Requires coordinated effort within a market

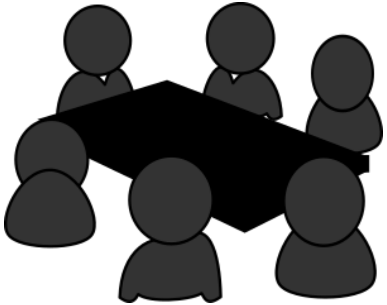
Stand alone only



Stand alone + Coordinating Entity


From coordinating entity root
Manager certificate
Intermediary signed by coordinating entity
In Transport Stream
Verification key certificate

Market stakeholders



Choose the Trust Establishment scheme most suitable for your market or region.

- If service providers are autonomous with no way of organising a common trust anchor and controlled certificate hierarchy, then the standalone method can be deployed.
- Alternatively, if service providers are used to working together they can provide trust anchors to devices and coordinate a trust hierarchy, broadcasters may use a dual hierarchy utilising both the coordinated trust anchor and stand alone mode.

Even where there is only partial coverage of the protection there is a benefit to the market as whole as the attack surface is reduced compared to no deployment

=> Analogous to vaccination – some protection is better than none

Summary

- Market stakeholders should discuss:
  - Do they want to authenticate broadcasts in their market
  - How can authentication work in their market (trust establishment, proportion of services that will be authenticated etc.)
  - How to achieve inter-operability, particularly:
    - Device response to new service
    - Device response to service trust updates
    - Sample transport streams
  - How to achieve conformance in their market

- Services/broadcasters can start operating using the stand-alone scheme independently
  - Can migrate to using a coordinating entity later

More Information

- For more information, see
  - https://www.dvb.org/resources/public/events/dvb_mitm_webinar.pdf and
- Webinar
  - https://goo.gl/2vCTHx

Thank you