Protecting DVB broadcasts from hackers

Using TS 102 809 1.3.1

Webinar
9 May 2017

Overview

- The problem
  - Robert Esterer (IRT robert.esterer@irt.de)
- The DVB Solution
  - Nick Birch (S&T nick.birch@s-and-t.com)
- How to secure your market!
  - Nigel Earnshaw (BBC R&D nigel.earnshaw@rd.bbc.co.uk)

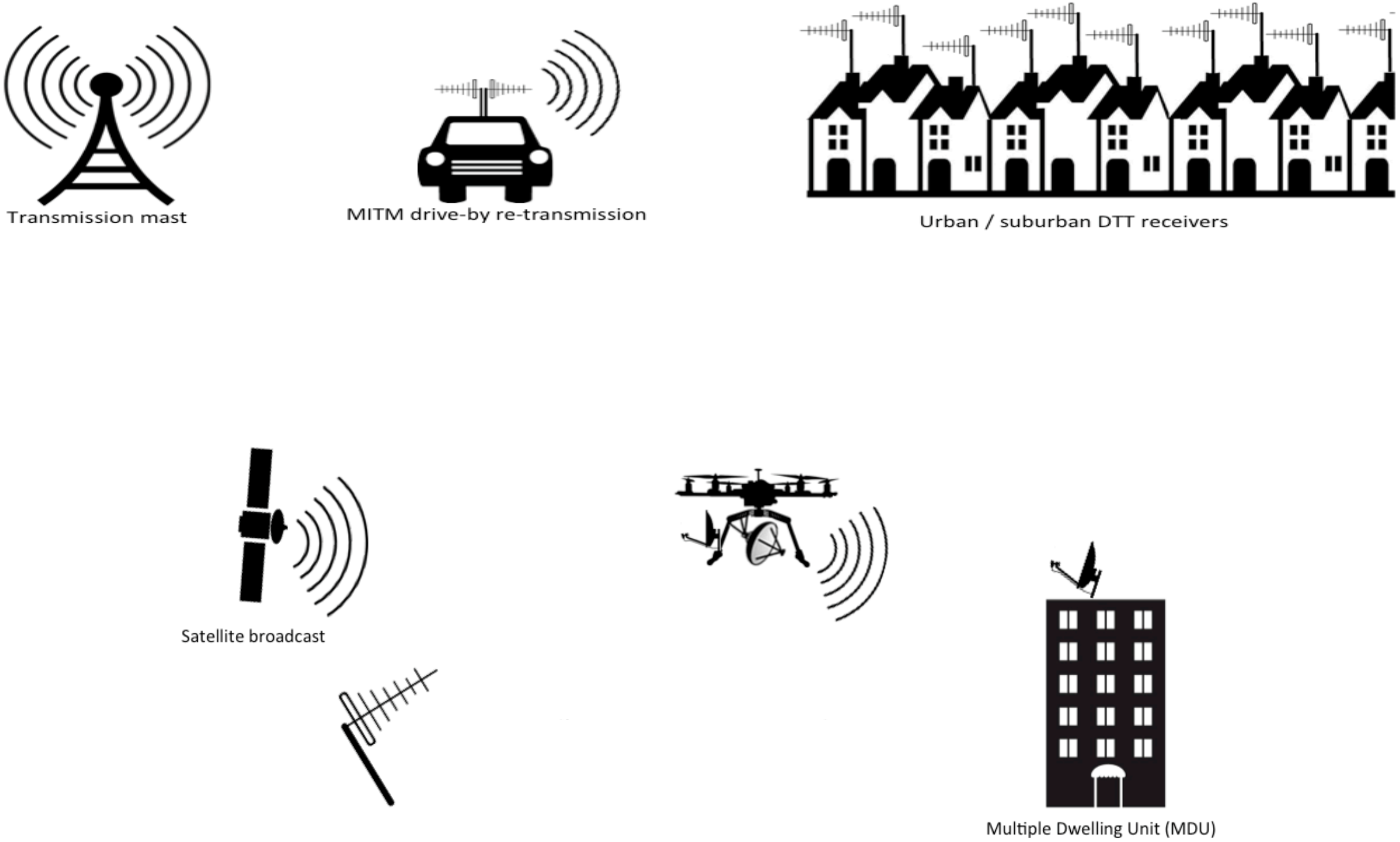
The problem

Robert Esterer
(IRT robert.esterer@irt.de)

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

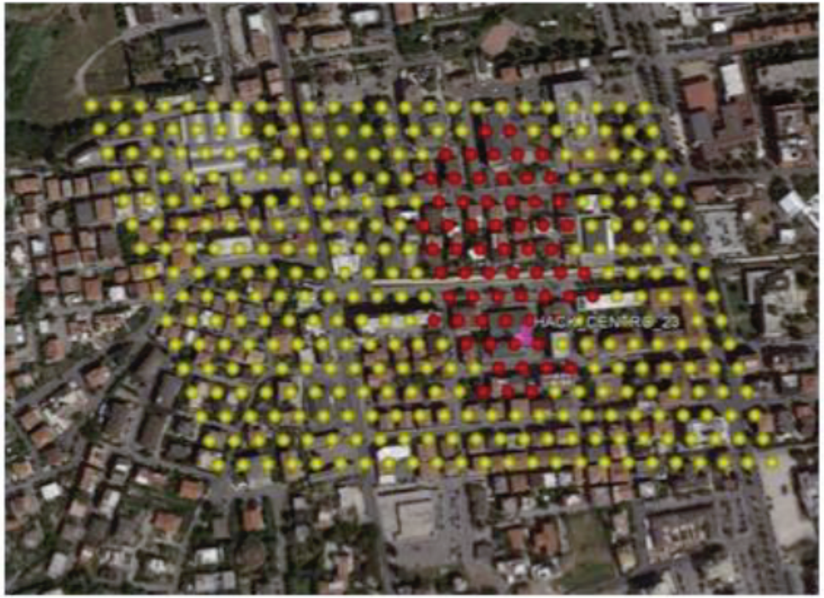

Transmission mast
MITM drive-by re-transmission
Urban / suburban DTT receivers
Satellite broadcast
Multiple Dwelling Unit (MDU)

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

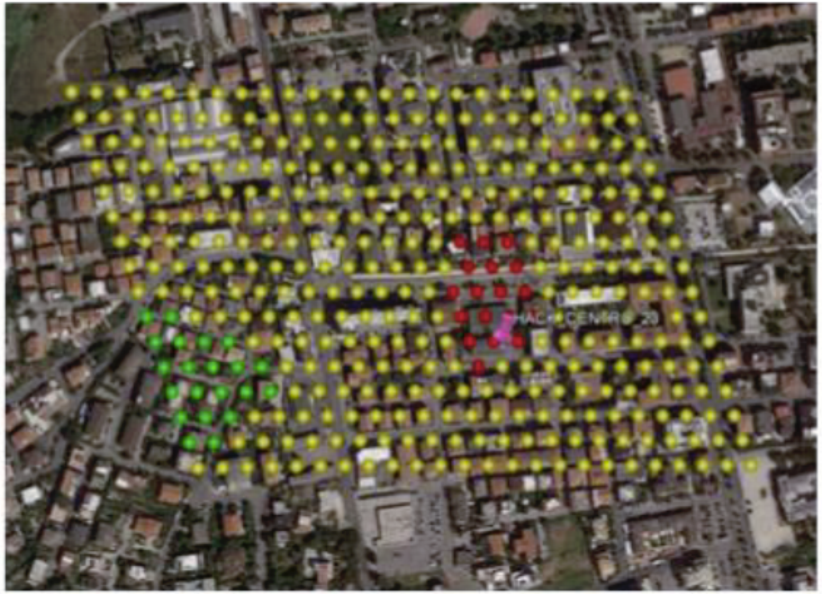
Affected and "Mush" Area

Signal level, DTT Rx: -60 dBm



Grid step = 21m

Signal level, DTT Rx: -50 dBm



Grid step = 21m

Rai - Centro Ricerche e Innovazione Tecnologica

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

What could happen?

Examples from the Real World

Example 1: The Stagefright vulnerability

- An Android vulnerability first discovered on July 27, 2015
- It had existed for over 5 years before it was discovered and affects devices from Android version 2.2 through 5.1 (2010 – 2015).
  - A second vulnerability (called Stagefright 2.0) was discovered on October 1, 2015 which affected Android versions 1.5 through 5.1
- Affected devices from all manufacturers and from all countries, including alternate OSs like CyanogenMod
  - It was estimated that over one billion devices have been vulnerable

- The original Stagefright vulnerability was in an Android library that processed video files
  - This library was also used when processing videos contained in MMS
  - Many messaging apps like Google Hangouts automatically processed any incoming message, including any videos they contain
  - This allowed attackers to automatically execute malicious code on android devices

- The second vulnerability was in the Android Mediaserver
  - Could be triggered with manipulated MP3 and MP4 files

Example 2: Weeping Angel hack

- Details from a secret government document from 2014 which was leaked by Wikileaks in March 2017
- The hack specifically targeted Samsung's F8000 series TVs released in 2013
  - It was successfully tested on TVs running firmware versions 1111, 1112, and 1116
  - Because the document is from 2014, no information about any future versions is available
- Permanently installed malware that could put the TV in a fake sleep mode in which camera and microphone still worked
  - SmartTV effectively turned into a surveillance device
- Could also extract the WiFi (WPA) password
  - SmartTV as bridgehead into the private network

On the reality of the threat

- SmartTVs offer a multitude of features which are provided by an ever increasing number of software libraries, each of which might contain a flaw
- Manufacturer independent operating systems like AndroidTV offer the possibility of exploits that work across devices from different manufacturers
- The concrete interest of intelligence agencies in hacking SmartTVs shows that there is gain in doing so

The need for being proactive

- The Stagefright exploit showed not only that exploits can exists in multi-year old components, but also that it is often impractical for manufacturers to patch such devices
- It is therefore necessary to pro-actively take measures to protect devices from receiving malicious applications to protect against vulnerabilities that have not yet been discovered

Questions?

The DVB Solution

Nick Birch
(S&T nick.birch@s-and-t.com)

Solution Provided by DVB

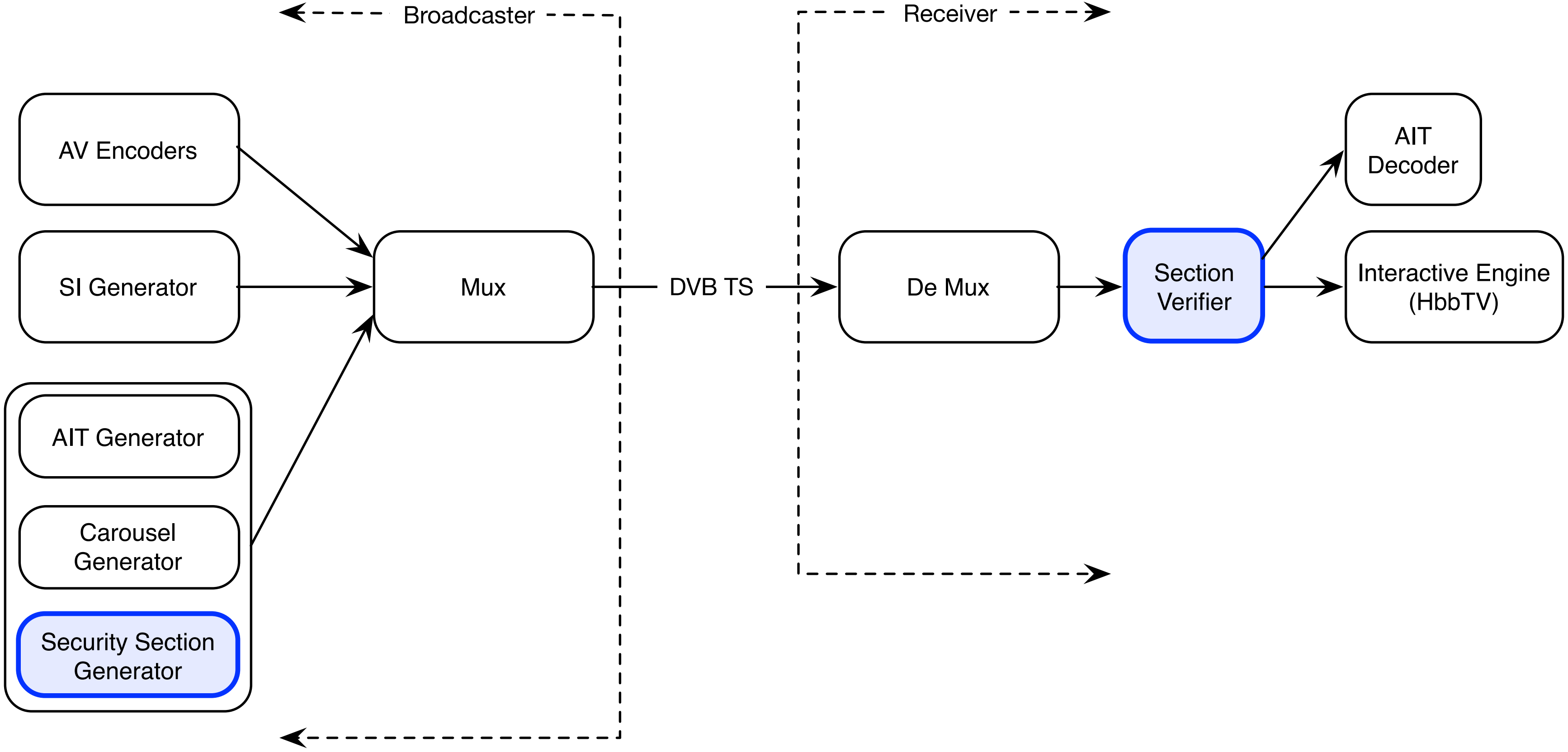
- Authentication of broadcast data for interactivity
- Trust establishment for public keys used for verification of the authentication messages

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

Part 1: Authentication

Authentication Overview



Authentication principles

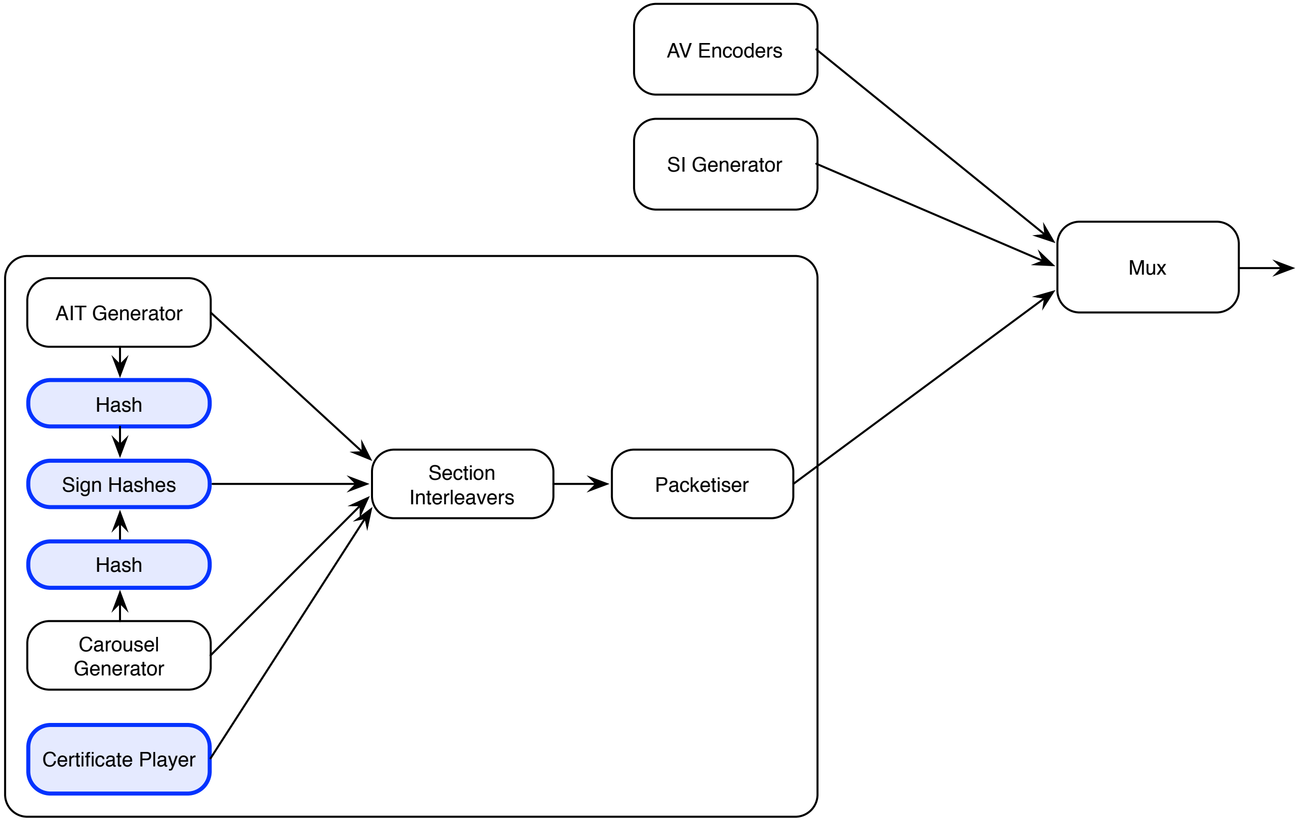
- The broadcaster:
  - Calculates Hash for payload sections
  - Signs groups of Hashes with a Private Key
  - Transmits signed Hashes

- The receiver:
  - Receives signed Hashes and validates with a Public Key
  - Calculates Hash for received payload sections
  - Check that the Hash for each received payload section matches a validated signed Hash

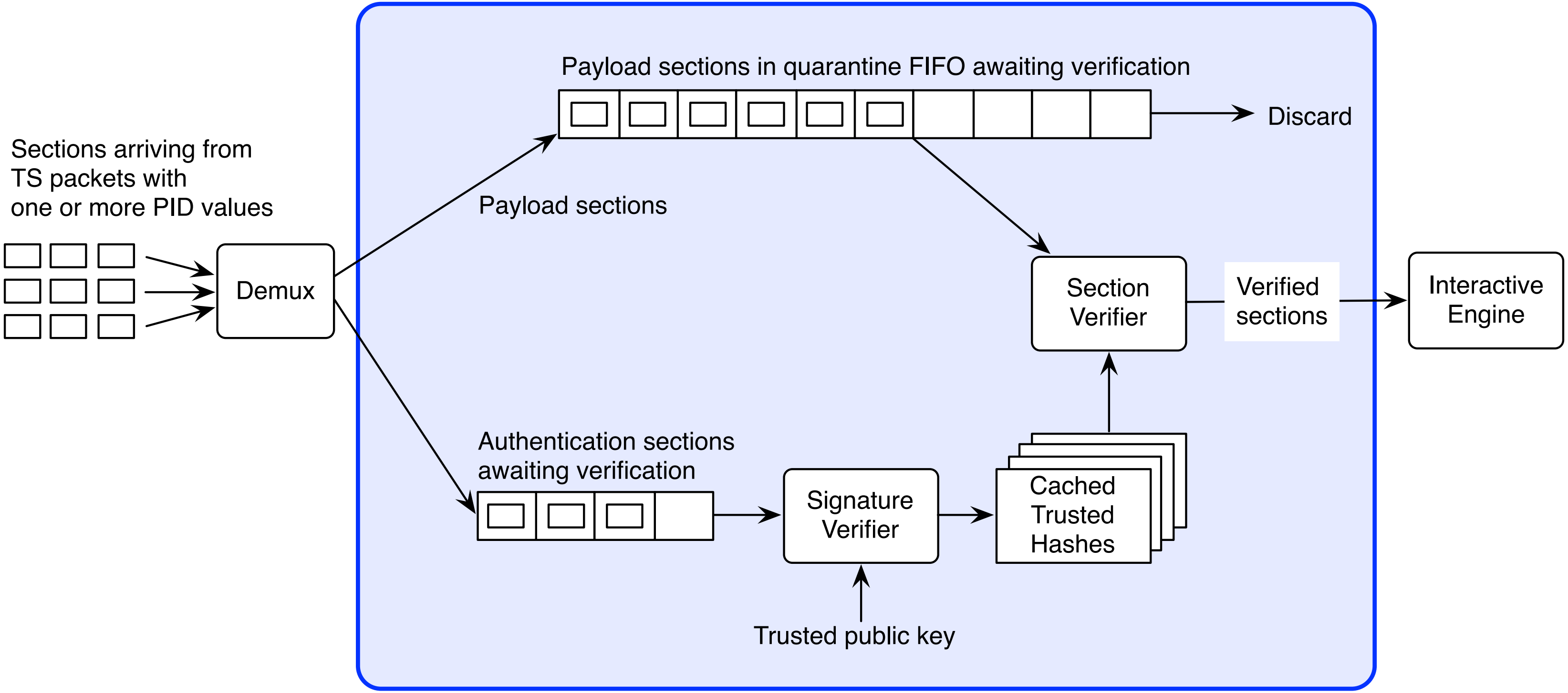
Cryptographic toolkit

- Section hash algorithm
  - SHA-256 or SHA-512
  - Well established and standard algorithms
- Signature algorithm
  - At least Edwards-curve Digital Signature Algorithm
    - ED25519 (RFC8032)
    - Offers significant benefits
    - Adoption spreading in the internet and other places
  - Optional support for RSA and ECDSA

Authentication at the Broadcaster



Verification at the Receiver

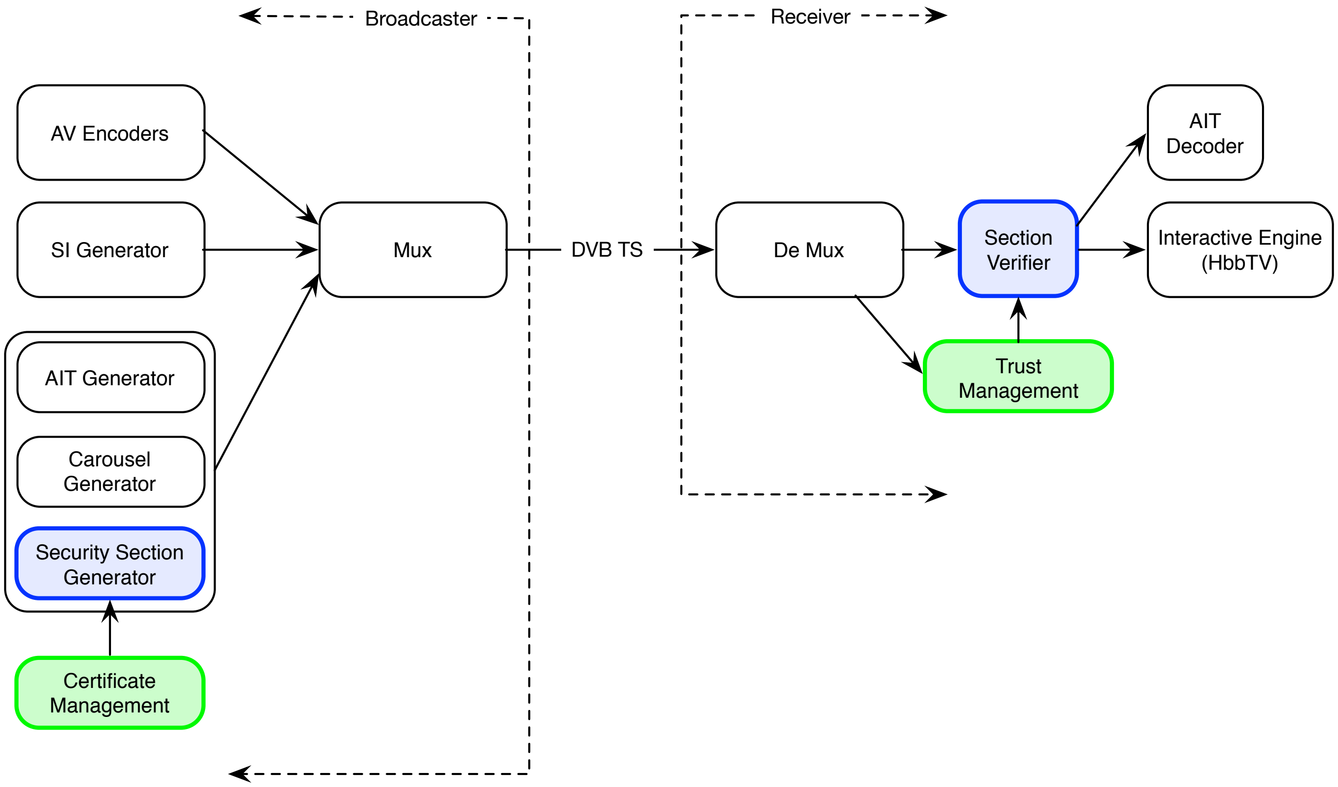


Part 2: Trust Establishment

Establishing Trust: Introduction

- Receivers need a “trusted” Public Key to verify Authentication Sections
- Broadcast Certificate Collection Messages deliver a certificate chain that provides a Public Key
- Initially “trust” comes from the receiver observing the same certificates for a period of time
- Certificate updates are authenticated by previous certificates

Including Trust Establishment



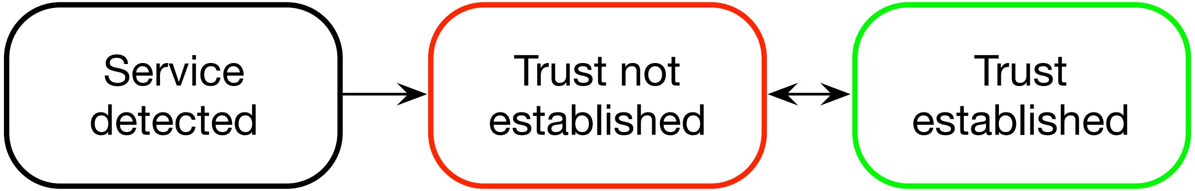
Establishing Trust: Two schemes

- Stand alone mode
  - Basic mode supported by all implementations
  - Relies on persistence of certificate signalling in the broadcast

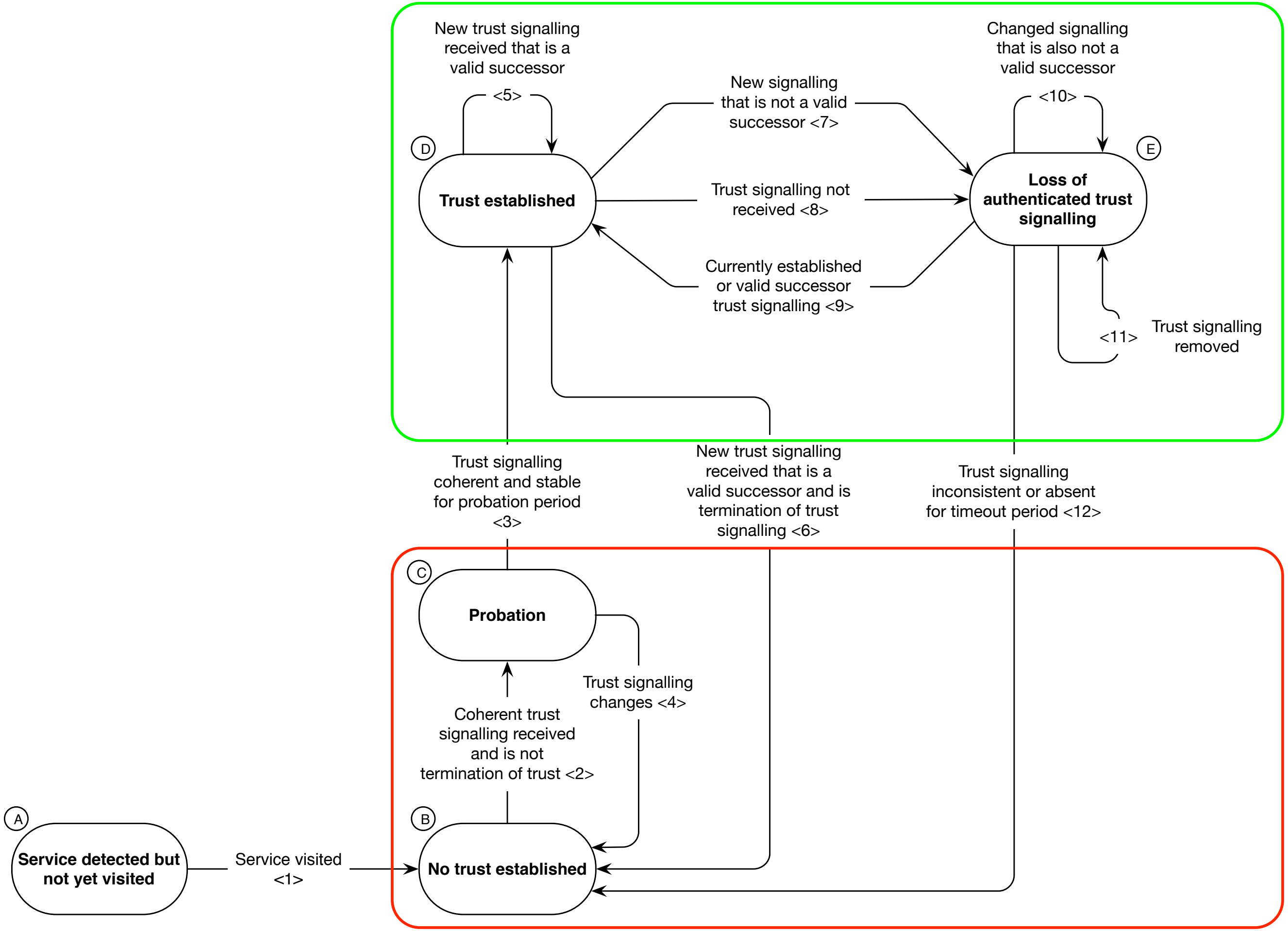
- Coordinating entity mode (optional)
  - Uses a certificate pre-installed in the receiver
  - Requires coordinated effort within a market

Scheme 1: Stand alone Trust Establishment

Trust Establishment:
Receiver State Machine (overview)



Trust Establishment : State Machine (detail)



New trust signalling received that is a valid successor
<5>
D
Trust established
New signalling that is not a valid successor <7>
Trust signalling not received <8>
Currently established or valid successor trust signalling <9>
Changed signalling that is also not a valid successor
<10>
E
Loss of authenticated trust signalling
<11>
Trust signalling removed
Trust signalling coherent and stable for probation period <3>
New trust signalling received that is a valid successor and is termination of trust signalling <6>
Trust signalling inconsistent or absent for timeout period <12>
C
Probation
Trust signalling changes <4>
Coherent trust signalling received and is not termination of trust <2>
A
Service detected but not yet visited
Service visited <1>
B
No trust established

Establishing Trust: New services

The time for new service to establish trust depends on the user and receiver behaviour:

- Following receiver installation or manual channel scan: 300s
- If receiver detects new service automatically: 1800s

Carriage of protection data

- The Authentication and Certificate Collection messages can be carried on the same PID as the AIT or the Object Carousel
- No new PID required
- Naturally will go with the service if it is re-multiplexed

Scheme 2: Using a Coordinating Entity

Option to use a Coordinating Entity Certificate

- In addition establishing trust via persistence (the stand alone scheme) a Coordinating Entity Root can be used
- Coordinating Entity provides an “anchor” that is installed in receivers
- Broadcasts include certificates leading to this anchor

Properties of using a Coordinating Entity

- Allows trust to be established instantly
  - Services can be trusted immediately when a new receiver is first used
  - Removes the delay before new services become trusted
- Potentially more secure
- Removes the “persistence” state machine
- Requires coordinated activity by the stake holders in a market
  - This might not be possible due to commercial or legal obstacles in some markets
- May require regulator oversight

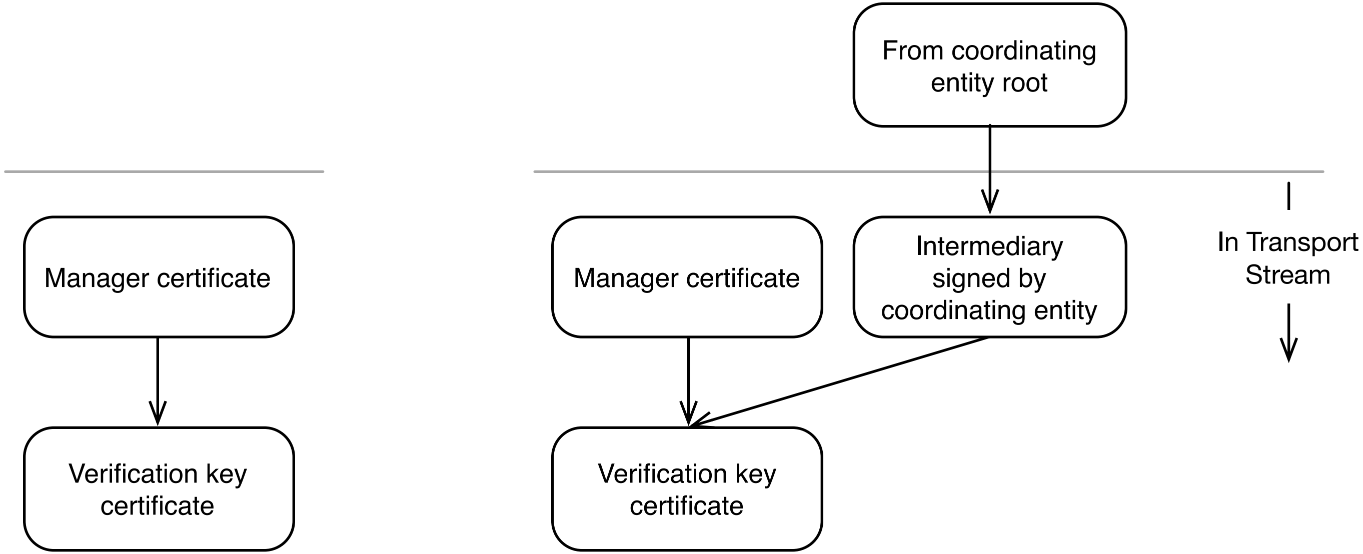
Coexistence of Coordinating Entity and Stand-alone schemes

- The Coordinating Entity scheme is designed to coexist with the Stand-alone Scheme
  - All receivers support Standalone Scheme
  - All receivers tolerate Coordinating Entity signalling if present
  - Optionally receivers can use the Coordinating Entity signalling
  - Both schemes can be efficiently supported by the same broadcast signalling

Certificate chain examples

Stand alone only

Stand alone + Coordinating Entity



From coordinating entity root

Manager certificate

Verification key certificate

Manager certificate

Intermediary signed by coordinating entity

In Transport Stream

Verification key certificate

Trust Management

Trust Management

- Broadcast certificates for Trust Establishment can be securely updated
- The Public Key provided by the certificates for authenticating payload sections can be securely updated
- The generation of new certificates can be done off-line (which may be operationally convenient)

ETSI TS 102 809 V1.3.1 (2017-04)

Technical Specification

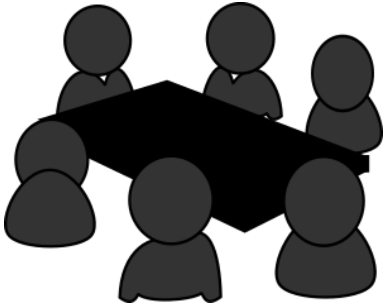
Digital Video Broadcasting (DVB);
Signalling and carriage of interactive applications and services in Hybrid broadcast/broadband environments

Questions?

How to secure your market!

Nigel Earnshaw
(BBC R&D nigel.earnshaw@rd.bbc.co.uk)

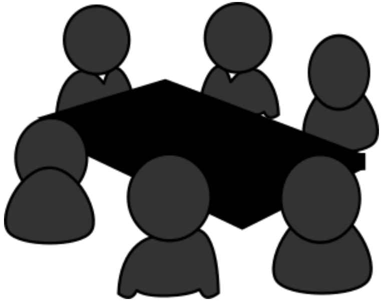
Market stakeholders



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.

Different approaches to trust



- Within a market that has a coordinating entity not all broadcasters may participate
- Within a market that has a coordinating entity possibly not all receivers will support the coordinating entity (e.g. imports from other markets)
- A highly regulated market may choose to encourage or enforce a co-ordinated trust anchor approach.
  - E.g. as a condition for a trademark

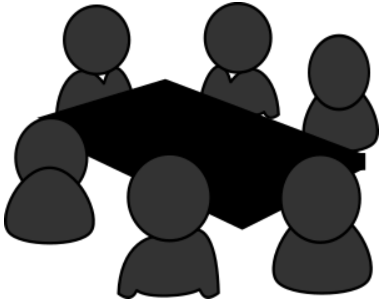
The signalling is compatible across these scenarios.

A market can have a mix of support and can evolve over time to get the best level of robustness in general over a range of mixed business strategies.

=> Which approach suites your market?

Partial deployment

- Within a market perhaps not all broadcasters are ready to authenticate their services
- Within a market perhaps not all receivers implement authentication



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

Technical Community

Moving from a specification to consistent and robust deployment requires the development of a test regime.

Ensure predictable behaviour when pairing a receiver with a broadcast service in terms of all aspects of the functionality including;

device response to attack
device response to new service
device response to service trust updates
sample transport streams

⇒ Develop a conformance strategy for your market

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 conformance in their market

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

Conclusions

Conclusions

- Vulnerabilities likely in advanced TV receivers!
- Patching receivers may not be practical
- TS 102 809 describes a method to protect against malicious applications added to a broadcast signal

- Deployment doesn’t require all stakeholders in a market to participate but becomes more beneficial as more stakeholders participate

Questions?

Thank you

Credits

Some images are from community commons sources:
https://openclipart.org/detail/217930/meeting-around-a-table-in-grayscale
Vtheikki
https://openclipart.org/detail/179429/worldwide-community
colinda
https://openclipart.org/detail/273315/signal-spectrum-analyst
Juhele