AMWA NMOS API Security

Simon Rankine – Research Engineer
BBC Research and Development

BBC | Research & Development

IP SHOWCASE THEATRE AT IBC – SEPT. 14-18, 2018

Motivation

- To get the most out of the NMOS APIs we need to be able to run them on networks which we cannot fully control
- In particularly sensitive environments it may not be enough to isolate the broadcast network
- Attacks on broadcasters such as TV5MONDE highlight that the broadcast industry is a high profile target.
- Security protects against accidental as well as deliberate misuse

BBC | Research & Development

2

AMWA NMOS APIs and Security

- Part of the motivation for using HTTP is that we can harness carefully scrutinised and well developed technology from the web industry.
- As such have always been *"securable"* using standard mechanisms, but to do so would have broken interoperability.
- The AMWA set up the API security workgroup to investigate how the APIs could be secured in an interoperable way.

BBC | Research & Development

Objectives

Confidentiality Data passing between client and the APIs is unreadable to third parties.

Identification The client can check whether the API it is interacting with is owned by a trusted party.

Integrity It must be clear if data travelling to or from the API been tampered with.

Authentication The client can check if packets actually came from the API it is interacting with, and vice versa.

Authorisation The API can determine whether the client interacting with it has authorisation to carry out the operation requested.

BBC | Research & Development

IP SHOWCASE THEATRE

Work Areas

Connection Security

- HTTP over TLS (HTTPS)
- Identify cipher suites for interoperability
- Establish best practice for use of TLS with AMWA NMOS APIs

Establishing Trust

- Public key infrastructure with x509 certificates
- Explore how PKI can be used in a broadcast environment

Client Authorisation

- OAuth 2.0 with JSON Web Tokens
- Identify what is needed to ensure interoperability

BBC | Research & Development

IP SHOWCASE THEATRE

Scope

Riedel will cover this at 15:30 ->	Application	API Client Authorisation (Web Tokens)
	Transport	Session Security (TLS)
	Network	Network access control
	Physical	Site/Server room access etc.

BBC | Research & Development

6

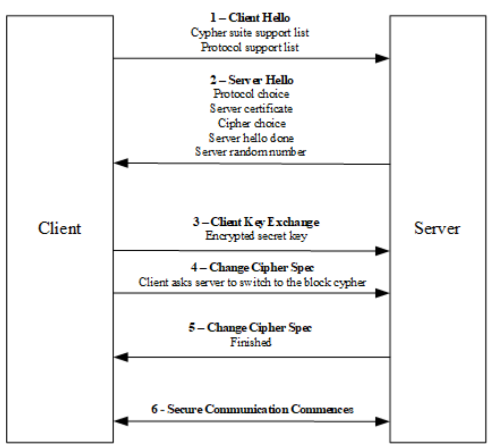
Connection Security

- Tunnels insecure traffic like HTTP through an encrypted connection so that it cannot be read or modified during transit.
- The TLS protocol is widely used for securing a wide range of traffic across the internet and on private/corporate networks.
- This is achieved using a collection of different algorithms, which together form the “cipher suite”.

BBC | Research & Development

7

TLS Handshake



BBC | Research & Development

Cipher Suites

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS	ECDHE	RSA	AES_256	GCM	SHA384
Protocol	Key exchange cipher	Key authentication algorithm	Block cipher	Block cipher mode	Hashing Algorithm

BBC | Research & Development

HTTP over TLS (HTTPS) – Cipher Suites

TLS ECDHE ECDSA WITH AES 128 GCM SHA256
TLS ECDHE ECDSA WITH AES 256 GCM SHA384
TLS ECDHE ECDSA WITH AES 128 CBC SHA256
TLS ECDHE ECDSA WITH AES 256 CBC SHA384
TLS ECDHE RSA WITH AES 128 GCM SHA256
TLS ECDHE RSA WITH AES 256 GCM SHA384
TLS DHE RSA WITH AES 128 GCM SHA256
TLS DHE RSA WITH AES 256 GCM SHA384
TLS ECDHE RSA WITH AES 128 CBC SHA256
TLS ECDHE RSA WITH AES 256 CBC SHA384
TLS DHE RSA WITH AES 128 CBC SHA256
TLS DHE RSA WITH AES 256 CBC SHA256
TLS ECDHE ECDSA WITH AES 128 CCM 8

BBC | Research & Development

IP SHOWCASE THEATRE

But isn't this SSL?

SSL	SSL 1.0, 2.0, 3.0 all insecure – don't use them!
TLS 1.0	No longer considered secure, avoid use.
TLS 1.1	Still considered secure, but generally TLS 1.2 is preferred as there is little difference.
TLS 1.2	Current best practice – use wherever possible.
TLS 1.3	Very recently published as RFC , still finding its way into implementations.

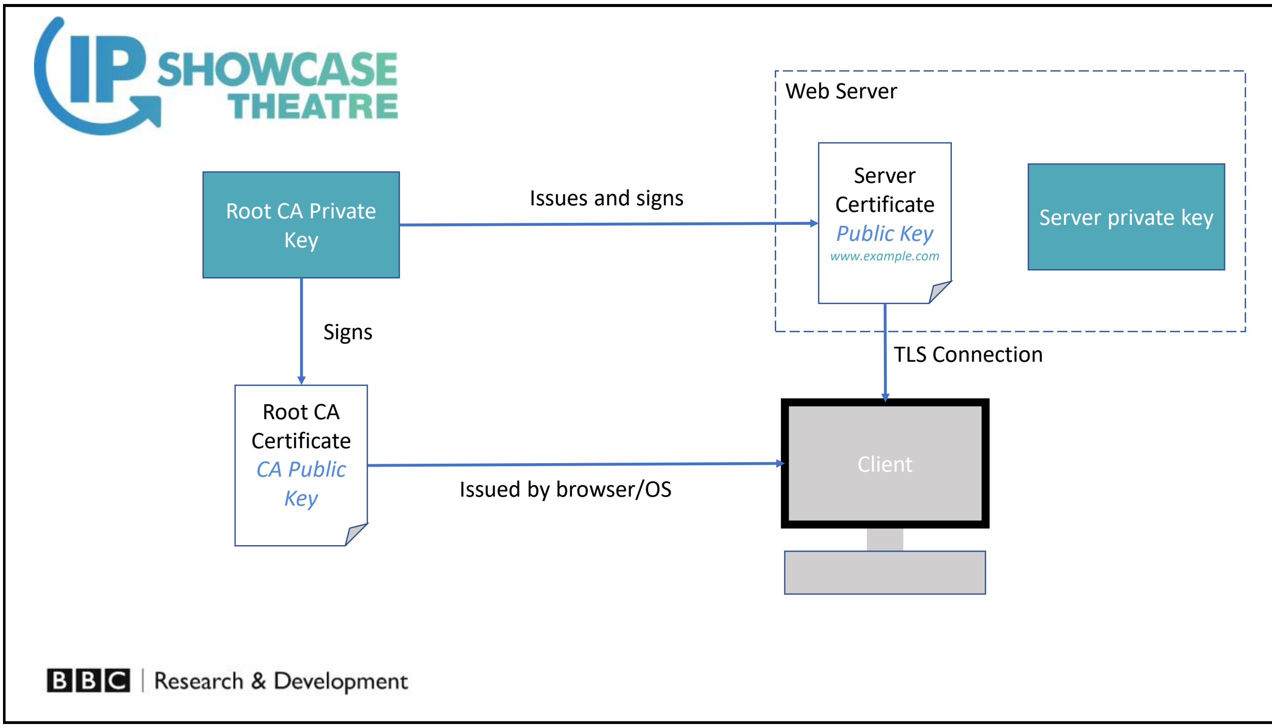
BBC | Research & Development

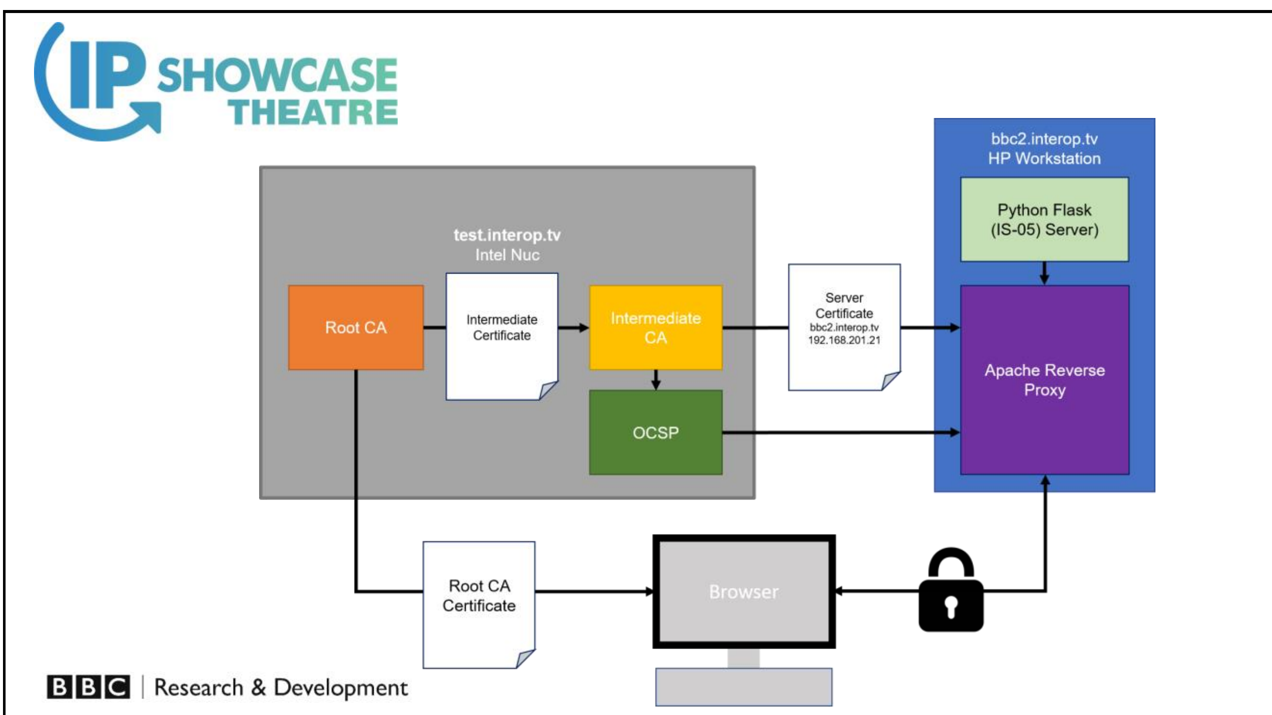
IP SHOWCASE THEATRE

Establishing Trust

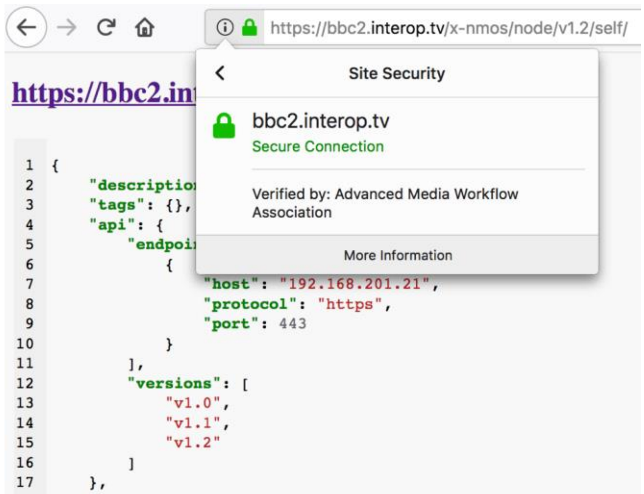
- API servers need to hold a certificate trusted by the client. This certificate must match its subject name (e.g. URL).
- Certificates are issued by a trusted 3rd party – the "Certificate Authority".
- Asymmetric encryption is used to allow the certificate authority to "sign" the server's certificate such that the client can check its authenticity using the public key of the certificate authority.

BBC | Research & Development 12


IP SHOWCASE THEATRE
Web Server
Root CA Private Key
Issues and signs
Server Certificate
Public Key
www.example.com
Server private key
Signs
TLS Connection
Root CA Certificate
CA Public Key
Issued by browser/OS
Client
BBC | Research & Development


IP SHOWCASE THEATRE
bbc2.interop.tv
HP Workstation
test.interop.tv
Intel Nuc
Python Flask
(IS-05) Server)
Root CA
Intermediate Certificate
Intermediate CA
Server Certificate
bbc2.interop.tv
192.168.201.21
OCSP
Apache Reverse Proxy
Root CA Certificate
Browser
BBC | Research & Development

IP SHOWCASE THEATRE



BBC | Research & Development

15

IP SHOWCASE THEATRE

CURATED BY VSF VIDEO SERVICES FORUM

Thank You

Simon Rankine, BBC Research and Development

Simon.Rankine@bbc.co.uk

@RankineSimon

https://www.bbc.co.uk/rd/publications/whitepaper337

BBC | Research & Development

IP SHOWCASE THEATRE AT IBC – SEPT. 14-18, 2018