Securing IS-04/05 - How to Lock My Media Streams

Arne Bönninghoff – Head of IP Research
Riedel Communications GmbH & Co. KG
TR-1001 - THE MEDIA NODE MATURITY CHECKLIST FOR NAB SHOPPING
TR-1001 - THE MEDIA NODE MATURITY CHECKLIST FOR NAB SHOPPING

- TR-1001-1
TR-1001 - THE MEDIA NODE MATURITY CHECKLIST FOR NAB SHOPPING

- TR-1001-1
BCP-003-02

- As a user, I want my main control system to be the only system being authorized to query the network for IS-04 resources.
- As a user, I want my main control system to be the only system being authorized to make connections with IS-05.
Authorisation vs. Authentication

• Authentication:
  – verify that someone is who they claim to be
  ➢ Covered by exchange of certificates

• Authorization:
  – deciding which resource a user should be able to access, and what they should be allowed to do with those resources
  ➢ Additional techniques needed
BCP-003-02

• Describes techniques how to retrieve a token and get authorized access
• Describes techniques for NMOS nodes how to validate tokens
• Describes the type of information stored in the token
How to become authorized?
Initial setup
OAuth2 + JWT for NMOS

• Authorization server issues keys to resource servers (=NMOS Nodes)
  – Needed to be able to decrypt tokens for validation
  – Keys are refreshed in short intervals (1 hour)

• Authorization server issues tokens to Clients (=control systems)
  – Needed to be able to perform actions against resource servers
  – Clients need to be listed in advance in the auth server (out of scope
    • LDAP/AD/SSO
Accessing Resources
Token based auth

• Stateless
  – No record on Server about a session
• Traditional Token flow:
  1. User enters their login credentials
  2. Server verifies the credentials are correct and returns signed token
  3. Token is stored client-side (most common in local storage, but cookie is possible as well)
  4. Subsequent requests to the server include this token as an additional Authorization header
  5. Server decodes the token and if token is valid process the request
  6. Once a user logs out, the token is destroyed client-side. No interaction with server is needed.
JWT

- Header, Body, Signature
- Body containing claims
- Rfc7519
  - Issued key needed to verify the signature
  - only valid tokens are processed
JWT Claims

• Define more granular claims

```
{
  "iss": "https://euth.example.com",
  "sub": "username@example.com",
  "aud": "https://node.example.com",
  "iat": "154979460",
  "exp": "154979870",
  "x-nmos-api": {
    "name": "is-04",
    "node-read": true
  }
}
```

"x-nmos-api": {
  "name": "is-04",
  "version": ["1.0","1.1","1.2"],
  "node-read": true
}
IP Showcase Demonstration

- Audio senders, receivers, and audio level meters
- NMOS APIs secured by TLS as per BCP-003-01
Prototype using JWT & proposed Oauth2 workflow
Prototype using JWT & proposed OAuth workflow
Prototype using JWT & proposed OAuth workflow
“NMOS World”

• Authorisation server visible through DNS-SD (unicast!)

• Backwards compatible
  – Just send IS-04 and IS-05 without token

• Also applicable for IS-04 query API
  – Example: only some controllers are allowed to retrieve information
Conclusion

• IS-04 and IS-05 are based on standard IT technology
• HTTP and JSON are used by many other applications
• Other applications use OAuth2 and JWT already in large scale
• Key exchange workflow provides the fundamental environment for HTTPS transport
• Secure Transport enables OAuth2
• Backwards compatibility given
Next steps

• Finish discussion around grants
  – Define grant types for different applications
  – Need more user input and testing

• Test interoperability

• Test backwards compatibility

• Get involved!
Thank You

Arne Bönninghoff, Riedel Communications GmbH
arne.boenninghoff@riedel.net // +49 177 8347500