DICOM℠
Digital Imaging and Communications in Medicine

TLS Security Profiles

Rob Horn
WG-14: Security

TLS Profile Changes

- **Two new TLS profiles defined**
  - **Best Practices**
  - **Non-downgrading Best Practices**

- **Two existing (old) TLS profiles retired**
- **Motivation for profile changes**
  - **Changes to security threat environment**
  - **Changes to cryptographic methods**
  - **Known flaws in older TLS versions**
  - **IETF new best practices guidance**
  - **Device documentation.**
    - It is easier to state compliance with a profile than to document all the RFC's and options involved.

Motivation and IETF actions

- **Motivation**
  - **Flaws have been found in TLS**
  - **Cryptographic technology has changed**
    - Old methods are becoming vulnerable
    - New methods have been invented
- **IETF Action**
  - **Best Practices Recommendations issued in 2015**
  - **Shorthand summary: “Use TLS 1.2”**
  - **Connection negotiation starts with best strength options, then accepts several downgrades if needed.**
  - **IETF’s goal is to have gradual upgrades everywhere without sacrificing interoperability (within limits). The lowest downgrade is still considered “good enough”.**

New Profiles

- **Best Practices TLS Profile**
  - **Complies with BCP-195, the IETF's best current practice guidance.**
  - **No other changes to use of TLS for DICOM.**
- **Non Downgrading Best Practices TLS Profile**
  - **Complies with the BCP-195 recommendation for initial TLS versions, cryptography, etc.**
  - **Does not permit downgrading to lower strength.**

- **Customers can determine and choose whether to accept negotiated downgrades.**
  - **Downgraded connections still provide good protection in most situations.**
  - **Customers can make their own decision about accepting risks.**

Old Profiles

- **Basic TLS Secure Transport Connection Profile is retired**
  - **Use of Basic TLS does not meet BCP-195. Devices that only support this profile will not be able to connect to devices that comply with either of the new profiles.**
  - **Basic TLS may still be useful in some situations.**
- **AES TLS Secure Transport Connection profile is retired.**
  - **BCP-195 permits connections using the AES setting as a downgrade only. It is acceptable but not preferred.**
  - **The new Best Practices TLS profile will negotiate a downgrade to devices that only support the AES profile.**
  - **The new Non Downgrade Best Practices TLS profile will not negotiate a downgrade. They will not connect with devices that only support the AES profile.**