Canada Health Infoway | Inforoute Santé du Canada

Transport Layer Interoperability Cryptography Update

A Discussion Document

December 10, 2010

Presented by André Carrington, P.Eng, CISSP, CISM, CISA, CIPP/C
Director, Implementation, Privacy & Security, SPS

Purpose of this presentation

To advise stakeholders on:

- updates drafted for the Transport Layer Interoperability specification
- as it proceeds toward Canadian Draft For Use (CDFU) status in the Standards Collaborative's decision making process
- for feedback and consensus-building

Outline

- The need for changes
- A brief history
- The proposed settings
- Prior lack of support for the proposed settings
- More technical detail

The need for changes

- The Canadian and US federal authorities for cryptography, CSEC and NIST, are deprecating the following key-lengths & algorithms by Dec 31, 2010:
  - 1024 bits re RSA modulus, DSA key size, DH field size
  - 160 bits re ECC modulus
  - 160 bits re SHA/SHA-1
- CSEC and NIST allow the use of 3DES until 2030, but AES is recommended instead

Changes in the TLI specification

- CSEC and NIST have deprecated lesser encryption key lengths and algorithms
- The TLI spec, rather than deprecate:
  - notes that, in general, TLS clients and TLS servers negotiate the strongest mutually shared ciphersuite
  - requires support for sufficient algorithms, which are then used ***by default***, for implementations that meet the spec…while also supporting legacy systems
- This approach ensures that the TLI spec:
  - facilitates interoperability
  - supports algorithms & approaches that avoid undue risk, and meet requirements
  - lets each jurisdiction determine their own roadmap/ timing for POS systems to meet the TLI spec

A brief history

- The new/current TLI spec is version 3.
  - It is being proposed as a Canadian Draft for Use (CDFU)
  - Some rule numbers have changed since the previous version (v1.02)
  - Going-forward, rule numbers should be stable

- The previous version, v1.02, was published circa February 2009 at the conclusion of:
  - the iEHR Technical II Project TLI stream
  - and many SCWG 6 meetings (and SCWG 8 meetings too)
  - Note (caution): v2.0 is older than v1.02; and v2.0 can still be found on the SCWG 6 forum.

Cryptography in the TLI spec

- the Transport Layer Interoperability (TLI) spec secures the transport &/or payload via ciphersuites

1. authentication (dig sig) & key exchange
   - PKI, asymmetric encryption

2. transport encryption
   - symmetric encryption

3. transport integrity
   - hashes

Updates to cryptography in the TLI spec

1. authentication (dig sig) & key exchange
   - RSA*, DSS/DSA*, ***ECDH**, ECDHE**, ECDSA****
   - ***≥ 2048 bit RSA/DSS/DSA support required***
   - ***≥ 224 bit ECC required if supported, ECC preferred***
   - ***for key exchange, ECDH not recommended, ECDHE ok***

2. transport encryption
   - AES* ***(recommended over)*** 3DES/TDEA
   - ***≥ 128 bits (effective strength) support required***

3. transport integrity was not updated due to insufficient support for interoperability (at this time)

*affected, **new, ^previously deprecated, ^^CSEC/NIST deprecated end of 2010

Past support for these requirements, was limited

- Digital Signature Standard FIPS 186-3 (v3 Jun 2009)
  - v3 updated to support 2048 & 3072 bit DSS and SHA ≥224 bits
- Transport Layer Security standard (v1.2 Aug 2008)
  - 1.2 was brand new; fully standardizes extensions for AES and ECC support (AES now built-in) and uses SHA256 for RNG
- WS-I Basic Security Profile (v1.1 Jan 2010)
  - v1.1 recommends AES over 3DES; no mention of ECC, SHA ≥224 bits
- Industry & SCWGs
  - have since upgraded root and intermediate CA keys to 2048 bits
  - SCWGs and HIG did not previously identify these requirements

Insufficient support for better transport integrity

Transport integrity

- ~~MD5~~^, SHA-1^^ ***and ideally SHA256**, SHA384**, SHA512** to support hashes ≥ 256 bits***

Defined in the Secure Hash Standard FIPS 180-3 (v3 Oct 2008)

Not supported in:

- TLS 1.0 (widely implemented)
- TLS 1.1 (not widely supported)
- AES Ciphersuites for TLS
- ECC: Suite B Profile for TLS (TLS 1.1 transitional profile)

Only supported in:

- TLS 1.2 (very sparsely supported)
- ECC: Suite B Profile for TLS (TLS 1.2 profile)
- ECC: TLS EC Ciphersuites w SHA-256/384 and AES GCM

*affected, **new, ^previously deprecated, ^^CSEC/NIST deprecated end of 2010

Canada Health Infoway
Inforoute Santé du Canada

The End

(references follow)

Presented by André Carrington, P.Eng, CISSP, CISM, CISA, CIPP/C
Director, Implementation, Privacy & Security, SPS

References (1 of 3)

- Digital Signature Standard
  - http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
- Secure Hash Standard
  - http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf
- Transport Layer Security Protocol
  - http://tools.ietf.org/search/rfc2246 (v1.0)
  - http://tools.ietf.org/search/rfc4346 (v1.1)
  - http://tools.ietf.org/search/rfc5246 (v1.2)
- WS-I Basic Security Profile v1.1
  - http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html
- RFC 5430 Suite B Profile for TLS
  - http://tools.ietf.org/html/rfc5430
- AES Ciphersuites for TLS
  - http://tools.ietf.org/html/rfc3268
- TLS Elliptic Curve Ciphersuites with SHA256…
  - http://tools.ietf.org/html/rfc5289

References (2 of 3)

- CSEC ITSA 11D - general crypto guidance
  - http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html
- CSEC ITSB 60 - TLS crypto guidance
  - http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb60-eng.html
- NIST SP 800-57 Parts 1, 2, 3 - crypto guidance
  - http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
  - http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf
  - http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf
- Schneier, Bruce. Applied Cryptography 2nd ed.

References (3 of 3)

- Lenstra & Verheul
  - http://www.win.tue.nl/~klenstra/key.pdf
- Lenstra (updated)
  - http://www.keylength.com/biblio/Handbook_of_Information_Security_-_Keylength.pdf
- EuroCrypt II 03/2010
  - http://www.ecrypt.eu.org/documents/D.SPA.13.pdf
- NIST
  - http://csrc.nist.gov/groups/ST/toolkit/key_management.html
- FNISA
  - http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf
- NSA
  - http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml
- IETF RFC 3766
  - http://tools.ietf.org/search/rfc3766
- BSI
  - http://www.bundesnetzagentur.de/cae/servlet/contentblob/148572/publicationFile/3994/2010AlgoKatpdf.pdf