IHE Change Proposal

Tracking information:

IHE Domain	IT Infrastructure
Change Proposal ID:	CP-ITI-1145
Change Proposal Status:	Final Text
Date of last update:	Sep 13, 2018
Person assigned:	Charles Parisot, Vassil Peytchev, John Moehrke

Change Proposal Summary information:

ATNA – Add three options affecting ITI-19	
Submitter's Name(s) and e-mail address(es):	John Moehrke – JohnMoehrke@gmail.com
Submission Date:	May 4, 2018
Integration Profile(s) affected:	ATNA
Actor(s) affected:	Secure Node, Secure Application
IHE Technical Framework or Supplement modified:	ITI TF Vol 1 and 2a, Rev 15, July 2018 RESTful Query TI Supplement, Rev 2.2, July 2017
Volume(s) and Section(s) affected:	Volume 1, Volume 2a

****** This CP is a combination of the changes from CP-ITI-1094 and CP-ITI-1124 as they were resolved in ITI CP Ballot 49 ******

RATIONALE for CP-ITI-1124 - ATNA – Add two options related to BCP195 TLS Secure Transport Connection

Add two named options to ATNA to enable systems to declare that they have support for TLS 1.2 with minimally a known-good set of cypher suites.

It is proposed to introduce two options called:

1. BCP195 TLS Secure Transport Connection – All TLS versions
2. BCP195 TLS Secure Transport Connection - TLS 1.2 Floor

Both options rely on the IETF published "Best Current Practice" BCP195 for TLS Secure Transport Communications.

The first option offers the highest level of protection for the TLS-protected communication channel by adopting the IETF Best Current Practice (BCP195), but include backward compatibility requirements to keep interoperation with systems that do not support BCP195, by down-grading to TLS Version 1.1 or Version 1.0 and/or cipher suites under specific conditions that are allowed by BCP195. Note the baseline requirement for ATNA is TLS 1.0 with TLS_RSA_WITH_AES_128_CBC_SHA cipher which is not recommended by BCP195, but is allowed by BCP195 under specific circumstances. Therefore this option will maintain interoperability as appropriate with existing ATNA implementations.

The second option adds additional requirement to (a) not allow any TLS protocol lower than TLS 1.2 and (b) makes mandatory some newer cypher suites that are only recommended in BCP195.

Both options are compatible with similar options present in DICOM

- B.9. BCP195 TLS Secure Transport Connection Profile
- B.10. Non-Downgrading BCP195 TLS Secure Transport Connection Profile

  Note: BCP 195, is an evolving specification (updates are made by the IETF when security failures are detected and corrected (every 5-10 years as the technology evolves). It means that new options may have to be created to keep up with BCP 195 evolution.

  Note: The BCP 195 TLS Secure Transport Connection - TLS 1.2 floor option raises the cyber protection requirements to a level, where backward compatibility or upgrade scheduling with ATNA implementation without at least one of these options is not supported in order to prevent lesser protected communications from happening.

This CP includes the following:

- The specification for these options added to the current ATNA Actors as well as to the Audit Consumer in the RESTful Query TI Supplement
- Two explanatory sections in Vol 1 describing each of the two options and their intended use.
- Specification in Volume 2 for the technical requirements by summarizing the BCP195.

Note: ITI TF-2a: 3.19.6.2 is unchanged by this CP, but the text in that section will be updated by CP-ITI-1131 in a way that is compatible with the contents of this

RATIONALE for CP-ITI-1094 - Require server certificate domain name validation for all traffic over the public Internet

Current IHE documentation does not follow best practices for verifying server identities within the context of TLS, creating a security vulnerability

Overview

In order for a client to verify the identity of a server over TLS, the client must verify that an appropriate reference identifier within the server certificate matches the source domain the client is attempting to reach (RFC 6125, Section 6). If this verification does not take place, and if a malicious actor is able to intercept traffic, that actor could acquire a certificate for an arbitrary domain from any certificate authority trusted by the client (by proving control over that domain), present this certificate to incoming traffic, and effectively impersonate the server.

Current IHE documentation

The current documentation makes no direct reference to the security vulnerability this reveals, and only states that enforcing this verification "could introduce a new failure mode, e.g. DNS failure". But appropriate functioning of DNS is already a presupposition for the vast majority of Internet traffic; a client-side DNS failure will almost always result in the client failing to even make initial contact with the server.

Perhaps the current documentation assumes that most clients have only installed trust for a very small number of certificate authorities, where certificate issuance is very infrequent and available exclusively for healthcare-exchange purposes. Yet this is not the case for the vast majority of clients. Any client that connects with networks like Carequality or HISPs like Healthbridge needs to at least have trust installed for a root Entrust or DigiCert CA. These certificate authorities can and do issue certificates to many domains for many purposes; it is quite feasible for a malicious actor to obtain one. Additionally, Windows machines have trust installed for a large list of "widely-trusted" root certificates from Microsoft by default.

Scope of proposed changes

Although failure to properly verify the identity of a server may be concerning in all cases, it is significantly more dangerous over the public Internet, since more methods exist by which a malicious attacker can intercept traffic. Therefore, this Change Proposal is intended to modify requirements **exclusively for traffic sent over the public Internet**. This also reduces the likelihood that administrators will have additional problems with intra-organization communication following this change.

Current methods by which a malicious actor could intercept traffic

In order for a malicious actor to take advantage of the current lack of server verification requirement, the actor needs to intercept traffic intended for a server. Below are several methods a malicious actor could use; this is not an exhaustive list.

- ARP spoofing: If a malicious actor had access to the client's LAN, the actor could mimic the gateway of the LAN by sending misleading ARP messages to the client machine.
- DNS spoofing: If a malicious actor had sufficient access, the actor could poison the client's hosts file, corrupt the client's DNS settings, or corrupt the server's DNS table to intentionally route messages to the wrong machine.
- IP hijacking: If a malicious actor had sufficient access, the actor could corrupt intermediary routing tables to intentionally route messages to the wrong machine.
- Domain squatting: If a legitimate server fails to renew their domain, a malicious actor could purchase the domain directly from the domain provider. (In this case, the malicious actor could eventually successfully impersonate the server even if the client did perform server certificate verification; but the malicious actor would first need to purchase a domain-validated certificate from a trusted certificate authority for the particular domain they now control, which is an additional time-consuming step.)

Many of these methods are widely known; this is why RFC 6125 requires server certificate verification for all TLS traffic.

Consequences of intercepted traffic

The use of any of these methods could, at minimum, allow a malicious actor to impersonate a server. If a legitimate server does not appropriately require client certificate authentication, the malicious actor could become a full-fledged Man-in-the-Middle and observe all valid traffic between a client and server.

20180718 note: Version -10 of this CP in Ballot 49 contains updates to address Ballot 48 comments. For reference, the Ballot 48 comments are here: https://docs.google.com/spreadsheets/d/18TI1XBE-Ym6ssHpX5ZPphcMZRr166m9jxcsWYL_TPHM/edit#gid=0

EDITOR: *Update the Table 9.2-1 in Volume 1 Section 9.2… This is mostly indicated by bold-underline, but also includes the creation of table rows and doing merging of some cells.*

(Note that subsections 9.2.3 and 9.2.4 are added in the "Add RESTful Query to ATNA TI Supplement", so the new options get numbered 9.2.5 – 9.2.7).

9.2 ATNA Actor Options

Options that may be selected for this Integration Profile are listed in the Table 9.2-1 along with the actors to which they apply. Dependencies between options when applicable are specified in notes.

Table 9.2-1: ATNA - Actors and Options

Actor	Options	Vol. & Section
Audit Record Repository	None	–
Audit Record Forwarder	None	--
Secure Node	Radiology Audit Trail	RAD TF-1: 2.2.1 RAD TF-3: 5.1
	FQDN Validation of Server Certificate	**ITI TF-1: 9.2.5** **ITI TF-2a: 3.19.6.1.4**
	BCP195 TLS Secure Transport Connection - All TLS Versions	**ITI TF-1: 9.2.6**
	BCP195 TLS Secure Transport Connection - TLS 1.2 Floor	**ITI TF-1: 9.2.7**
Secure Application	Radiology Audit Trail	RAD TF-1: 2.2.1 RAD TF-3: 5.1
	FQDN Validation of Server Certificate	**ITI TF-1: 9.2.5** **ITI TF-2a: 3.19.6.1.4**
	BCP195 TLS Secure Transport Connection – All TLS Versions	**ITI TF-1: 9.2.6**
	BCP195 TLS Secure Transport Connection - TLS 1.2 Floor	**ITI TF-1: 9.2.7**

EDITOR: *Add the following sections to Volume 1 section 9.2.*

9.2.5 FQDN Validation of Server Certificate Option

The FQDN Validation of Server Certificate Option applies the rules presented in RFC6125 when a client authenticates the server using an X.509 certificate in the context of Transport Layer Security (TLS).

In an environment where clients have implemented this option, a server's X.509 certificate must contain a subjectAltName entry of type DNS-ID, per RFC6125 Section 4.

See ITI TF-1: 9.4.1.2.2 and ITI TF-2a: 3.19.6.1.4.

Note: BCP195 recommends, but does not require, FQDN validation.

When an actor implements this option, it need not be capable of functioning without this validation.

9.2.6 BCP195 TLS Secure Transport Connection – All TLS Versions Option

Actors that support this option have the ability to both:

- Operate with the highest level of protection for the TLS-protected communication channel by adopting the IETF Best Current Practice (BCP195), and
- Continue to interoperate with systems that do not support BCP195, by downgrading from TLS version 1.2 to TLS version 1.1 or TLS version 1.0 and/or to less secure cipher suites under specific conditions that are allowed by BCP195.

This option adopts valuable recommendations from the IETF BCP195 while providing flexibility when communicating with an installed base.

An actor that supports the BCP195 TLS Secure Transport – All TLS Versions Option shall be able to comply with BCP195 from the IETF with the additional restrictions enumerated in ITI TF-2a: 3.19.6.1.5.

9.2.7 BCP195 TLS Secure Transport Connection - TLS 1.2 Floor Option

Actors that support this option have the ability to both:

- Operate with the highest level of cyber protection for the TLS-protected communication channel per the IETF Best Current Practice (BCP195 with TLS 1.2 and selected cipher suites), and
- Be restricted to use TLS version 1.2 [RFC5246] or higher.

This option adopts valuable recommendations from the IETF's BCP195, and prohibits less secure behavior. It is well suited for ensuring a high level of cyber protection.

An actor that supports the BCP195 TLS Secure Transport – TLS 1.2 Floor Option shall be able to comply with BCP195 from the IETF with the additional restrictions enumerated in ITI TF-2a: 3.19.6.1.6.

EDITOR: *Update Vol 2a Section 3.19.3*

3.19.3 Referenced Standards

DICOM:

- PS3.15 Security Profiles. Annex B1: The Basic TLS Secure Transport Connection Profile.

IETF:

- RFC2246 - Transport Layer Security (TLS) **Protocol Version** 1.0 ~~**and later revisions**~~
- **RFC4346 - Transport Layer Security (TLS) Protocol Version 1.1**
- **RFC5246 - Transport Layer Security (TLS) Protocol Version 1.2**
- ~~**RFC7525 - Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)**~~

- RFC3851 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification
- **RFC6125 - Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)**
- **BCP195 - Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), MAY 2015**

ITU-T:

- Recommendation X.509 (03/00). "Information technology - Open Systems Interconnection - The directory: Public-key and attribute certificate frameworks"

EDITOR: *Update Vol 2a 3.19.6.1.3 as follows*

Note that the inserted text includes adding two bullets to existing text. The addition of bullets is not indicated by bold/underline markup below.

3.19.6 Message Semantics

…

3.19.6.1.3 Other Certificate requirements

~~**The Secure Node shall not require any specific certificate attribute contents, nor shall it reject certificates that contain unknown attributes or other parameters. Note that for node certificates the CN often is a hostname, attempting to use this hostname provides no additional security and will introduce a new failure mode (e.g., DNS failure).**~~

The certificates used for mutual authentication shall be ~~**X509**~~ **X.509** certificates based on **either:**

- RSA key with key length in the range of 1024-4096, where the key length chosen is based on local site policy**, or**
- **BCP195 certificate recommendations**.

Maximum expiration time acceptable for certificates should be defined in the applicable security policy. The IHE Technical Framework recommends a maximum expiration time of 2 years.

The method used to determine whether a node is authorized to perform transactions is not specified. This may be use of a set of trusted certificates, based on some attribute value contained in the certificates, access control lists, or some other method. Using a certificate chain back to an external trusted certificate authority to determine authorizations is strongly discouraged.

EDITOR: *In Vol 2a, 3.19.6.1 Message Semantics, add three new subsections: 3.19.6.1.4, 3.19.6.1.5 amd 3.19.6.1.6*

3.19.6.1.4 FQDN Validation of Server Certificate Option

The FQDN Validation of Server Certificate Option applies the rules presented in RFC6125 when a client authenticates the server using an X.509 certificate in the context of Transport Layer Security (TLS).

A client, who is validating a server's identity, shall validate that the reference identifier present in a subjectAltName entry of type DNS-ID matches the source domain of the server, per RFC6125 Section 6. Note that the rules described in RFC6125 Section 6 require the validation to be performed based on the input source and the DNS-ID fully-qualified domain name.

In an environment where clients have implemented this option, a server's X.509 certificate must contain a subjectAltName entry of type DNS-ID, per RFC6125 Section 4.

3.19.6.1.5 BCP195 TLS Secure Transport Connection – All TLS Versions Option

An actor that supports the BCP195 TLS Secure Transport Connection – All TLS Versions Option:

- Shall be able to comply with BCP195. This implies that the implementation:
    - Utilizes the framework and negotiation mechanism specified by the Transport Layer Security protocol.
    - Supports TLS 1.0, and TLS 1.1, and TLS 1.2.
    - Should support the following cipher suites:
        - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- Shall be able to negotiate down to TLS 1.1 or TLS 1.0 following the BCP195 version negotiation criteria.

3.19.6.1.6 BCP195 TLS Secure Transport Connection – TLS 1.2 Floor Option

An actor that supports the BCP195 TLS Secure Transport – TLS 1.2 Floor Option:

- Shall be able to comply with BCP195. This implies that the implementation:
    - Utilizes the framework and negotiation mechanism specified by the Transport Layer Security protocol.
    - Supports TLS 1.2.
- Shall be able to restrict to use TLS 1.2
- Shall support the following cipher suites:
    - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384