Securing Connections for IBM Traveler Apps

Bill Wimer (bwimer@us.ibm.com), STSM for IBM Collaboration Solutions
December 13, 2016

IBM Technote Article #21989980

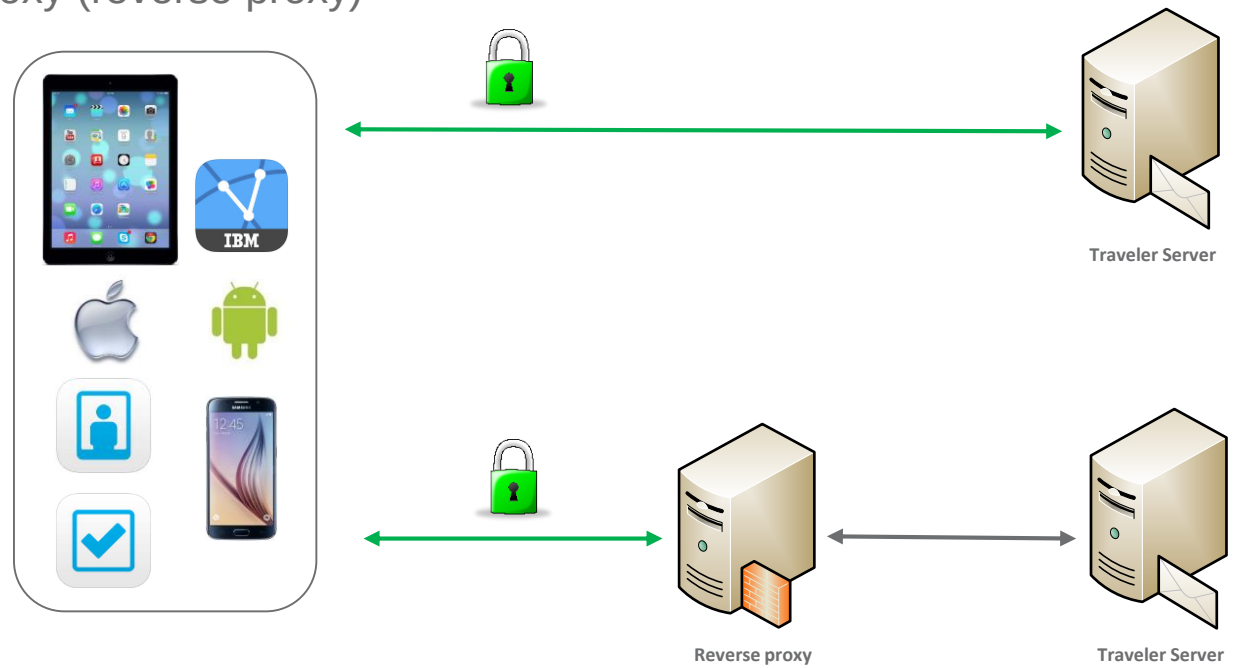
- Securing Connections for IBM Traveler mobile applications
  - https://www-01.ibm.com/support/docview.wss?uid=swg21989980
- Provides a list of minimum transport layer connection security requirements for the following mobile apps
  - IBM Verse for iOS
  - IBM Traveler Companion (iOS)
  - IBM Traveler ToDo (iOS)
  - IBM Verse for Android
- Focused on apps, but provides best security practices for any mobile connection
- Applies to customer running on premises IBM Traveler servers, or IBM SmartCloud customers that are using federated login using an Identity Provider

Why is this important?

- Cyber attacks are increasing, always searching for vulnerabilities to expose your private data
- Data transmitted and received over the internet over unencrypted or weakly encrypted connections is extremely vulnerable to compromise
- IBM does regular application scanning of our mobile apps, penetration testing of our Traveler server code and Ethical Hacking testing of our product
  - Strongly encrypted connections using valid certificates is required to ensure security for data traveling over the Internet
- Mobile OS vendors are removing support for vulnerable ciphers and protocols
  - Apple is requiring ATS for all public app store app submissions in 2017
  - Android recently removed the RC4 cipher when Android 7 was released
- IBM will be modifying our mobile apps in the future to **require** a secure connection that meets these minimum security requirements

What is the context of the '**connection**' here?

- Communications link between the mobile app and the TLS session endpoint
- TLS session endpoint may be the Traveler server if connecting directly
- Very often it is an edge proxy (reverse proxy)
  - IBM Mobile Connect
  - F5
  - Citrix Netscalar
  - MobileIron Sentry
  - Many others

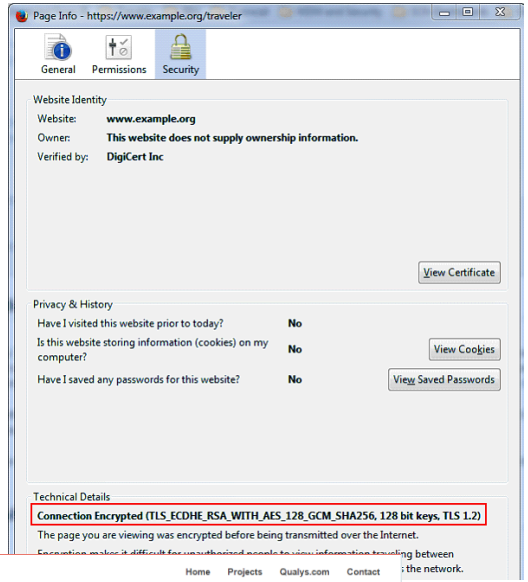


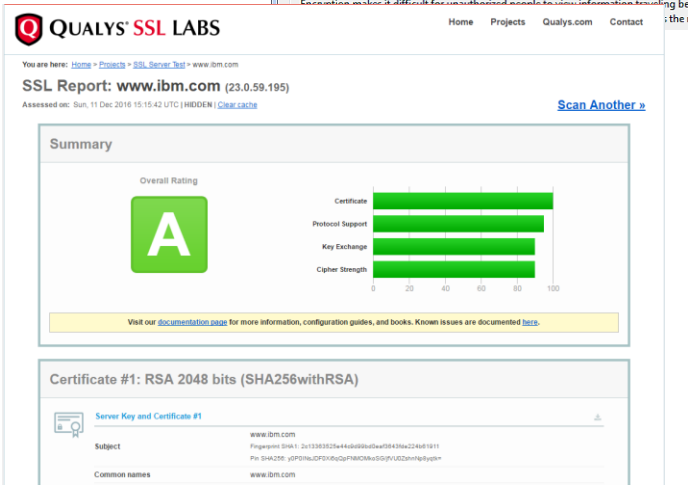
Minimum transport layer security requirements

1. Mobile apps must connect over HTTPS and not unencrypted HTTP
2. Server certificate cannot be expired or invalid
3. Server certificate Common Name (CN) or Subject Alternate Names (SAN) list must contain hostname which the mobile app is using to connect
4. Negotiated Transport Layer Security version must be TLS 1.2
5. Server certificate must be trusted
6. TLS cipher suite must support forward secrecy (see article for list)
7. Server leaf certificate must be signed with RSA 2048 bit or ECC 256 bit key (or higher)
8. Server leaf certificate hashing algorithm must be SHA256 (or higher)

How do I check my environment?

- Most browsers provide a mechanism to examine your certificate
  - Connect your browser to the Traveler URL in your environment
  - https://www.example.org/traveler
  - Technote provides step by step procedures using the FireFox browser
- Use an SSL Certificate checker, such as Qualsys SSL Labs
  - Note if the certificate and site are valid for Apple ATS connections





When do we have to implement these changes?

- Originally IBM was saying January 1, 2017 to match a similar deadline from Apple
- IBM now extending this deadline to ensure that customers have enough time to review their environments and ensure that beta apps with enforcement enabled can be validated.
- IBM will work with Apple to get the ATS requirement extended
- Expect only a short term extension, likely end of 1Q 2017, so validate that your environment is secure!

I found problems, how do I fix them?

Mobile Apps connecting to an edge proxy?

- Contact the edge proxy provider for assistance on mitigating the issue. Typically this means installing a new certificate or enabling TLS 1.2.

Mobile Apps connecting directly to IBM Traveler server?

- Depending on the problem, see related technote articles on how to mitigate
- The Domino server which is hosting Traveler MUST be running Domino 9.0.1 Fix Pack 5 or later. This is the version which provides a secure TLS stack.
  - See Download options for Notes & Domino 9.0.1 Fix Packs
  - http://www-01.ibm.com/support/docview.wss?uid=swg24037141

Fixing Problems – HTTPS is not enabled

#1 Mobile apps must connect over HTTPS and not unencrypted HTTP

- Enable SSL (TLS) on your Domino web server
  - See How to set up SSL using a third-party Certificate Authority (CA) and follow the section called **Steps for Configuring SSL**
  - http://www-01.ibm.com/support/docview.wss?uid=swg21268695
- You will need to create a Domino keyring file containing a valid certificate prior to turning on SSL
- Both HTTP and HTTPS can run on your Domino server at the same time

Fixing Problems – Certificate is invalid or weak

#2 Server certificate cannot be expired or invalid
#3 Server certificate Common Name or Alternate Names list must contain hostname which the mobile app is using to connect
#7 Server leaf certificate must be signed with RSA 2048 bit or ECC 256 bit key (or higher)
#8 Server leaf certificate hashing algorithm must be SHA256 (or higher)

- Create and deploy a valid, strong certificate
  - See Generating a keyring file with a third party CA SHA-2 cert using OpenSSL and kyrtool
  - https://www-10.lotus.com/ldd/dominowiki.nsf/dx/3rd_Party_SHA-2_with_OpenSSL_and_kyrtool?open
- Install the keyring on your Traveler server(s)
  - How to set up SSL using a third-party Certificate Authority (CA)
  - http://www-01.ibm.com/support/docview.wss?uid=swg21268695

Fixing Problems – TLS 1.2 and ciphers

#4 Negotiated Transport Layer Security version must be TLS 1.2
#6 TLS cipher suite must support forward secrecy

- Upgrade the Domino server which is hosting Traveler to run Domino 9.0.1 Fix Pack 5 or later
  - See Download options for Notes & Domino 9.0.1 Fix Packs
  - http://www-01.ibm.com/support/docview.wss?uid=swg24037141
- This version automatically enables TLS and the required ciphers which support forwarding secrecy
- No additional configuration is required

Fixing Problems – Certificate is not trusted

#5 Server certificate must be trusted

- IBM recommends using a certificate from an external Certificate Authority
  - Validate with the 3rd party CA that their certificate is compatible and preinstalled on iOS and Android devices
  - These certificates are automatically trusted on the device
- Can I use a self signed certificate or one signed by my local certificate authority?
  - Technically possible, but requires some additional steps
  - Must distribute the certificate (or root and intermediate certificate) to the mobile devices
    - MDMs can provision certificates to mobile devices
    - End users can manually install by clicking the certificate in an email or website
  - See Generating a keyring file with a self-signed SHA-2 cert using OpenSSL and kyrtool
  - https://www-10.lotus.com/ldd/dominowiki.nsf/dx/Self-signed_SHA-2_with_OpenSSL_and_kyrtool?open

Do I need to make any changes if I am using an AppTunnel with a MobileIron Sentry?

- The MobileIron Sentry has a feature called AppTunnel
  - Allows app level VPN connections from Verse, ToDo, and Companion to an internal Traveler server
- It is same topology as a reverse proxy environment
  - Connection between app and Sentry must be secured
  - It is NOT mandatory that the connection between the Sentry and the internal Traveler server is secured

Beta testing – try out any changes before they go live

- Best way to validate that your environment meets requirements
- Verse for Android
  - Anyone can signup by logging into Google Play, find the Verse for Android app and click **Become a Tester**
- Verse for iOS, ToDo and Companion
  - Testing is done through the Apple TestFlight app
  - Available via invitation only, so send an email to **heyibm@us.ibm.com** requesting access
  - For each individual tester, provide IBM with:
    Company Name
    Tester Name
    Tester's email address associated with their Apple ID
    Application to test (Any or all of Verse for iOS, ToDo and Companion)
- Look for announcements mid January 2017, expected to release beta updates with changes

Questions?

Please contact us using email to heyibm@us.ibm.com if we cannot get your question answered today!