Connected X Cyber Security

Vehicle to Cloud Connectivity Security Requirements

Version 1.1

UNCONTROLLED COPY IF PRINTED

FORD CONFIDENTAL

1 Version History & Table of Contents

1.1 Table of Contents

1.3 Revision History:

Version	Revision Date	Description of Change	Affected Sections	Author
V0.1	7/15/2018	Initial Version	N/A	Matt Burris
V1.0	11/9/2018	First release	All	Matt Burris
V1.1	1/14/2019	Added 2.1.8, 2.1.9	2.1.8, 2.1.9	Matt Burris

2 Requirements

2.1 Functional Requirements

2.1.1

###CLOUD_SEC_00001### TLS

The minimum version of TLS implemented shall be TLS 1.2. No module that uses cellular connectivity, nor the SDN, shall allow negotiation to a lower version or the usage of cipher suites other than those agreed upon.

Requirement ID: ###CLOUD_SEC_00001###			
Rationale			
The Transport Layer Security (TLS) standard shall be used to provide authentication of senders and recipients, and integrity and confidentiality of data sent over TCP/IP. Using the latest version of TLS mitigates known man-in-the-middle attacks and replay attacks.			
Acceptance Criteria			**V&V Method**
• Module is running TLS 1.2 • System shall verify that the TLS endpoint URL and expiration date is specific to its connection where applicable • Module does not support any lower version of TLS • Pinning shall be used where possible to associate a specific host with each certificate/public key			DV Testing
Notes			
Use of TLS 1.2 is a critical enabler for the TLS-based replay solution to known replay attacks. If a lower version of TLS must be used, an alternative solution to mitigate the threat of replay attacks (such as implementation of SyncP message IDs) must be implemented. Refer to the Key and Certificate Management Specification for additional requirements.			
Version	**Date**	**Author**	**Change**
1.0	7/15/2018	Mburris6	Initial version

2.1.2

###CLOUD_SEC_00002### TLS Timeout

All TLS sessions shall timeout no later than six hours after they were initiated. A new TLS handshake shall be performed if more than six hours has passed.

Requirement ID: ###CLOUD_SEC_00002###			
Rationale			
Maintaining a TLS session for extended periods of time allows attackers more time to target it, putting the integrity of the connection at risk.			
Acceptance Criteria			**V&V Method**
• TLS session performs a full handshake to resume after it has been six hours since the last time a packet was sent			DV Testing
Notes			
TLS sessions may resume with a full handshake if less than six hours has passed since the connection was initiated.			
Version	**Date**	**Author**	**Change**
1.0	11/9/2018	Mburris6	Initial version

2.1.3

###CLOUD_SEC_00003### Message Level Encryption

Command and control messages sent to, and from, the vehicle shall be signed, and encrypted using Ford's proprietary SyncP standard.

Requirement ID: ###CLOUD_SEC_00003###			
Rationale			
Communications sent over cell may contain sensitive data. Using SyncP signing and encryption provides integrity, confidentiality and availability. Keys shall be protected on the backend by a HSM, (e.g. Ford, within the SDN, etc.).			
Acceptance Criteria			**V&V Method**
• Payloads must be digitally signed from the cloud endpoint to the target microcontroller on the vehicle • Digital signature shall be decoded using the same PSK that is used for message level encryption			DV Testing
Notes			
Version	**Date**	**Author**	**Change**
1.0	7/15/2018	Mburris6	Initial version

2.1.4

###CLOUD_SEC_00004### TLS Cipher Suites

All TLS communications shall only support the following cipher suites, listed in order of priority:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

Requirement ID: ###CLOUD_SEC_00004###			
Rationale			
The strength of encryption used in a TLS connection is dependent on the cipher suite used. Using a strong cipher ensures that the connection is adequately encrypted.			
Acceptance Criteria			**V&V Method**
• TLS connection utilizes highest possible cipher suite listed • TLS connection does not support use of any other cipher suites • 2048-bit RSA crypto • Root CA cert with up to 30 years before expiration (individual certs on the backend will have a shorter lifespan, e.g. 2 years)			DV Testing
Notes			
Version	**Date**	**Author**	**Change**
1.0	11/7/2018	Mburris6	Initial version

2.1.5

###CLOUD_SEC_00005### TLS Compression

TLS-level compression shall not be used.

Requirement ID: ###CLOUD_SEC_00005###				
Rationale				
Use of compression is an enabler for the Compression Ratio Info-leak Made Easy (CRIME) exploit, which allows an attacker to access user authentication cookies from HTTPS for session hijacking.				
Acceptance Criteria				**V&V Method**
• System has compression disabled for all TLS connections				DV Testing
Notes				
Please refer to **NIST Special Publication 800-52 for more details**.				
Version	**Date**	**Author**	**Change**	
1.0	11/9/2018	Mburris6	Initial version	

2.1.6

###CLOUD_SEC_00006### TLS Certificate Authorities

TLS connections shall only use Ford-approved certificate authorities.

Requirement ID: ###CLOUD_SEC_00006###				
Rationale				
The security of non-Ford CAs cannot be verified. Using a non-Ford CA could leave TLS connections vulnerable to mishandled CAs.				
Acceptance Criteria				**V&V Method**
• System only uses Ford-approved CAs				DV Review
Notes				
Version	**Date**	**Author**	**Change**	
1.0	11/9/2018	Mburris6	Initial version	

2.1.7

###CLOUD_SEC_00007### mTLS Certificate Pinning

Where mutual TLS authentication is being used, the system shall use certificate pinning, with OSCP responses, to verify the identity of each host.

Requirement ID: ###CLOUD_SEC_00007###				
Rationale				
Certificate pinning allows the client to verify the identity of the host it's connecting to prevent spoofing and man-in-the-middle attacks.				
Acceptance Criteria				**V&V Method**
• Application inspects certificate at runtime to verify the identity of the server • Application closes the connection if the identity cannot be verified/the certificate is unexpected				DV Testing and Review
Notes				
Version	**Date**	**Author**	**Change**	
1.0	11/9/2018	Mburris6	Initial version	

2.1.8

###CLOUD_SEC_00008### Host Authentication

Module connecting to external systems shall verify that the host URL matches the Subject and Subject Alternative Name fields in the TLS server certificate. If the hostname in the certificate does not match the host URL, the module shall reject the connection.

<table>
<tr><td colspan="4"><b>Requirement ID: ###CLOUD_SEC_00008###</b></td></tr>
<tr><td colspan="4"><b>Rationale</b></td></tr>
<tr><td colspan="4">Without verifying the host URL there is no guarantee that the client module is connecting to the correct, trusted external system. Modules must only connect to specific, trusted external systems.</td></tr>
<tr><td colspan="3"><b>Acceptance Criteria</b></td><td><b>V&V Method</b></td></tr>
<tr><td colspan="3">• Module verifies the hostname of the service its connecting to matches the hostname in the Server Certificate
• Module rejects any connection where the hostname does not match the hostname in the Server Certificate</td><td>DV Testing and Review</td></tr>
<tr><td colspan="4"><b>Notes</b></td></tr>
<tr><td><b>Version</b></td><td><b>Date</b></td><td><b>Author</b></td><td><b>Change</b></td></tr>
<tr><td>1.1</td><td>1/10/2019</td><td>Mburris6</td><td>Added requirement</td></tr>
</table>

2.1.9

###CLOUD_SEC_00009### Verify Peer

Any module connecting to external systems shall use “Verify Peer” or similar function to validate the authenticity of the certificate when negotiating a TLS connection. If verification fails, the module shall reject the connection.

<table>
<tr><td colspan="4"><b>Requirement ID: ###CLOUD_SEC_00009###</b></td></tr>
<tr><td colspan="4"><b>Rationale</b></td></tr>
<tr><td colspan="4">Without verifying the certificates a module could potentially establish a connection with an untrusted server.</td></tr>
<tr><td colspan="3"><b>Acceptance Criteria</b></td><td><b>V&V Method</b></td></tr>
<tr><td colspan="3">• Module authenticates the presented Server Certificate to ensure it matches a certificate kept in its internal store
• Verify Peer is used to validate certificate authenticity
• Connections are rejected when certificate cannot be validated</td><td>DV Testing and Review</td></tr>
<tr><td colspan="4"><b>Notes</b></td></tr>
<tr><td><b>Version</b></td><td><b>Date</b></td><td><b>Author</b></td><td><b>Change</b></td></tr>
<tr><td>1.1</td><td>1/10/2019</td><td>Mburris6</td><td>Added requirement</td></tr>
</table>