

Final Public Report

Document Title	<i>LOGIIC Mobility Project Public Report</i>
Version	<i>Version 1.0</i>
Primary Author	<i>A. McIntyre (SRI)</i>
Distribution Category	LOGIIC Approved For Public Distribution
Approval Status	Approved For LOGIIC Use
Reviewed by AF Legal	6/14/17
Approved (date)	6/14/17
Approver (EC or AF)	EC
Digital Signature for PDF	

EXECUTIVE SUMMARY

The LOGIIC¹ Consortium was established by members of the oil and gas industry in partnership with the Cybersecurity Research and Development Center (CSRDC) of the U.S. Department of Homeland Security (DHS), Science and Technology Directorate (S&T) to review and study cybersecurity issues in Industrial Automation and Control Systems (IACS) which impact safety and business performance as they pertain to the oil and gas sector. LOGIIC has sponsored research initiatives that involve the interests of oil and gas sector stakeholders.

The LOGIIC Mobility Project focused on the assessment and analysis of Industrial Automation and Control Systems (IACS) data movement to mobile devices. These devices may exist on the plant floor or entirely offsite. This project evaluated the security of the device, application, base server architecture, data at rest, and data in motion.

In the recent past, mobility options have expanded well beyond the enterprise level and into the industrial control space. Speed and efficiency of decision-making has created a demand for increased awareness of real time activities in the control center, without the physical boundaries of the site. To meet this demand, automation vendors and third party vendors have created a host of mobility applications to display the activities of the IACS system on mobile devices. Some applications present data, while others provide the capability to perform control functions.

LOGIIC conducted a series of research surveys and studies to identify product offerings in the marketplace, their applicability to Industrial Automation and Control Systems (IACS) environment, and their cybersecurity capabilities. Hands-on assessment activities conducted in an IACS environment evaluated the security of mobile solutions.

The scope of this project included an assessment of risks in data transmission, end devices and/or applications, mobile architecture, and operational use. To identify technical findings and risks, LOGIIC conducted hands-on testing activities. The mobility solutions assessed contained combinations of native applications, iOS and Android, and web-based applications accessible from common browser technology. The objectives of these activities focus on answering key technical questions related to the use of mobility in IACS and operational environments.

The objective of this report is to convey important factors that should be weighed when considering a mobility solution in the IACS environment and to support a dialogue between asset owners and automation vendors. This project identified technical and operational findings in mobility solutions assessed in an IACS laboratory environment. These findings include:

- **Common Risks in Native Applications**

These include risks that exist due to the application not making use of the platform's security options, or those options are not present in the platform. Examples include certificate validation, pinning, jailbreak detection, debug detection, Automatic Reference Counting, and other mechanisms.

¹ LOGIIC - Linking the Oil and Gas Industry to Improve Cybersecurity.

- **Common Risks in Web Applications**
 Like native applications, web applications have common risks. While they may require a more sophisticated threat and effort, these risks can have a high impact if they are successfully exploited. Examples include cross site scripting vulnerabilities, session handling and termination risks, and mishandled cookies.
- **Platform Risks**
 Throughout the assessments, conclusions were derived about the attack surface available on the differing mobile device platforms. At the time of testing, the attributes of the Android platform led to a greater attack surface than iOS. Android and iOS have differing Transport Layer Security (TLS) version requirements, key handling, and signature verification processes.
- **Connectivity**
 A spectrum of vendor solutions exist that vary in their design and connection to the IACS network. Many vendors offer 'internal' and 'external' connection options. Vendors also differ in the central management of the solution. Asset owners should perform a risk analysis, based on their own operations, to select a solution within the spectrum of vendor offerings that best meets objectives within their security and policy framework.
- **Nature of Mobility**
 A number of security and operational findings can be identified from the very nature of a mobile solution. These solutions are implemented to move data and situational awareness information outside the physical boundaries of a control center or site. Technical mechanisms and operational policies that mitigate risk and control access to high-value data must be considered. A level of ongoing management of numerous mobile devices must also be considered by the asset owner.
- **Device Handling**
 Mobile devices can be difficult to fully protect, both from a physical security aspect, and a protection of unauthorized view. Display of data or alerting would need to be carefully considered and controlled by the user. Single-user devices may be necessary to prevent unauthorized access to data. If a mobile device retains data, alerts, login information, or other application data, policies and procedures should exist for decommissioning or reuse of a device.
- **Supply-Chain Components**
 With the use of web and application tools and components, new security risks may be introduced that become inherent to the broader solution. The efficiency and flexibility that these tools can add to the development cycle are beneficial to the vendor and ultimately to the end user. However, neither the vendor nor the end user may have the ability to mitigate these vulnerabilities.
- **Installation, Maintenance, and Management**
 As with the implementation of any new technology in the IACS environment, the installation and ongoing maintenance of the solution should be considered. Once implemented, ongoing management and maintenance should be considered at several levels including the server, application, users, and devices.

The implementation of new technologies in a critical operational environment requires careful evaluation and planning to ensure protection of core IACS assets, data, and operational stability. This project concludes that implementing mobility in this environment can be done securely if technical and design aspects are managed with appropriate security controls. Likewise, life-cycle management is required to ensure a level of security is maintained in the mobile architecture.

Table of Contents

Executive Summary	2
1 Introduction	6
2 Project Summary and Background	7
3 Technical Approach	10
Assessment Methodology	10
Assessment Approach	10
Analysis of Findings	12
4 Assessment Findings	13
Technical Risks.....	13
Connectivity	14
Operational Findings	14
5 Conclusions	17
Appendix	20
Acronyms.....	20
Acknowledgements.....	20
Distribution	20

Table of Figures

Figure 1: Internal Connection.....	8
Figure 2: External Connection	9
Figure 3: Test Scenarios and Attack Vectors	11
Figure 4: Test Tools for Web Apps	11
Figure 5: Test Tools for Android and iOS.....	12

1 INTRODUCTION

The LOGIIC program was established to review and study cybersecurity issues as they pertain to the oil and gas sector, and has sponsored research initiatives that involve the interests of oil and gas sector stakeholders. LOGIIC initiatives are applicable to many industries with control systems.

The LOGIIC Mobility Project focused on the assessment and analysis of Industrial Automation and Control Systems (IACS) data movement to mobile devices. These devices may exist on the plant floor or entirely offsite. This project evaluated the security of the device, application, base server architecture, data at rest, and data in motion.

In the recent past, mobility options have expanded well beyond the enterprise level and into the industrial control space. Speed and efficiency of decision-making has created a demand for increased awareness of real time activities in the control center, without the physical boundaries of the site. To meet this demand, automation vendors and third party vendors have created a host of mobility applications to display the activities of the IACS system on mobile devices. Some applications present data, while others provide the capability to perform control functions.

Based on surveys of the LOGIIC members, expanded use of mobile solutions is likely to occur over the next two years. An understanding of the security aspects and operational requirements of these solutions will assist asset owners in choosing a solution that best fits their risk portfolio.

Expanding upon the present day focus on securing control center perimeter networks, an analysis must be performed on the security ramifications of moving IACS data, and possibly control, to mobile devices. Deploying mobile capabilities requires significant effort and cost. Like other large technology roll-outs, a risk assessment of these mobile technologies should occur to fully understand the potential vulnerabilities, needed mitigations, and life-cycle management aspects of using mobility in the IACS environment.

LOGIIC conducted a series of research surveys and studies to identify product offerings in the marketplace, their applicability to an IACS environment, and their cybersecurity capabilities. Solutions provided by automation vendors and third-party vendors were included in the project.

Given the rapid deployment of mobile technology in the operational space and the interests of the LOGIIC members, this project was developed to present an understanding of security risks and needed mitigations in an implementation of mobile solutions that handle IACS data. This project identified security aspects that must be considered when implementing a mobile solution for the purpose of optimizing IACS decisions and increasing awareness, as well as the needs for overall life-cycle management

The objective of this report is to convey important factors that should be considered when selecting and implementing a mobility solution in the IACS environment. The intended audience for this report is the IACS technical and security communities, and automation and security vendors.

2 PROJECT SUMMARY AND BACKGROUND

The LOGIIC Mobility Project was established and defined by the LOGIIC members (Technical Team, Executive Committee, and the DHS sponsor). Automation vendors were engaged and invited to participate in an assessment.

The broad project objective is to evaluate the mobility solutions currently available in the market. These solutions provide connectivity to the Industrial Automation and Control System (IACS) environment from outside the physical boundaries of the control center. Mobility solutions provide data and connectivity to the core IACS environment to support decisions and increase situational awareness.

A data transfer survey conducted in December 2014 showed that data movement outside the IACS environment was a significantly important topic to the LOGIIC members. That study included mobility as a sub-topic for data transfer. In November 2015, a second survey was conducted that focused on the use of mobility and collected the opinions of the LOGIIC members. Findings indicated that members recognize the rapid market and technology changes with mobility, as well as its role in movement of data outside the core control center.

Findings of the member survey included:

- Over half of the LOGIIC member companies are currently using a mobility solution
- Many members plan to implement a new solution or expand their current solution in the near future.
- Automation vendor accreditation is clearly important to the members
- Members are tentative about the capabilities that should be available in a mobility solution
- While all agree that IACS staff should be able to read data using a mobile tool, only some would consider the ability to perform control remotely

The scope of this project included an assessment of risks in data transmission, end devices and/or applications, mobile architecture, and operational use. To identify technical findings and risks, LOGIIC conducted hands-on testing activities. The objectives of these activities focus on answering key technical questions related to the use of mobility in IACS and operational environments.

- What security controls are required on the end devices? Are some devices more secure than others?
- What is provided by the vendor? Can a third-party mobile device be used?
- What security controls are required to secure the server or application?
- How do the mobile devices connect to the server?
- What functionality is provided within the application? Read data only, or perform control?
- What security controls are required to maintain the integrity of data in transit?
- Is data stored on the device?
- What authentication mechanisms are in place?

Nearly all automation vendors provide a form of mobility for IACS data. These capabilities can be at the application level or full hardware devices. This project focused on technologies that are commercially available from automation vendors and third-parties. App-only solutions available on iTunes or the App Stores were not included.

Vendors offer different connectivity options. Unless purely hosted and maintained by the vendor at their site, most mobile solutions are implemented at the asset owner site. Vendors offer internal and external connection options. Internal connections indicate that a mobile user is wirelessly connected to the IACS network, such as plant floor, or demilitarized zone (DMZ) at Level 3.5. Some solutions offer an internal user connection at the enterprise Level 4 (Figure 1). External connections are typically mobile users who are connecting through an Internet connection and through Level 4 to reach a server (Figure 2). Exact definitions vary depending upon the vendor.

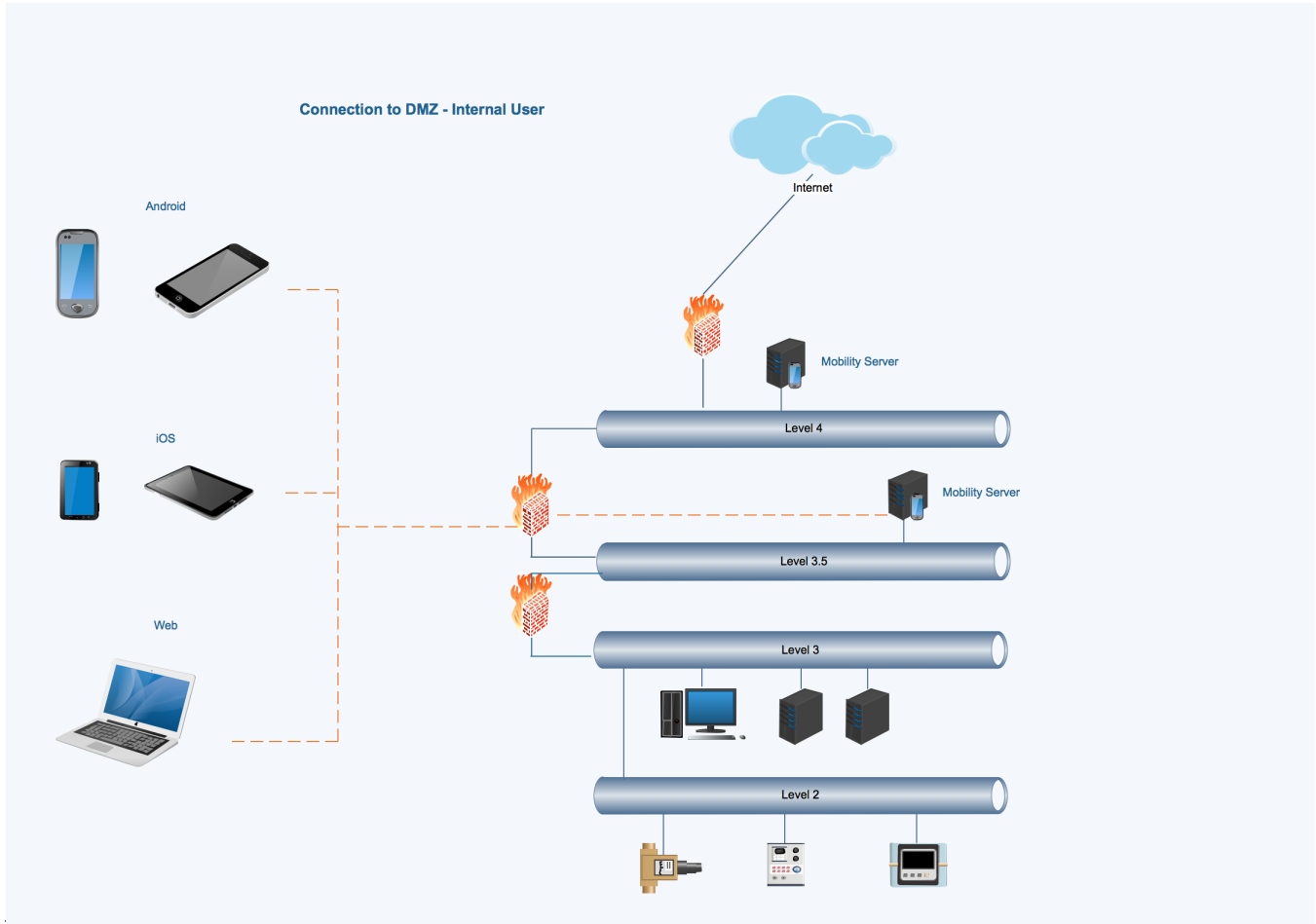


Figure 1: Internal Connection

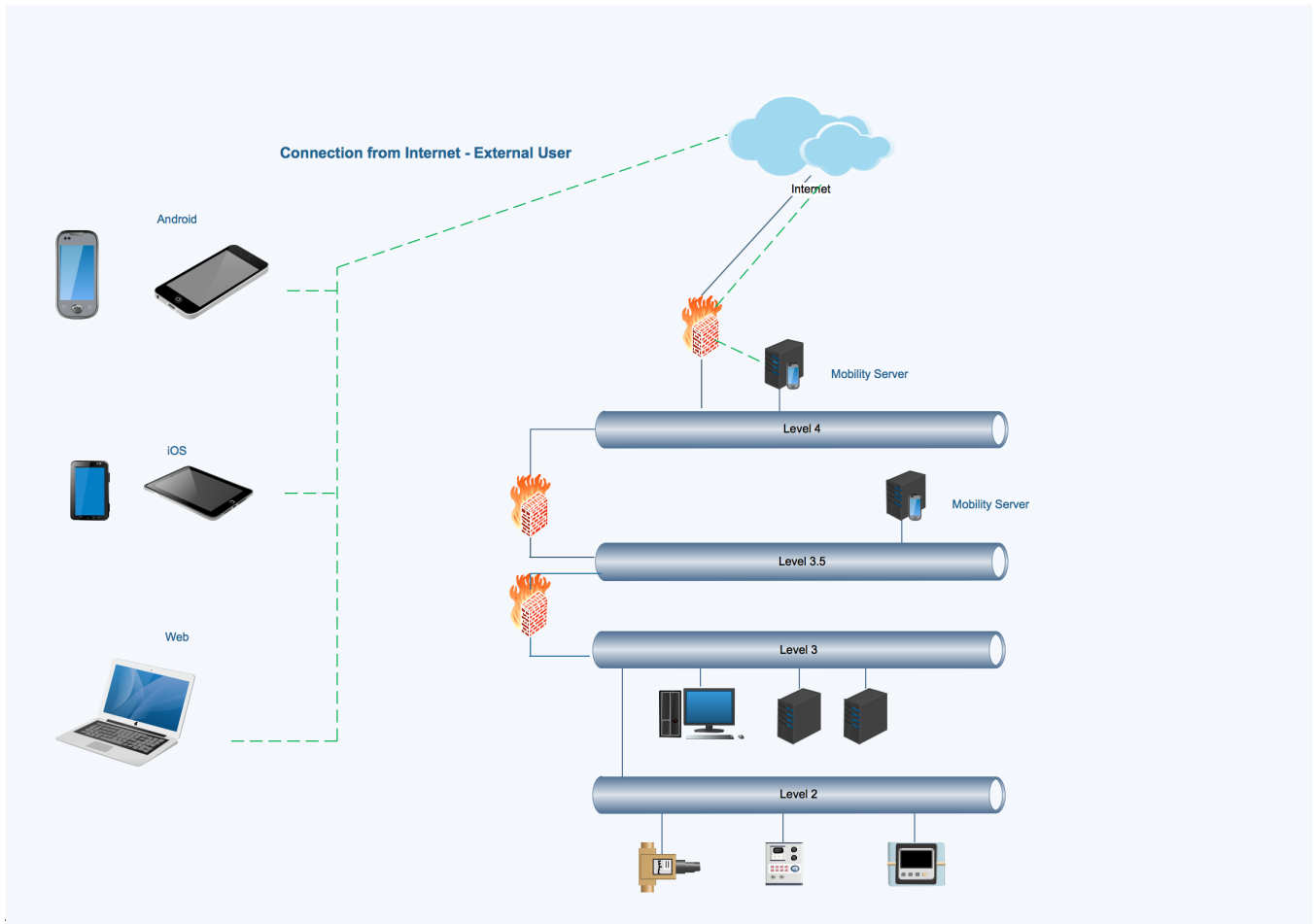


Figure 2: External Connection

3 TECHNICAL APPROACH

Technical surveys, market reviews, and engagement with automation vendors contributed to defining the project scope and individual test scenario. Assessment and analysis followed a standard approach and used previously tested assessment methodologies. The details of the approach are outlined in this section.

Assessment Methodology

LOGIIC consistently bases all assessments on the foundational risk equation, where $Risk = Threat \times Vulnerability \times Consequence$, to ensure that all testing expresses a plausible threat that is applicable to the oil and gas industry. The assessment scope and individual test scenarios were defined by characterizing risk in terms of threat, vulnerability and consequence.

After selecting an automation vendor and a subject matter expert (SME) in testing data transfer technologies, the team developed a Test Plan that identified test scenarios and rules of engagement. The automation vendor provided network and design diagrams in advance. Because test cases were developed with this architecture knowledge, the assessments were considered partial-knowledge assessments. While in the laboratory, each participating vendor provided a demonstration and overview of their systems.

The assessments for each device or system of devices used the following high-level steps:

1. Reconnaissance
2. Information Capture/Data Retrieval Attempts
3. Targeted Attack
4. Denial of Service (DoS)

As with the standard LOGIIC assessment approach, attacks were only considered viable if they were traceable and reproducible.

While technical activities, such as reconnaissance and attack, formed the basis for most of the assessment findings, observations about interactions with devices, setup, and troubleshooting provided valuable information for the LOGIIC team. Performance of security features, resilience, and robustness were measured by technical results and by general observations during the assessment.

Assessment Approach

Multiple mobility solutions provided by automation vendors and relevant third-party vendors were assessed during this project. The LOGIIC team and SME developed test vectors and test scenarios to answer key questions of specific interest to the LOGIIC members. Example test vectors were used by the SME to develop broader test scenarios and select applicable tools (Figure 3).

Example Test Scenarios and Attack Vectors
Packet captures (between mobile application and server)
Data storage and leakage
Insecure communication
Application authentication and authorization
Cryptographic algorithm and key management
Session management
Client-side injection
Server-side controls
Reverse engineering and binary protections
Code analysis (fuzzing, user input, etc.)
Default application configuration
Applicable existing exploits

Figure 3: Test Scenarios and Attack Vectors

The SME conducted the test scenarios using their attack methods, payloads, and equipment. Each assessment included vendor setup and a pre-work phase conducted by the SME. The pre-work phase included connection of test equipment, network validation, reconnaissance, and traffic capture. During the pre-work and testing phases, the SME used publicly available tools and SME-developed customized scripts.

The mobile solutions tested offered native applications in Android and iOS platforms and web-based applications. These platforms created different attack vectors that required various tools. The following tools were used on these platforms during the pre-work and testing phases (Figure 4).

Test Tools
Web App Tools
Wireshark® (Network traffic monitor)
Burp Suite (Web Application Testing Platform)
SSLstrip (HTTPS stripping attacks)
Nessus® (Vulnerability scanner)
SQLiteSpy (Evaluate sqlite database files)
sqlmap® (SQL injection tool)
Kali Linux™ (Linux distribution for penetration testing)
SoapUI Pro (Automated REST service scanner)

Figure 4: Test Tools for Web Apps

Test Tools
Android and iOS Tools
Wireshark® (Network traffic monitor)
Burp Suite (Web Application Testing Platform)
ADB (Android debugger)
Jadx (Dex to Java decompiler)
SSLstrip (HTTPS stripping attacks)
Nessus® (Vulnerability scanner)
Apktool (Android APK reverse engineering tool)
drozer (Android security framework tool)
SQLiteSpy (Evaluate sqlite database files)
Otool (Object file display tool)
ondeviceconsole (Tool to view system log)
keychain_dumper (Tool to check keychain)
Cycript (iOS application explorer)
sqlmap (SQL injection tool)
Kali Linux™ (Linux distribution for penetration testing)
KingoRoot (Android application to root the phone)
Big Boss Tools (iOS jailbreak application)
Pangu (iOS jailbreak)

Figure 5: Test Tools for Android and iOS

White cell² activities during the assessment were performed by the LOGIIC Technical Lead. All test techniques, steps, results, and observations were noted during the assessment.

Analysis of Findings

The technical conclusions described in the following sections of this report are based on a series of inputs and data sources, including

- Background research conducted under the project
- Product documentation, technical briefings, and design details from the automation vendor
- Assessment test scenario results
- Background information on each threat vector provided by the SME
- Observations during the assessment
- Functional and usability testing

In addition to technical test findings, operational observations also contributed to overall project conclusions. These observations included usability, ease of setup, maintenance requirements, and skillsets required to maintain and use the system. These findings assisted LOGIIC members in determining a return on investment if they choose to implement this technology in an operational setting.

² A white cell is an independent person who collects findings and records events during the assessment. White cell activities are not typically performed by a red team member or a vendor.

4 ASSESSMENT FINDINGS

The assessment produced numerous technical and operational findings. This section presents technical and operational findings and key discussion points. Approximately 50 to 80 individual test cases were conducted during each assessment, depending on the test architecture. Findings from each test case were reviewed and ranked by consequence-based severity and likelihood. These technical findings were merged with operational conclusions, and observations were categorized into broader areas. Each area is relevant when considering the selection and implementation of a mobility solution.

Technical Risks

The mobility solutions assessed contained combinations of native applications, iOS and Android, and web-based applications accessible from common browser technology. Individual tests and findings were grouped in these application categories, allowing for broader conclusions to be formed. Common technical risks existed across many of the solutions tested. These are discussed below.

- **Common Risks in Native Applications**

Many low-impact, but common, high-likelihood attack vectors were present across the solutions tested, including

- No validation of the certificate and connection to a legitimate server
- No certificate pinning, associating a host with a particular certificate (not applicable to Android)
- No jailbreak detection to ensure that restrictions that prevent a user from fully accessing the root level of the device have not been removed
- No debug detection, allowing an adversary's tools to attach to the application process for further attack
- No obfuscation of keys or credentials in the application code
- No implementation of Automatic Reference Counting (ARC) memory management, which reduces the risk of vulnerabilities due to memory allocation
- Not using the latest versions of TLS

- **Common Risks in Web Applications**

Like native applications, web applications have common risks, which are often high in impact and low in likelihood. Because these risks can have a high impact if they are successfully exploited, they require a more sophisticated threat and effort. Web application risks include

- Vulnerabilities to cross-site scripting and reflected cross-site scripting
- Session handling and termination risks. Terminating a session when a user logs out or after the appropriate timeout is critical to ensuring that residual sessions cannot be hijacked
- Cookie management. To ensure that an adversary cannot leverage a mishandled cookie to use a session, cookies should not be usable after their expiration or be created by a request from an expired token

- **Platform Risks**

Throughout the assessments, conclusions about the attack surface available on the differing mobile device platforms became clear. At the time of testing, the attributes of the Android platform led to a greater attack surface than iOS. For example, requirements for TLS versions in Android applications are lower than those for iOS, which could allow for a less secure application to be developed and distributed on the Android platform.

Key handling is another example regarding the differences between the Android and iOS platforms. In iOS, keys are stored in the iOS Keychain; in Android, they are stored in the Android Keystore. In iOS, keys in the Keychain are only accessed by the associated application. In Android, the entire default Keystore is accessible by all applications.

Signature verification testing also identified differences between Android and iOS. In cases where signature checking does not occur and a developer-signed certificate is in use, an attacker could create a new certificate, modify code, and perform other actions, such as installing a keylogger to capture credentials for use in a spear-phishing attack. If signature checking is invoked, iOS performs the check throughout the entire process of using the application, but Android, however, does not perform continual checking. Even if signature checking is invoked on the Android platform, it performs the check at a single point in the user's interaction with the application. At that point, credentials could already have been captured using the certificate modification process described above. There are no options within Android to change the signature verification, so mitigation choices are limited. This example illustrates how a platform-specific vulnerability affects a vendor solution and how an asset owner might evaluate that risk based on their current and future use of specific mobile devices.

Regardless of platform (iOS or Android) or the use of web or native applications, securing servers and data hosts within the IACS environment is critical. As for all systems in this environment, maintaining a secure design through good coding practices, patches, and updates is an important aspect of the entire mobile solution.

Connectivity

Mobility is an evolving technical area within data movement from IACS environments. This evolution has resulted in a spectrum of vendor solutions that vary in their design and connection to the IACS network. Many vendors offer internal and external connection options. While exact vendor definitions vary, mobility in IACS is expanding to allow remote users to receive IACS data and situational awareness through an Internet connection. When selecting and implementing a mobile solution, asset owners should conduct a risk analysis to assess the value of their data and operational-state information.

Vendors also differ in their management of the solution. Some vendors assist asset owners with management of the mobile solution. In fact, some solutions are entirely managed by the vendor at their location, allowing asset owners to connect remotely and only manage the applications on their mobile devices. This model shifts responsibilities of access control, management, and monitoring to the vendor, rather than the asset owner. Other vendor solutions are implemented and entirely managed by the asset owner at their site. Asset owners should perform a risk analysis, based on their own operations, to select a solution within the spectrum of vendor offerings that best meets their objectives within their security and policy framework.

Operational Findings

Operational findings, collected throughout the assessment, include installation, management, and human interactions with the solution.

- **Nature of Mobility**

A number of security and operational findings can be identified from the nature of mobile solutions, which move data and situational awareness information outside the physical boundaries of a control center or site. While these findings may appear obvious, the mobility model, in which potentially high-value data is handled on a small, movable device, is contrary to past best practices and standards. Technical mechanisms to mitigate risk and control access to this data must be considered; moreover, dependencies on adherence to user-handling policies may become critical to maintaining overall security.

The asset owner must also consider the ongoing management of numerous mobile devices. Regardless of the selected vendor solution, implementation of a mobile solution requires management of devices, user accounts, permissions, and device updates. A solution must be coordinated and integrated with existing mobility policies and management plans, and ongoing device management and security maintenance should be included in a return-on-investment analysis of a mobile implementation.

- **Device Handling**

Mobile devices can be difficult to fully protect from a physical access and protection from unauthorized view. For example, if an application provides alerts, the alerts may appear on a mobile device screen even when the device is locked. Display of data or alerts need to be carefully considered and controlled by the user.

Single-user devices may be necessary to prevent unauthorized access to data. Even if devices are shared with different login credentials, stored data or displayed application alerts may be accessible by any user. It should be assumed that if an authorized person has physical access to a mobile device, he or she may be able to access the data. Unfortunately, physical protection of the device and single-user access is often controlled only through operational user policies. Likewise, policies preventing a user's ability to backup data to the cloud or to download to unprotected devices may be necessary.

If a mobile device retains data, alerts, login information, or other application data, policies and procedures should exist for decommissioning or reusing a device. These procedures should address device disposal at levels commensurate with the data and information on the device and in conjunction with other IACS asset policies.

- **Supply-Chain Components**

As is common in the development of technology solutions, third-party components are often included to facilitate development or provide additional features. With the use of web and application tools and components, new security risks can become inherent to the broader solution. The efficiency and flexibility that these tools can add to the development cycle are beneficial to the vendor and ultimately to the end user, however, neither the vendor nor the end user may have the ability to mitigate these vulnerabilities. Awareness of these components in the broader solution can help asset owners weigh the risks. A discussion with the vendor can provide the asset owner with a detailed understanding of the coding framework and backend.

- **Installation, Maintenance, and Management**

As with the implementation of any new technology in the IACS environment, the installation and ongoing maintenance of the solution should be considered. Initial installation and setup is often coordinated with the vendor. The installation and testing of typical configurations can range from one to multiple days. Planning considerations should include user permissions and access as defined by the asset owner. Once implemented, ongoing management and maintenance should be considered at several levels:

- **Server**

Data and application servers in the IACS environment must be kept current with operating system and application patches and updates.

- **Application updates**

Vendor application updates, hotfixes, and patches are necessary to maintain security.

- **Users**

Changes in user permissions, such as for staff who no longer need access, must be addressed in a timely manner that complies with the asset owner's security policies.

- **Devices**

In addition to security and version updates on devices, the overall lifespan of mobile devices must be managed including replacement and decommissioning schedules that take into account the mobile applications and data. Long-term support from the vendor that includes updates and alignment with the vendor's roadmap should also be considered. Mobility is a dynamic space with many expanding capabilities in IACS applications.

5 CONCLUSIONS

As part of the movement to provide real time data to decision makers outside the physical control center or site, mobility solutions are becoming more common and more capable in the IACS environment. Movement of the data to mobile applications or web access requires careful planning and risk analysis. Operational efficiencies, speed of decisions, and increased situational awareness are all benefits of accessing data, status, or alerts on a mobile platform. This project evaluated multiple mobile solutions, resulting in the identification of risks from diverse solutions.

Like all LOGIIC assessments of new technologies for IACS, this project identified both technical and operational findings. The nature of the mobile solution lends itself to the risks inherent in moving data outside the control center or site. Asset owners can work closely with vendors to ensure that technical risks are mitigated through the solution's design and life-cycle maintenance. Operational risks may be best handled through organizational security policies and procedures.

Asset owners should conduct a risk analysis of any potential mobile solution before selection and implementation. Solutions vary in design, connectivity options, levels of asset owner management, and other factors. The spectrum of possible implementation solutions requires the asset owner to make a selection based on risk, return on investment, resources available for management, among other considerations.

After reviewing the initial project questions, the project team drew the following brief conclusions:

What security controls are required on the end devices? Are some devices more secure than others?

Access control and security management are required on end devices and application and web browsers. Technical security controls are included in most vendor solutions. These must be configured and managed to maintain security. Device management may also be controlled through operational policies.

What is provided by the vendor? Can a third-party mobile device be used?

Most vendors provide software solutions that can be integrated on the asset owner's mobile devices. While vendors may provide native applications to run on Android or iOS, some offer web applications that can be accessed by most browsers, either on a mobile device or a remote system.

What security controls are required to secure the server or application?

Servers in the IACS environment must be maintained with good security practices including access control, lifecycle maintenance, and change management. Vendor applications, whether on the server or the devices, should be maintained with updates and patches as necessary. Supply chain management of risks must also be passed down from the vendor to the asset owner for mitigation. This includes maintaining security of third-party components and tools in the solution.

How do the mobile devices connect to the server?

Vendor solutions vary in their connectivity to the IACS environment. Most vendors offer two ways of connecting, from some level inside the network or from the Internet. Connectivity choices should be made by the asset owner based on operational need, value of data, and acceptable risk.

What functionality is provided within the application? Read-only data access or perform control?

The solutions tested in this project provided read-only access to data. Other available solutions advertise that control capability is provided from the mobile device. LOGIIC members did not identify these solutions as viable considerations for their operations; however, the capability to perform remote control may exist in the market.

What security controls are required to maintain the integrity of data in transit?

Data in transit requires the vendor to successfully implement encryption mechanisms in their solution. The asset owner should verify that these mechanisms are using the most current and secure methods and can be maintained throughout the life-cycle.

Is data stored on the device?

Data, alerts, and status messages can be stored on the mobile device in many of the vendor solutions. Data at rest on the device should be encrypted and use controls to prevent unauthorized access. Data residing on the device should also be considered if the device is shared among multiple users or when the device is decommissioned or repurposed.

What authentication mechanisms are in place?

Most vendor solutions require authentication if an application or web browser is used to access the data. Viewing application alerts and status messages that appear on the device may not require authentication.

Mobility solutions for IACS are evolving rapidly and eliminate the need for a decision maker to be onsite or communicate by voice or email to make operational decisions or respond to issues. Given the disparities in solution designs and connectivity options, no single model for securing mobile solutions in IACS exists.

Rather, an asset owner should work with the vendor to gain a full understanding of the attributes and technical details. This information can be used by the asset owner to ensure that a solution is selected and implemented to best match their risk portfolio and operational goals. Examples of this information include:

- Solution design
 - Native or web application design
 - Supply chain components
 - Encryption mechanisms
- Network configuration
 - Connectivity options
 - External and internal users
- Device options
 - Platform options
 - Control of displayed data
 - Device handling and user policies
- Security of data
 - Data in transit
 - Data in storage
- Management
 - Users, permissions
 - Server
 - Applications
 - Devices
 - Patches and updates

Given the nature of mobile devices, implementing them for use with IACS data or within the IACS environment requires consideration of the technical security measures and operational user policies. From the assessments, it can be concluded that these solutions can be used in the IACS environment securely if these measures are considered and carefully implemented.

Studies performed by LOGIIC as part of this project indicate asset owners' desire to increase the speed and efficiency of decisions by movement of IACS data to mobile devices to eliminate the need to physically access the control system to gain this information. Vendors are currently offering a spectrum of solutions for mobility in the IACS environment. This is a rapidly evolving market space with a variety of options for connectivity, data display, and user awareness. Given the variance in solutions offered today, asset owners should select a design that best meets their risk portfolio and operational needs, but also consider long-term

life-cycle management and growth. Increased real-time data availability, growth of DMZ structures, and expansion of situational awareness outside control center boundaries will contribute to the expanded role of mobility in IACS environments. This project concludes that implementing mobility in this environment can be done securely if technical and design aspects are managed with appropriate security controls. Likewise, life-cycle management is required to ensure that a level of security is maintained in the mobile architecture. Because moving data outside the physical protections of the IACS environment diverges from past standards and best practices, mitigating risks requires putting the right controls in place throughout selection, design, implementation, and ongoing maintenance processes.

APPENDIX

Acronyms

Term/Acronym	Definition
APK	Android Package Kit
ARC	Automatic Reference Counting
CSRDC	Cybersecurity Research and Development Center
DHS S&T	Department of Homeland Security, Science & Technology Directorate
DMZ	Demilitarized Zone
DoS	Denial of Service
HTTPS	HyperText Transport Protocol Secure
IACS	Industrial Automation and Control System
LOGIIC	Linking the Oil and Gas Industry to Improve Cybersecurity
REST	Representational State Transfer
SME	Subject Matter Expert
SQL	Structured Query Language
TLS	Transport Layer Security

Acknowledgements

The project to evaluate mobility technologies was developed and guided by the members of the international LOGIIC forum, who devote their time and expertise to conduct projects that will lead to improvements to cybersecurity in the oil and gas industry, and in the IACS community in general. The Automation Federation serves as the LOGIIC host organization and provides a necessary home and legal framework for our efforts.

LOGIIC would like to thank the DHS S&T Directorate for providing leadership, vision, and commitment to enhancing cybersecurity. We would also like to express our appreciation to the vendors who participated in the project and the work of our team of SMEs who refined the evaluation strategy, performed the system evaluations, and developed the project reports. Since the inception of LOGIIC, the scientific research organization SRI International has provided coordination, project management, and subject matter expertise.

The work performed on this project by SRI International and its subcontractors was funded under contract to the DHS S&T Directorate. The content is solely the product and responsibility of the LOGIIC program and does not necessarily represent the official views of DHS.

Distribution

This report is approved by U.S. Department of Homeland Security and the LOGIIC Executive Committee for unlimited public distribution.

© 2017. The Automation Federation. All rights reserved.