Project 10: Mobility

“Name of Presenter”
Presenter

Enter details about the presenter here.
More details about the presenter.
The LOGIIC Model of Government and Industry Partnership

Linking the Oil and Gas Industry to Improve Cyber Security
Project 10: Mobility

Background

Assessment Approach

Assessment Findings

Conclusion
Overview

• Focused on assessment and analysis
• Mobile devices to display IACS situational data
• Evaluated different mobility technologies
• Conducted assessments in an IACS laboratory
• Findings were published in a report
Objective

Evaluate currently available solutions that provide connectivity between the IACS environment and decision makers on the outside.
Surveys

• Surveyed Executive Committee members in December 2014 and November 2015

• Findings show mobility is significantly important to LOGIIC members

• Many plan to implement or expand mobility in their operations
Architectures

• Vendors offer different connectivity options
• Most mobile solutions are implemented at the asset owner site
• ‘Internal’ and ‘External’ connection options
Internal User Connects to DMZ

Level 4
Corporate Domain

Level 3.5
DeMilitarized Zone (DMZ)

Level 3
Industrial Automation and Control Systems (IACS)

Level 2
Control Systems

© 2017 LOGIC APPROVED FOR PUBLIC RELEASE — 10
External User Connects through Internet

- **Level 4**
  - Corporate Domain
  - MOBILITY SERVER

- **Level 3.5**
  - DeMilitarized Zone (DMZ)

- **Level 3**
  - Industrial Automation and Control Systems (IACS)

- **Level 2**
  - Control Systems

- **Level 1**
  - Web, iOS, Android

© 2017 LOGIIC APPROVED FOR PUBLIC RELEASE — 11
Mobility
Assessment Approach
Methodology

Risk = Threat x Vulnerability x Consequence
Onsite Assessment

• Reconnaissance
• Information capture and data retrieval attempts
• Targeted attacks
• Denial of service (DoS)
Vendor Approach

- Automation vendor & third-party solutions
- Each assessment conducted as an independent sub-project
Test Approach

Insider and outsider threat scenarios

SME attack methods

Public and customized exploits and payloads

Test equipment
Pre-work Phase

• Vendor Set-up
• Connection of test equipment
• Network validation
• Reconnaissance
• Traffic capture
Test Scenarios

01 Packet Captures
02 Data Storage and Leakage
03 Insecure Communication
04 App Authentication and Authorization
Crypto Algorithm and Key Management

Session Management

Client-side Injection

Server-side Controls
Reverse Engineering and Binary Protections

Code Analysis

Default App Configuration

Applicable Existing Exploits
Test Tools

Android and iOS

Kali Linux™
KingoRoot
Wireshark®
Burp Suite

ABD
Jadx
SSLstrip
Nessus®
Apktool

SQLiteSpy
drozer
Otool
ondevice console
Pangu

keychain dumper
Cycrypt
sqlmap
Big Boss Tools
## Analysis of Findings

<table>
<thead>
<tr>
<th>TECHNICAL</th>
<th>OPERATIONAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research</td>
<td>Usability</td>
</tr>
<tr>
<td>Documentation</td>
<td>Ease of Setup</td>
</tr>
<tr>
<td>Assessment Tests</td>
<td>Maintenance Requirements</td>
</tr>
<tr>
<td>Background Info</td>
<td>Skillsets to Maintain and Use System</td>
</tr>
<tr>
<td>Observations</td>
<td></td>
</tr>
<tr>
<td>Functional Tests</td>
<td></td>
</tr>
</tbody>
</table>
Mobility

Assessment Findings
Native Applications
Web Applications
Platform
Connectivity
Installation & Maintenance
Nature of Mobility
Device Handling
Components
Common Risks in Native Applications

• No certificate checking and pinning
• No jailbreak or debug detection
• No obfuscation
• No ARC memory management
Common Risks in Web Applications

• Cross site scripting vulnerabilities
• Session handling and termination risks
• Cookie management
Platform Risks

• Android vs iOS

• Key handling and platform requirements

• Signature verification

• Good coding practices, patches, and maintenance needed to mitigate any risks
Connectivity Risks

• “Internal User” vs “External User” connections
• Vendor management
• Asset Owner management
Nature of Mobility

• High-value data on a small, movable device
• User policies
• Management of accounts, permissions, devices
• Updates
Device Handling

• Unauthorized view
• Single-user devices
• Operational user policies
• Decommissioning
Supply-Chain Components

• Web and application tools and components can introduce new risks

• Ability of the vendor or asset owner to mitigate risks

• Important to understand coding framework
Installation, Maintenance & Management

Installation typically with vendor, followed by:

- Server maintenance
- Application updates
- User and device management
- Long-term support considerations
Mobility

Conclusion
Mobility Considerations

• Movement of data outside the IACS environment requires careful planning
• Many benefits exist to using mobility
• Close collaboration with vendor needed to mitigate technical risks

• Operational risks may best be handled through security policies and procedures
• A risk analysis should be conducted prior to selection and implementation of a solution

• Solutions vary in design, connectivity options, and management

• Selection may be based on risk, return on investment, resources available for management, etc
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

• Vendors may provide native applications to run on Android or iOS, or web app access
What security controls are required to secure the server or application?

- Server access control, lifecycle maintenance, and change management
- Vendor applications should be maintained and patched
- Mitigation of supply chain management of risks
How do the mobile devices connect to the server?

- Most vendors offer two ways of connecting:
  - From inside the network
  - From the Internet

- Connectivity choices should be based on operational need, value of data, and acceptable risk
Within the application, what functionality is provided – read data only, or perform control?

- Solutions tested provided read-only access to data
- Other solutions advertise control capability is may be possible
What security controls are required to maintain the integrity of data in transit?

- Data in transit requires implementation of encryption
- Asset owners should verify the most current and secure methods are in place and can be maintained
Is data stored on the device?

- Data, alerts, and status messages can be stored on the mobile device.
- Data at rest on the device should be encrypted and controlled.
What authentication mechanisms are in place?

- Authentication if an application or web browser is used to access the data
- Alerts and status messages that appear on the device may not require authentication to view
Approach to Mobility

• Solution designs vary

• No single model for securing mobile solutions in IACS

• Asset owners should work with the vendor to understand all technical details

• Select a solution that best matches a risk portfolio and operational goals
Important Technical Details

An asset owner should be aware of:

• Solution design
• Network configuration
• Device options
• Security of data
• Management
Conclusions

Implementing mobility for IACS data, while maintaining a secure environment, requires carefully implemented:

• Technical security measures
• Operational user policies
Additional Considerations

Spectrum of available mobile solutions

Rapidly evolving market space

Selecting a solution based on risk portfolio, operational needs, and life-cycle

Variety of options for connectivity, data display, user awareness
Implementing mobility in IACS can be done securely if technical and design aspects are managed with security controls and security is managed throughout the life-cycle.