Mobile Security and Deployment: Secure your apps using out-of-the-box capabilities and EMM

Charlie Temkin
Senior Associate, Product Management
Copyright and Safe Harbor Notice

This presentation may include statements that constitute “forward-looking statements” for purposes of the safe harbor provisions under the Private Securities Litigation Reform Act of 1995, including descriptions of technology and product features that are under development and estimates of future business prospects. Forward-looking statements inherently involve risks and uncertainties that could cause actual results of MicroStrategy Incorporated and its subsidiaries (collectively, the “Company”) to differ materially from the forward-looking statements.

Factors that could contribute to such differences include: the Company’s ability to meet product development goals while aligning costs with anticipated revenues; the Company’s ability to develop, market and deliver on a timely and cost-effective basis new or enhanced offerings that respond to technological change or new customer requirements; the extent and timing of market acceptance of the Company’s new offerings; continued acceptance of the Company’s other products in the marketplace; the timing of significant orders; competitive factors; general economic conditions; and other risks detailed in the Company’s Form 10-K for the year ended December 31, 2016 and other periodic reports filed with the Securities and Exchange Commission. By making these forward-looking statements, the Company undertakes no obligation to update these statements for revisions or changes after the date of this presentation.
Agenda

• Security Concerns
  • Mobile Security Threats

• Build Up Mobile Security
  • Operational Security
  • Device Security
  • Application Security

• MicroStrategy’s Mobile Security Architecture
  • EMM
  • Out-of-the-Box

• Summary
What are the Main Mobile Security Threats?
Mobile Security Risks and Threats

- **Lost or stolen devices**
  - BYOD policy risks
  - Data theft

- **Jailbreak/rooting easy to achieve**

- **Malware threat is growing**
  - Social engineering attacks

- **Data integrity threats**
  - Modify or corrupt data without permission; motivations may include disrupting enterprise operations and financial gain.

- **Resource abuse attacks**
  - Misuse network, computing or identity resources of a device; sending spam and launching DoS attacks.
Mobile Security Threats

- Data Loss
- Device Tampering
- Always-on Connectivity
- Form Factor
- Malicious or Risky apps
Mobile Security Threats

Public Wi-Fi

Hackers can use fake Wi-Fi hotspots to steal information. “Safe” Public Wi-Fi is actually non-existent.

Pay special attention to Wi-Fi connections in:

- Coffee shops and restaurants
- Hotels
- Train and bus stations
Build Up Mobile Security
How can Mobile Security Risks be Mitigated?

1. Operational Security

2. Device Security

3. Application Security
   - Communications
   - Access
   - Data
What is Operational Security?
Operational Security

Establish security policy
• Passcode required
• Passcode complexity

Procedures for reporting lost/stolen device

Device management
• Proactive monitoring
• Response to lost/stolen device report

Information management
• Policies for handling of sensitive data
• Sensitivity reduction
• Information deception

Ensure proper operation of WiFi equipment
What is Device Security?
Mobile Device Security
Passcode protection

• Require alpha character
• Minimum length
• Minimum number of complex characters
• Expiration (1-730 days)
• Auto-Lock (1-5 minutes, or none)
• Grace period for device lock
• Passcode history
• Maximum number of Failed Attempts
• Touch/Face ID
iOS Security Features and Model

System Security
- Secure Boot Chain
- System Software Authorization
- Secure Enclave
- Touch/Face ID

Encryption and Data Protection
- Crypto Engine
- File Data Protection
- KeyChain

App Security
- App code signing
- Runtime process security
- App Transport Security
iOS Security Features and Model

52% of devices are using iOS 11.

As measured by the App Store on November 6, 2017.
iOS and Android

- Strict controls on device and store
- Well designed and thus far, resistant to attack
- Rigorous certification model which vets the identity of software authors and weeds out attackers

- Major improvement over traditional computing programs
- Less rigorous certification model which allows a more open development environment
- Relies on users to make important security decisions
What is the Application’s responsibility to make itself secure?
Application Security

Corresponds to measures that an application should support to protect its data, enterprise access and communication.

There are several strategies to enhance mobile application security including:

• Using the right methods to ensuring transport layer security (https and certificate management, certificate server)

• Proper session handling (session expired, clear footprints)

• Strong authentication and authorization

• Device data encryption

• Access control and user privileges
EMM - Enterprise Mobility Management
Enterprise Mobility Management (EMM)

THE CHALLENGE

THE SOLUTION

Copyright © 2017 MicroStrategy Incorporated. All Rights Reserved.
Solutions of EMM Technologies: MDM
Mobile Device Management (MDM)

**What is it?**

- Controlling the device to manage, secure and control the devices
- Security management
- Device configuration management
- Policy management
- Enterprise network integration
- Remote data wipe
- Blacklisting/whitelisting of apps/devices

**Limitations**

- Employees carry two devices
- BYOD
- B2C
- Application specific
- Data specific
Solutions of EMM Technologies: MAM
Mobile Application Management (MAM)

What is it?

• Manage the lifecycle of a mobile application
• Solution to enterprise MAC (manage, analyze & control) needs in B2C, B2B or B2E scenarios.
• Offers more integrity with application specific data and its security

Limitations

• Device level policy only applicable if containerization approach is leveraged.
• Upgrading agent or SDK is difficult as it is bundled with the application if containerizations approach is leveraged.
• Must validate and certify private applications for malicious code.
Solutions of EMM Technologies: MCM/MIM
Mobile Content Management (MCM) and Mobile Information Management (MIM)

What is it?

- Securing sensitive data
- User authentication
- Policy configuration (data access/wipe)
- Data security over the air
- Data security at rest
- Data sharing protection
- Data version update
- Data modification detection
- Sync content between device-server

Limitations

- Persistent memory of device only accessible through native APIs
- Limited platform support
- Focus is around corporate data only
- Few vendor support
Solutions of EMM Technologies
MicroStrategy EMM Solutions
EMM Using SDK Integration
Integration through SDK

<table>
<thead>
<tr>
<th></th>
<th>iOS</th>
<th>ANDROID</th>
</tr>
</thead>
<tbody>
<tr>
<td>airwatch® by VMWare</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>✔️</td>
<td>❌</td>
</tr>
<tr>
<td>MobileIron</td>
<td>✔️</td>
<td>❌</td>
</tr>
</tbody>
</table>
AirWatch
Complexity of Mobile Environments
BlackBerry Dynamics

Basic Distributed Servers

Diagram shows the flow of communication between BES12, internal firewall, routing components, Internet, external firewall, BlackBerry infrastructure, wireless network, and various devices (BlackBerry 10, iOS, OS X, Android, and Windows). The diagram includes optional components and notification services (APNs, GCM, or WNS).
MobileIron
Security Platform for Modern Enterprises
The AppConfig Community
Need for The AppConfig Community

THE CHALLENGE

THE SOLUTION
The AppConfig Community Members
AppConfig and MicroStrategy

App Configuration

App Tunnel

Security Policies and Access Control

Single Sign On
App Configuration

Process Flow:
1. App developer makes the app available to the organization. The application can be a public app in the iTunes or Google Play store, or may be an internally developed app signed for enterprise distribution

2. Configurations are specified in the EMM admin console

3. App is distributed to devices, along with the configurations specified, via the EMM
App Tunnel

Process Flow:
1. Organization deploys any needed VPN infrastructure
   (contact your VPN provider for details)

2. EMM vendor distributes the VPN app along with the Per-App
   VPN configuration profile

3. The end user opens an app that requires a backend connection,
   and the VPN will automatically turn on
Security Policies and Access Control

MicroStrategy Capabilities:

1. Encryption

2. Managed Open-In

3. Custom security settings:
   EnableDataLossPrevention, DisableEmail, DisableOpenIn,
   DisablePrint, DisableCopyPaste, DisableCameraAccess,
   DisableLocationServices, DisableSaveToPhotos
Single Sign On (SSO)

**Process Flow:**

1. Organization deploys any needed identity provider (IDP) infrastructure

2. App developers build in support for SAML (or equivalent) standard for identity federation into the mobile app and its backend service

3. The app is distributed to the device via the EMM

4. When the app is launched, the user will see the identity provider’s login screen in a web view window

5. The user may optionally have to authenticate to this page

6. Once the user is authenticated, any future apps that leverage the same IDP will be able to detect the existing authenticated session and will not need to prompt the user to login again.
Secure Communication
MicroStrategy
Out-Of-The-Box Security
MicroStrategy Mobile Security Solution

A complete, flexible, and customizable security model

Communication

• HTTPS
• Certificate pinning (validate server)
• Client certificate management (validate device)

Access

• SSO support.
• LDAP, Kerberos, NT Integration.
• Password required after timeout or suspended state
• Session handling
• User credentials are stored encrypted on device.
• Credentials can optionally be cleared when operating with single sign-on solutions.

Data

• Application data is encrypted on device.
• Caches can be cleared when exiting the application.
• Independent Third Party Security Testing.
## Communications Security

- **HTTPS**
- **Certificate pinning**
- **Client certificate**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Usage</th>
<th>Example(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric Encryption</td>
<td>Protect data at rest or in transit</td>
<td>AES</td>
</tr>
<tr>
<td>Asymmetric Encryption</td>
<td>Exchange Symm. Keys Digital Signature Authentication (x509 certificates)</td>
<td>RSA Algorithm, Elliptic Curve Cryptography (ECC)</td>
</tr>
<tr>
<td>Secure Hash Function</td>
<td>Validate Passwords for user authorization</td>
<td>SHA-2</td>
</tr>
</tbody>
</table>
Communications Security

HTTPS

HTTPS creates a secure channel over an insecure network

• Protects contents of the communication

• Composed of a set of algorithm
  - Key Exchange (DHE-RSA, ECDHE-RSA)
  - Cipher (AES CBC, AES GCM)
  - Data Integrity (HMAC-SHA256)
Communications Security

Certificate Pinning

Ensures that the client is communicating with the right Mobile Server

• Extra step beyond the normal X.509 certificate validation
• The client checks the public keys in the server's certificate chain against a set of public keys for the server name.
• Prevents man-in-the-middle attacks
Asymmetric Encryption

X.509 Certificates

- Identity
- Issues digital certificate
- Issues Private Key

- Version
- Unique serial number
- Certificate signature
- Algorithm
- CA Name

- Validity period
- Subject name
- Public key algorithm used by subject public key
- CA Signature
Communications Security

Client certificate management

- Identifies a particular client with an authentication server.
- Used as an enhanced security measure beyond simple user validation.
Secure Application and Data Access
Mobile Server Settings

• Cache for real-time data
• Cache for folders
• Clear caches when the application closes
• Clear caches on logout
• Allow users to modify settings
Application Login

Require passcode to access application when:

• application launch
• application back to foreground
• device unlocked
MicroStrategy Application Passcode

Double-encryption feature

```
App Passcode

Password-based Key Definition

AES
```

```
Red Processing

Username

Password

Key Generation

Concatenate

SHA256 Hash

AES Encryption

Secure Storage (Keychain)

Black Processing

Preferences.xml

Caches
```
Access Control to Individual Document

Secure your entire organization’s mobile analytics at the app and document level
Different Authentication Modes to Access Data

**Intelligence Server Authentication**

- Standard
- Windows
- LDAP
- Database
- Usher
- Trusted

**Mobile Server Authentication**

- Basic
- NTLM
- Kerberos
- Usher
- SSO (Basic, HTML Form, SAML)
Kerberos Authentication

Client

Auth Request

A,B

Authentication Server (AS)

C,D

Client/TGS,TGT

E,F

Client_to_server ticket

Client/server

E,G

Client_to_server ticket

Authenticator

Service Server (SS)

Authenticator

H

Time auth
Kerberos Authentication

Advantages

• High Performance
• Mutual Authentication
• Protected against eavesdropping and replay attacks

Limitations

• Single point of failure
• Strict time requirements
• symmetric cryptography adoption
• trusted relationship to the Kerberos token server
SSO Authentication

MicroStrategy Mobile Server

MicroStrategy Intelligence Server

SSO Server:
Siteminder
Tivoli
SAML
Security Assertion Markup Language
SAML
Security Assertion Markup Language
Device Data is Protected

• OS “sandbox” protects app data from other apps
• OS Hardware/Device Encryption of app data
• MicroStrategy’s Software Encryption
• Cache purged upon close
• Cache expiration
• Credentials Expiration
• Never Persistent Credentials
Platform Security

**Users**
- Are identified by a Unique Login and User Name
- Users are Defined in the Metadata Repository
- User Exist Across Multiple Projects

**User Groups**
- Are a Set of Users
- Privileges and ACLs can be Assigned to User Groups
- User Group Privileges Apply to All Projects

**Security Roles**
- Are a Set of Privileges
- Security Roles can be assigned to Users and/or Specific Groups
- Security Roles Apply to Specified Individual Projects and ACLs can be Assigned to User Groups
Summary


Operational Security

Device Security

Application Security
  • Communications
  • Access
  • Data
Thank You