



Securing your Zebra device

DevTalk – 20th June 2018

Darryn Campbell
Senior Software Architect

Agenda:

- Securing your Zebra device with MX
 - Threat Manager
 - Encrypt Manager
 - Access Manager
 - Other techniques
- Summary & Resources

Profile Manager

Profile Manager is an exclusive EMDK technology offered within your IDE, providing a GUI based development tool. This allows you to write fewer lines of code resulting in reduced development time, effort and errors.

Getting Started

- [Using Profile Manager](#)
- [MX Overview](#)
- [Choosing a Version](#)
- [Feature Compatibility](#)
- [Getting Device MX Version](#)

Core Framework

- [Persistence Manager](#)
- [XML Manager](#)

UI Settings

- [KeyMap Manager](#)
- [PowerKey Manager](#)
- [Settings Manager](#)
- [UI Manager](#)

Network

- [Bluetooth Manager](#)
- [Cellular Manager](#)
- [DHCP Options Manager](#)
- [GPRS Manager](#)
- [Hosts Manager](#)
- [WiFi Manager](#)
- [Wireless Manager](#)

Application Management

- [App Manager](#)
- [App Gallery Manager](#)
- [Browser Manager](#)
- [Enterprise Keyboard Manager](#)

Device Configuration

- [Analytics Manager](#)
- [Audio Manager](#)
- [Batch Manager](#)
- [Battery Manager](#)
- [Bug Report Manager](#)
- [Clock](#)
- [Component Manager](#)
- [Condition Manager](#)
- [Display Manager](#)
- [Ethernet Manager](#)
- [Personal Dictionary Manager](#)
- [Power Manager](#)
- [Touch Manager](#)
- [Remote Scanner Manager](#)

Data Capture

- [Activity Selection](#)
- [Barcode Input](#)
- [Data Capture Plus](#)
- [Int Output](#)
- [IP Output](#)
- [Keystroke Output](#)
- [MCP Input](#)

Security

- [Access Manager](#)
- [Camera Manager](#)
- [Cert Manager](#)
- [DevAdmin](#)
- [Encrypt Manager](#)
- [SD Card Manager](#)
- [Threat Manager](#)
- [USB Manager](#)

Securing your Zebra device with MX

Manager	Function
Threat Manager	Detect a potentially compromised device and enact countermeasures such as wiping or locking the device
Encrypt Manager	Encrypt internal storage or attached SD card. Supports full encryption or filesystem encryption
Access Manager	Prevent user applications from running or installing. Lock down what the user can do on the device
Camera Manager	Control access to the camera and imager for applications on the device
Cert Manager	Manage certificates in the Android KeyStore, e.g. install a trusted server certificate authority
DevAdmin	Controls which application acts as Device <u>Administrator</u> and has access to the Device Policy Manager APIs.
SD Card Manager	Block / unblock use of the SD card
USB Manager	Control adb and the USB storage mode

Threat Manager

Detect Threat:

- EMM client (or any app) has been removed
- Device is being managed by Microsoft Exchange ActiveSync
- “External Threat” detected (e.g. triggered by EMM)
- Device has been rooted (check on boot)
- Device has been rooted (periodic scan)



Perform Countermeasure:

- Lock the device
- Factory reset
- Format SD card
- Wipe the secure storage keys
- Send custom message to application
- Uninstall an application

Threat Manager

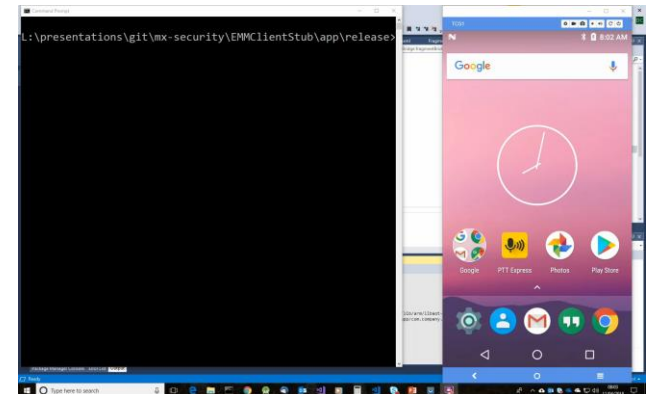
DEMO 1

Threat:

Detect removal of EMM client application
(substituted here by a test application)

Countermeasure:

Lock the device



Threat Manager

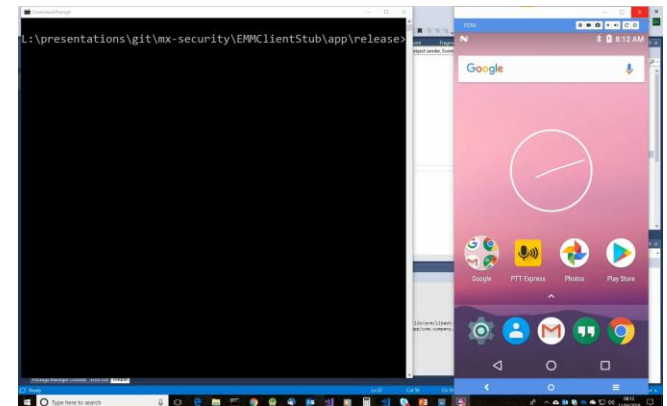
DEMO 2

Threat:

Detect removal of EMM client application
(substituted here by a test application)

Countermeasure:

Send a custom threat message

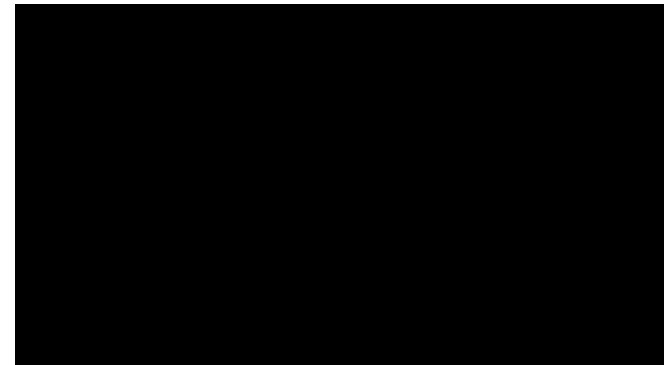


Encrypt Manager

- Supports full encryption for SD cards
- Supports folder-based encryption for **non-encrypted** internal or external storage.
- Manage the key storage database for that encryption
- **Wait a minute...**
 - Isn't full disk encryption (FDE) enabled by default on M+ devices?
 - Yes, you could **not** use folder-based encryption on M+ internal storage.
 - The Encrypt Manager has been around since MX4.3 (JB). Could offer a consistent approach in mixed deployments.
 - FDE only applies to internal storage and SD cards still remain unencrypted

Encrypt Manager

- Isn't full disk encryption (FDE) enabled by default on M+ devices?
- Don't we have adoptable storage on M+ devices for external SD cards?
 - Yes, but right now adoptable storage is a manual process
 - The Encrypt Manager has been around since MX4.3
 - Video shows adopting an SD card

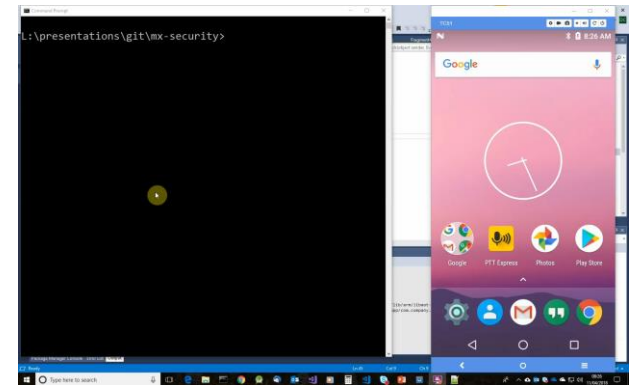


Encrypt Manager

DEMO 1

Encrypt Manager:

- Install encryption key
 - Generate key using `openssl enc -aes-256-cbc -k secret -P -md sha1`
- Encrypt external storage card
 - Card is wiped and can be subsequently read on device
 - Card is not readable off device

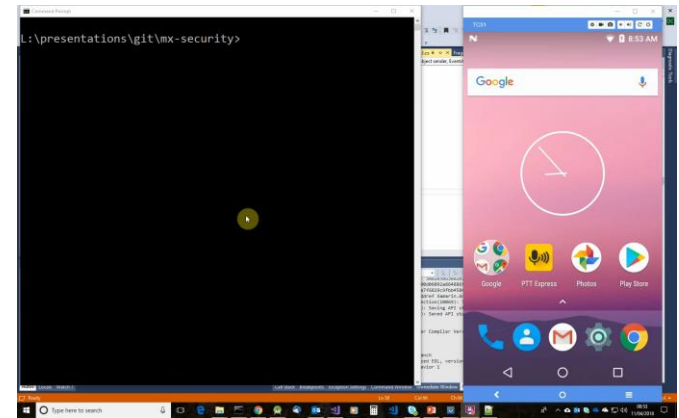


Encrypt Manager

DEMO 2

Encrypt Manager:

- Revoking & reinstalling keys
 - Install key
 - Encrypt SD card
 - Files can be written and read
 - Revoke encryption key & reboot device
 - Contents of card can no longer be read
 - Reinstall key & reboot device
 - Contents of card CAN now be read

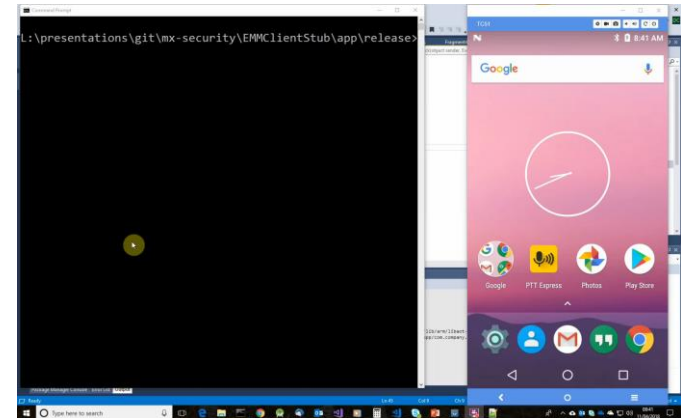


Encrypt Manager

DEMO 3

Combine Encrypt Manager with Threat manager:

- Threat is detected (emm client uninstalled)
- Encryption key is revoked
 - Reboot the device to see the effect.
- SD card can no longer be read



Access Manager

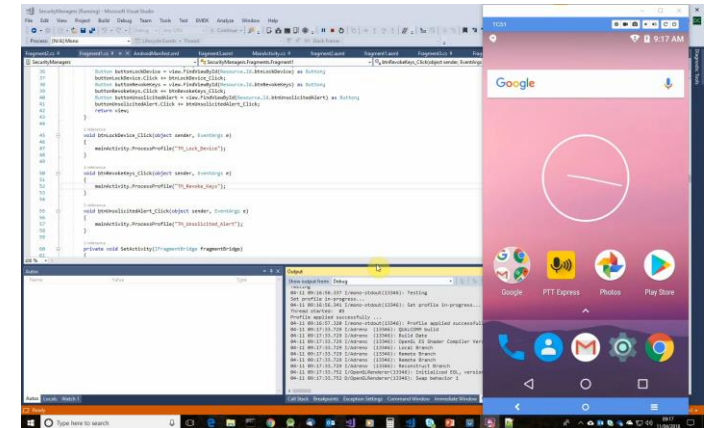
- Whitelist user applications (not system applications)
- Control whether whitelisted apps can utilize MX
- Packages can be removed from or added to the whitelist (so effectively it is a blacklist also)
- Lock down whitelist with application signatures
- Control whether the user has access to full or reduced settings

Access Manager

DEMO 1

A Simple Whitelist:

- Two test applications are whitelisted and allowed to use MX
 - all others not visible
- User access to settings is 'reduced'

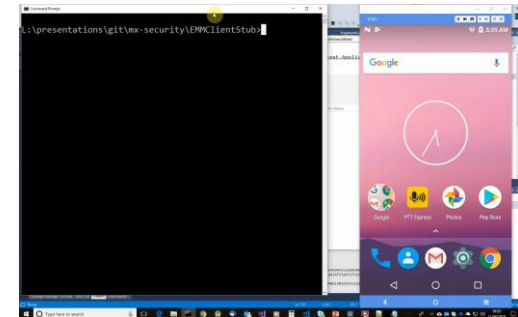


Access Manager

DEMO 2

A Signed Whitelist:

- Two test applications are whitelisted and allowed to use MX, all others not visible
- Whitelisted applications have their signatures verified
 - Signature:
<https://developer.android.com/reference/android/content/pm/Signature.html>
 - “Opaque, immutable representation of a signing certificate associated with an application package”
 - Not an md5 hash or application signing key(!)
- User access to settings is ‘reduced’
- Demo note: If I install the debug variant of emmclientstub it is whitelisted but the release variant is NOT



Access Manager

Obtaining the signature for an application

Xamarin:

```
System.Collections.Generic.IList<Signature> sigs =  
Application.Context.ApplicationContext.PackageManager  
.GetPackageInfo(Application.Context.ApplicationContext  
.PackageName,  
PackageInfoFlags.Signatures).Signatures;  
foreach (Signature sig in sigs)  
{  
    Console.WriteLine("MyApp: " + sig.ToCharsString());  
    String signatureString = sig.ToCharsString();  
    Signature s = sig;  
}
```


Access Manager

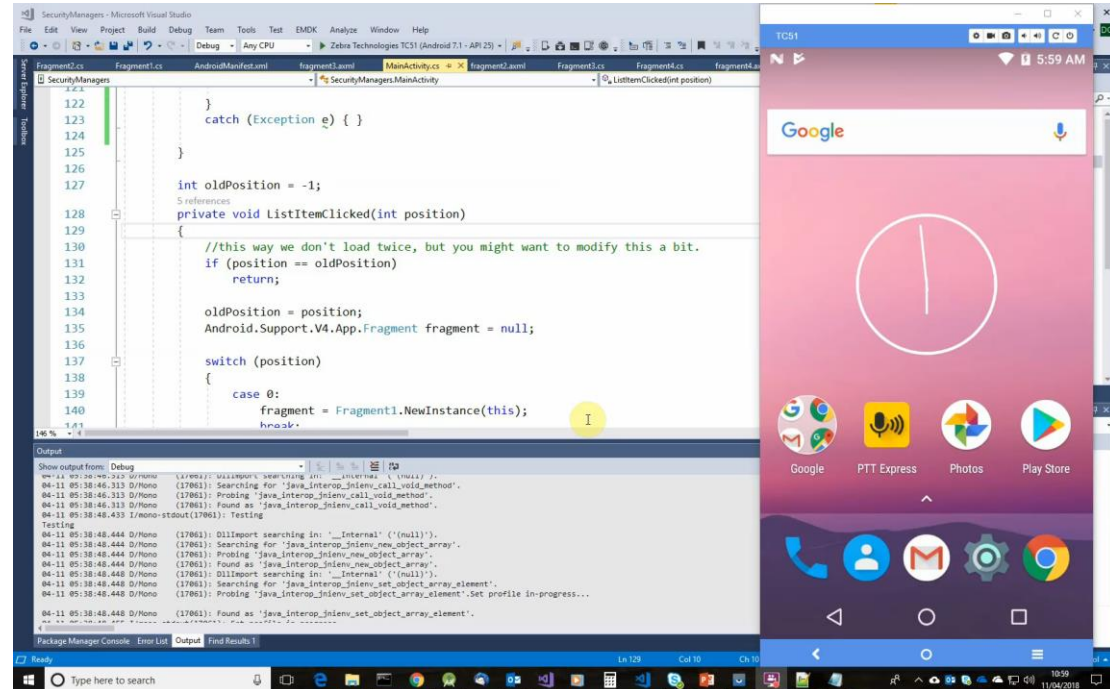
Obtaining the signature for an application

Java:

```
Signature[] sigs =  
context.getPackageManager().getPackageInfo(context.getPackage  
getName(), PackageManager.GET_SIGNATURES).signatures;  
for (Signature sig : sigs)  
{  
    Trace.i("MyApp", "Signature hashCode : " +  
sig.toCharsString());  
}
```

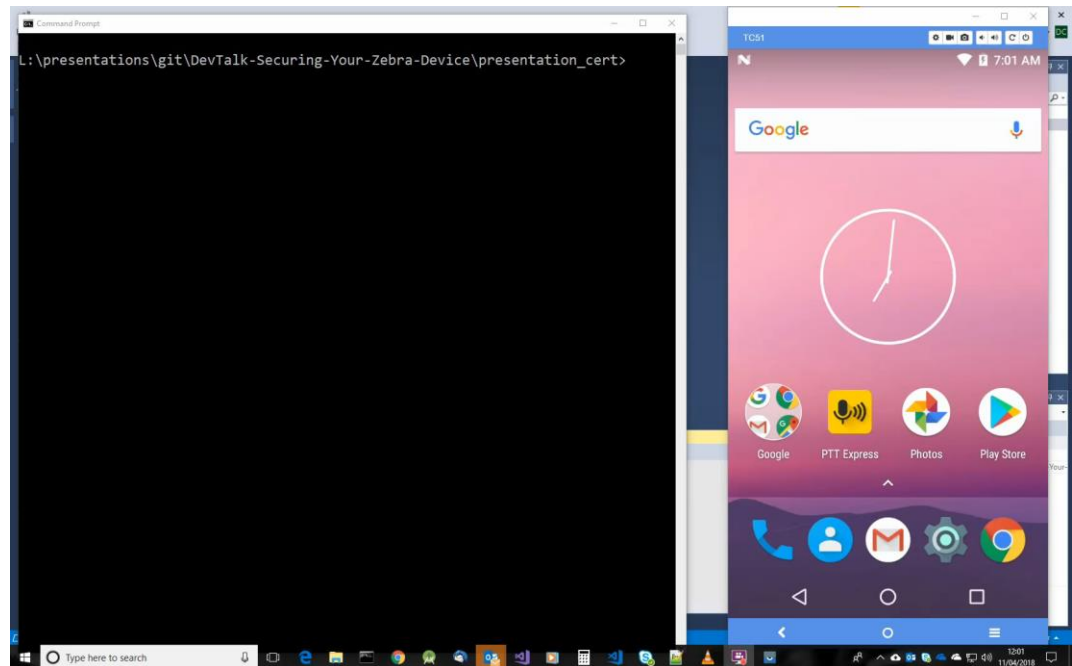
Other Security Managers

- Camera Manager



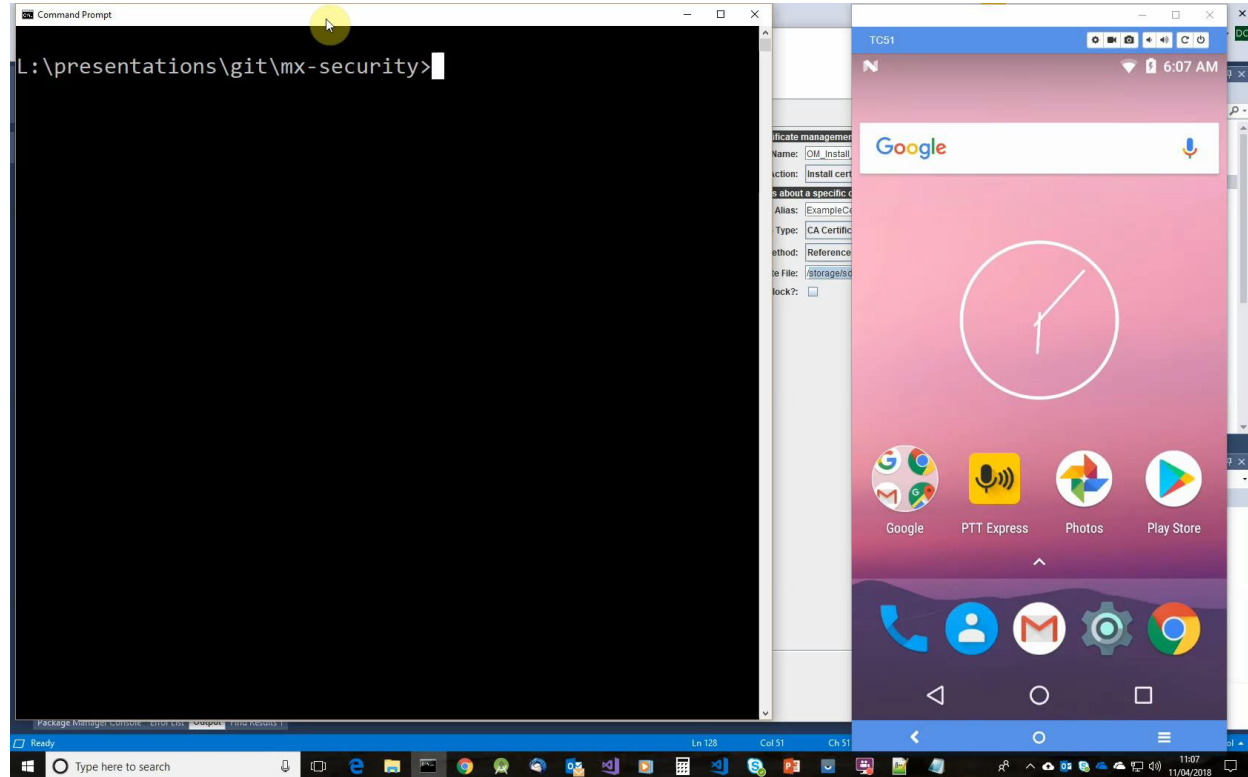
Other Security Managers

- Certificate Manager
 - Adb push ca.crt /storage/sdcard0/ca.crt
 - Settings → Security → Trusted Credentials → User (you also get a notification)



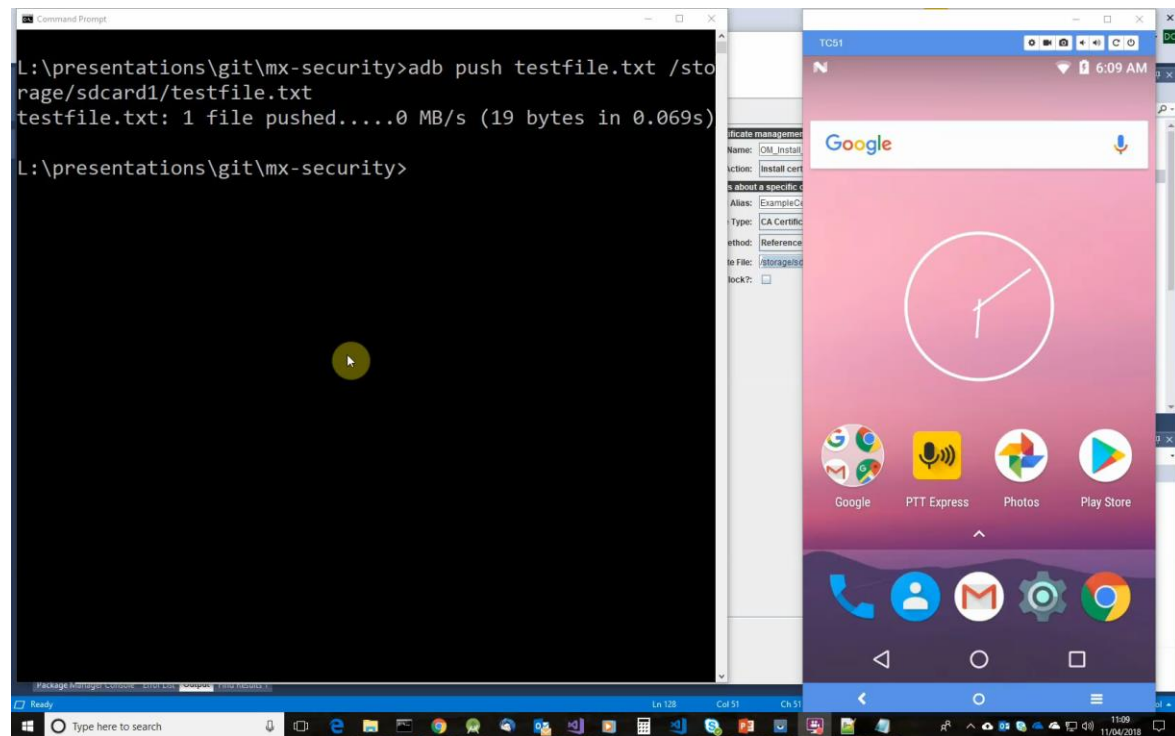
Other Security Managers

- SD Card Manager



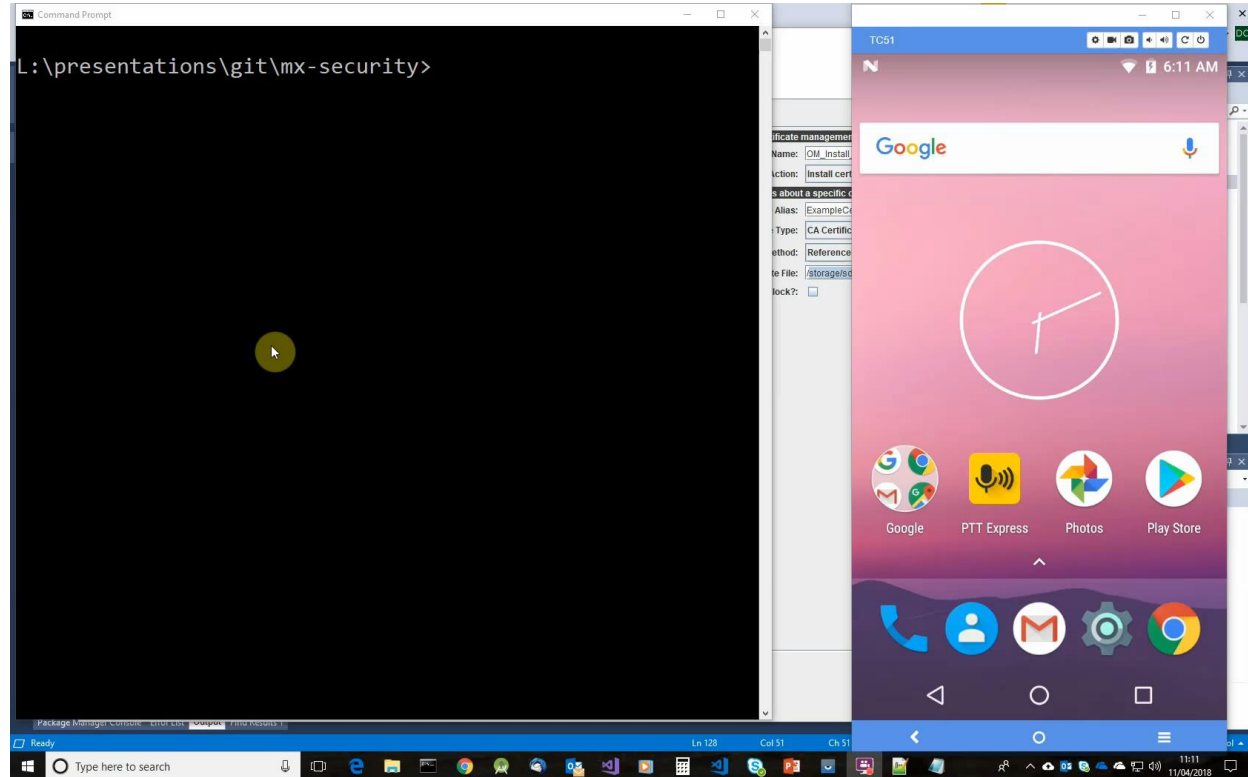
Other Security Managers

- DevAdmin
- Security → Unknown Sources



Other Security Managers

- USB Manager



Resources

- Sample Apps shown in this presentation:
 - All under the github repository: <https://github.com/darryncampbell/DevTalk-Securing-Your-Zebra-Device>
- Videos shown during this presentation:
 - Youtube playlist: <https://www.youtube.com/playlist?list=PLj8D9Diz5FBpAuyqjvT19he3BnjFkLr-l>

Questions?