Windows Phone 8 Security

Corsin Camichel

November 12th, 2012

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Security Features

System Integrity

- Secure Boot
- Extended Secure Boot

App Platform Security

- Chambers and Capabilities
- The Browser
- Windows Phone Store
- Enterprise Line-of-Business (LOB) Apps
- Windows Phone Updates

Data Protection

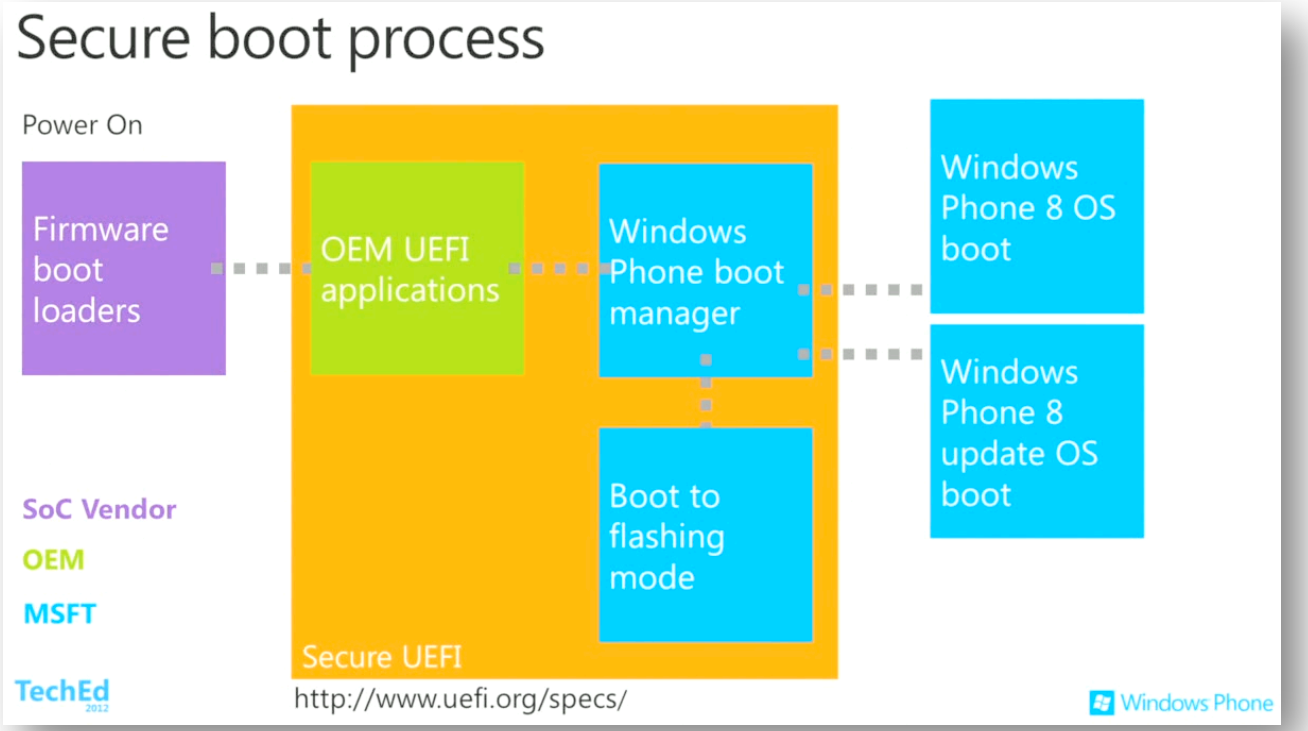
- Device Access and Security Policies
- Device Encryption
- Removable Storage
- Data Leak Prevention

Secure Access

System Integrity

Secure Boot

- Validates Firmware images on the device
- All boot components are digitally signed
- UEFI based



System Integrity (2)

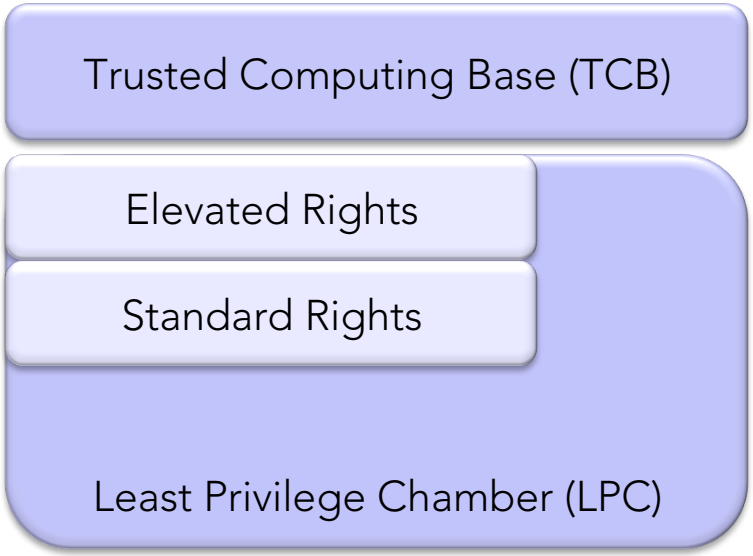
Extended Secure Boot

- Windows Phone Boot Manager (Microsoft Supplied)
  - Expects that everything went fine ahead of its launch
- All code in Windows Phone 8 is signed by Microsoft, including OEM apps & drivers! (different than Windows Phone 7.x)
- Apps from the store are also signed by Microsoft

App Platform Security

Chambers and Capabilities

- Same concept & terminology as Windows Phone 7.x
- Several chambers with different permissions on the system and its features
- Radically minimized attack surface compared to WP7 (only TCB & LPC)
- User consent and control (similar to Android's permission model)
- Isolation, no communication between apps other than via the Internet



Kernel, Drivers etc.

Services (media services, data shared among other apps

Microsoft Apps (Outlook etc.), OEM apps

Apps from Store/Marketplace

App Platform Security (2)

The Browser

- Internet Explorer 10
- Runs in a isolated chamber (see previous slide)
- No support for Plug-ins
- SmartScreen technology allows detection of malicious websites/content and blocks execution of it

Windows Phone Store

- Submitted apps analyzed and verified before made available to users
- Apps are signed by Microsoft ones they are approved

App Platform Security (3)

Enterprise Line-of-Business (LOB) Apps

- Sideloading of business apps
- Organization registers with Microsoft to obtain rights to privately sign applications and distribute them

Windows Phone Updates

- All updates come from Microsoft (OS, firmware etc.)
- Windows Phone was designed with the Microsoft Security Development Lifecycle (SDL)

Data Protection

Device Access and Security Policies

- Access to device is protected by password or PIN
- Enforcement of security settings Exchange ActiveSync and MDM solutions
- Windows Phone 8 is compatible with version 14.1 of EAS protocol
- Supports Exchange 2003 SP2 (and higher) and Microsoft Office 365
- Default features such as remote wipe, locking, locating etc.

Device Encryption

- Encrypts internal memory only (SD cards stay unencrypted)
- Can be controlled by EAS and MDM
- Uses BitLocker technology to encrypt storage
- Lock screen PIN not used for encryption$
- Not supported in countries like Russia and China (legal restrictions)
- Some BitLocker known from desktops not supported:
  - The key is not escrowed (no possibility to restore)
  - No PIN for boot process

Data Protection (2)

Removable Storage

- Only media data (photos, music, videos etc.) stored on SD card
- Will not be encrypted (trade-off, used so that data can be added from a computer)
- MDM can be used to forbid usage of removable storage
- Apps can be installed from a removable storage (some rules apply)

Data Leakage Prevention

- Support for Information Rights Management (IRM)
- Allows content creators to assign rights to shared documents
- Requires Windows Rights Management Service (RMS), a Microsoft solution
- Can also be applied to emails

Secured Access

- Built to take advantage of cloud-based services
- Encryption with AES-128 and/or AES-256
- No support for S/MIME
- No support for Smart Cards

MDM - Enterprise Reporting

Enterprise reporting

- Server configured policy values
- Query installed enterprise app Device name
- Device ID
- OS platform type
- Firmware version
- OS version
- Device local time
- Processor type
- Device model
- Device manufacturer
- Device processor architecture
- Device language

TechEd 2012

Windows Phone

MDM Support

MDM Support built-in for Windows Phone 8 (resides next to Exchange ActiveSync policies)

- Windows Phone 7.8 (upgrade for 7.5 with some features of WP8) does NOT support MDM

Mobile device management policy

Mobile Manager Policies	MDM	EAS
Simple password	✓	✓
Alphanumeric password	✓	✓
Minimum password length	✓	✓
Minimum password complex characters	✓	✓
Password expiration	✓	✓
Password history	✓	✓
Device wipe threshold	✓	✓
Inactivity timeout	✓	✓
IRM enabled	(NA)	✓
Remote device wipe	✓	✓
Device encryption (new)	✓	✓
Disable removable storage card (new)	✓	
Remote update of business apps (new)	✓	
Remote or local un-enroll (new)	✓	

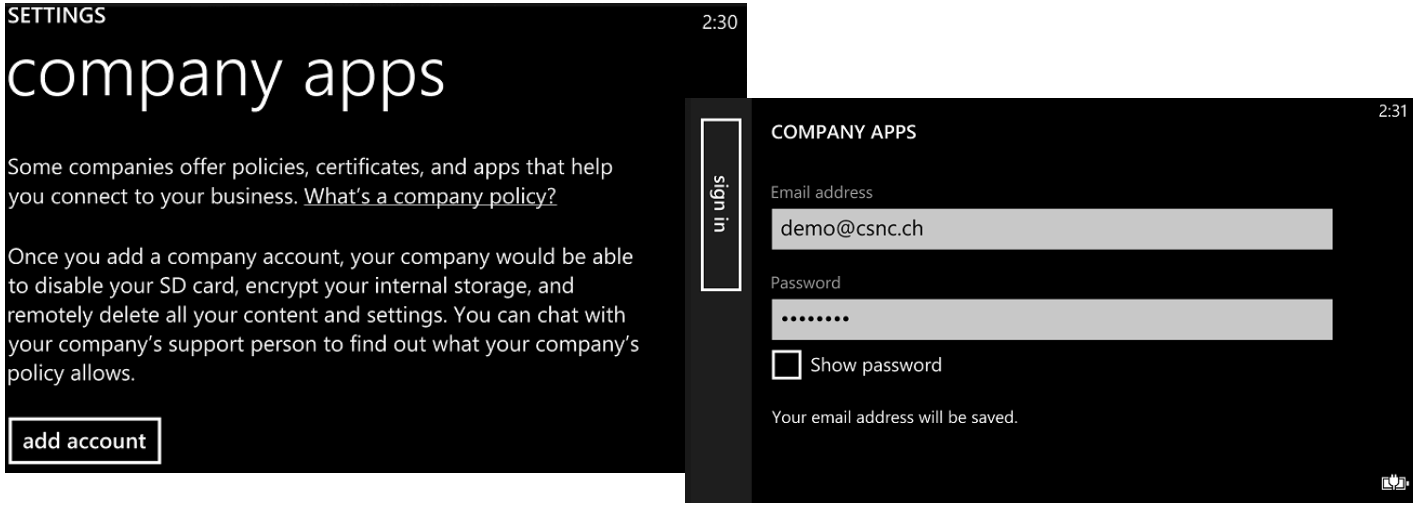
TechEd 2012

Windows Phone

MDM Support

Enrollment

- MDM provisions certificates to the phone
  - MDM sends the app enrollment token to the phone
- Allowed to install one application at enrollment
  - Microsoft recommends installing a custom hub application / app discovery
  - No other apps can be pushed to the device
- Enrollment is based on native functionality. No third party application is required



MDM Support

App Deployment

- Enterprise IT develops and signs XAP
- Signed XAP is published to the company App Catalog (Sharepoint, Website, database etc.)
- User opens the company's app discovery app/hub or receives link to application by mail etc.
- Installs application, as long as the token for installation is available on device (need to be pushed at enrollment)
- No market place volume license option

Policies

- Always the strongest policy is enforced
- White-/Blacklisting is not possible
  - No policy to block consumer-functionality
    - Consumers can use own Microsoft Accounts (you have to forbid it by written policies)

Exchange Active Sync Support

	Windows Phone 8	iOS 6	Android 4.x
Allow device encryption	Yes	Yes	Yes
Require Device Encryption	Yes	Yes	No
Encrypt storage card	Yes	N/A	Yes
Minimum password length	Yes	Yes	Yes
Minimum number of complex characters	Yes	Yes	Yes
Password History	Yes	Yes	Yes
Device Wipe Threshold	Yes	Yes	Yes
Disable removable storage	No	No	No
Disable Camera	No	Yes	Yes
Disable SMS text messaging	No	No	No

Exchange Active Sync Support (2)

	Windows Phone 8	iOS 6	Android 4.x
Disable Wi-Fi	No	No	No
Disable Bluetooth	No	No	No
Disable IrDA	No	No	No
Require manual sync while roaming	No	Yes	Yes
Allow Internet sharing from device	No	No	No
Allow desktop sharing from device	No	No	No
Disable email attachment access	Yes	Yes	Yes
Disable POP3/IMAP4 email	No	No	No
Allow consumer email	No	No	No
Allow browser	Yes	No	No

Exchange Active Sync Support (3)

	Windows Phone 8	iOS 6	Android 4.x
Configure message formats	No	No	No
Include past email items (days)	Yes	Yes	No
HTML email body truncation size (kb)	No	No	No
Include past calendar items (days)	No	No	No
Require signed S/MIME messages	No	No	No
Require encrypted S/MIME messages	No	No	No
Require signed S/MIME algorithm	No	No	No
Require encrypted S/MIM algorithm	No	No	No

Native Management Capabilities

	Windows Phone 8	iOS 6	Android 4.x
S/MIME	Yes	Yes	No
Over-the-air-data encryption	Yes	Yes	Yes
VPN	Yes	Yes	Yes
Configure VPN	No	Yes	Yes
Restrict/block app stores	Yes	Yes	No
Restrict/block wireless LANs	No	Yes	No
Configure allowable access points	No	Yes	Yes
Signed apps required	Yes	Yes	No
Selective wipe of business apps and data only	Yes	Yes	No

Native Management Capabilities (2)

	Windows Phone 8	iOS 6	Android 4.x
Secure Boot	Yes	Yes	No (some devices Yes)
Apps sandboxing	Yes	Yes	Yes
Disable cloud services and storage	No	Yes	No
Remotely update business app	Yes	Yes	No

Resources

Videos

- http://channel9.msdn.com/Events/TechEd/Europe/2012/WPH304
- http://channel9.msdn.com/Events/TechEd/Europe/2012/WPH205

Documentation

- http://blogs.msdn.com/b/sdl/
- http://msdn.microsoft.com/en-US/library/windowsphone/develop/jj206943(v=vs.105).aspx
- http://technet.microsoft.com/en-us/library/ff657743.aspx (IRM)