ACN elaboration

Lukas Prokop

24th of Sept 2014

Contents

1 At which frequency does WiFi operate on? 2

2 What does MDM and MAM stand for? 2

3 What does the current mobile Windows OS project branch look like? 2

4 Name smartphone applications / usecases 2

5 What are security threats specific for smartphones? 2

6 Define the structure of a risk analysis 3

7 What is the historical background of TLS? What are properties of TLS? 3

8 What is forward secrecy? 3

9 How are TLS connections established? 3

10 Which ciphersuites exist (for example)? 4

11 What is Certificate Pinning? 4

12 How does the renegotiation attack work? 4

13 How does the BEAST attack work? 4

14 How does the Padding Oracle attack work? 4

15 How does the Lucky Thirteen attack work? 4

16 How does the CRIME attack work? 4

17 How does the BREACH attack work? 4

18 What is the Heartbleed bug? 4

19 Where could passwords possibly come from? 5

20 Give statistics about Android malware 5

21 How does the Eurograbber trojan work? 5

22 Which circumstances support phishing attacks on mobile devices? 5

23 Which problems do user passwords on mobile devices have? 5

24 What are mobile Botnets? 5

25 Name applications for electronic signatures? 5

26 What is two-factor authentication? 6

27 Was ist eine qualifizierte Signature (Austrian national signature law)? 6

28 How does the Austrian Mobile Phone Signature work? 6

29 Why is encryption of the file system necessary for Remote Wiping? 6

30 What is crypto-shredding? 6

31 In what regards do encryption systems differ? 6

32 What does Mobile Device Management mean? 6

33 When were the two encryption systems introduced in iOS? 6

34 Where are data protection class keys derived from? 7

35 Where are filesystem keys derived from? 7

36 How does data protection in iOS work? 7

37 How does key derivation happen on iOS? 7

38 What is the iOS keychain? 7

39 Are iOS backups encrypted? 7

40 Which two keys are secured within chips of iOS devices? 7

41 How does the iOS Secure Boot Chain look like? 7

42 What are tethered jailbreaks? 7

43 Name a few iOS jailbreaks 8

44 How can we mitigate buffer overflows attacks? 8

45 What are characteristics of the Apple App Store? 8

46 How does the Apple app publishing process look like? 8

47 What are properties of the Android OS? 8

48 How does filesystem encryption on Android work? 8

49 What is the Android KeyChain? 8

50 How does Sandboxing on Android work? 8

51 Which feature of Android can be used to mitigate buffer overflow attacks? 8

52 How does Secure Boot take place on Android? 8

53 How does the Android permission system work? 9

54 Which application sources exist for Android? 9

55 What changed in regards of SMS handling with Android 4.4? 9

56 Which IPC mechanisms does Android offer? 9

57 Which backup system are available on Android? 9

58 How do Windows Phone backups work? 9

59 What is Blackberry? 9

60 Which operating system is used by BlackBerry devices? 9

61 What is BlackBerry Protect? 9

62 Which development platforms exist for BlackBerry? 10

63 Which security features does BlackBerry offer? 10

64 Which mobile operating systems support certificate revocation? 10

65 How do cold boot attacks work? 10

66 Describe how data-flow analysis can take place. 10

67 What does MDM and MAM stand for? 10

68 What are possible deployment scenarios? 10

69 How do key derivation functions work? 10

70 How does PBKDF2 work? 10

71 Which implementations use PBKDF2? 11

72 What is bcrypt? 11

73 What is scrypt? 11

74 Which side-channels of mobile devices do you know? 11

1 At which frequency does WiFi operate on?

The established protocols 802.11b and 802.11g use a frequency of 2.4 GHz. They use a bandwidth of 22 and 20 MHz respectively.

2 What does the current mobile Windows OS project branch look like?

- *Windows CE* (deprecated)
- succeeded by *Windows Mobile* (deprecated)
- succeeded by *Windows Phone*
  - Windows Phone 7
  - Windows Phone 8
  - Windows Phone 8.1[1] (upcoming)

3 Name smartphone applications / usecases

- Social networking, browsing
- Gaming
- Navigation, maps
- Business
- Augmented Reality
- Banking
- Security
- Spyware

4 What are security threats specific for smartphones?

- Mobility (sensors with more data available, easy theft)
- Mixed private/business usecases
- Limited security capabilities (short passwords / PINs)

5 Define the structure of a risk analysis

1. Define assets
2. Define threats
3. Prioritize threats
4. Identify security functions relevant for given threats

[1] Windows 8.1 is nicknamed “Windows Blue”.

6 What is the historical background of TLS? What are properties of TLS?

History:

- Initially developed by Netscape (starting with 1994)
- IETF standard (1999–2008)
- "Secure Sockets Layer" and "Transport Layer Security"
- SSL 2.0 (RFC 6176, 1994), SSL 3.0 (RFC 6101, 1996)
- TLS 1.0 (RFC 2246, 1999): No major differences to SSL 3.0, downgrade option to SSL 3.0
- TLS 1.1 (RFC 4346, 2006): Countermeasures to CBC attacks
- TLS 1.2 (RFC 5246, 2008): old ciphersuites removed, algorithm improvements

Properties:

- X.509 certificates (symmetric and asymmetric cryptography)
- Confidentiality, data and (partially) origin integrity, authentication
- Provides forward secrecy
- Only one communication partner is authenticated
-

7 What is forward secrecy?

Short-term session keys cannot be derived from long-term session keys. Hence assuming an attacker breaks long-term keys (server's private keys), the session keys cannot be derived and therefore past communications stay still confidential.

8 How are TLS connections established?

client to server packet:

- Client Hello
  - client TLS version
  - random number
  - session ID
  - ciper suites
  - compression methods
  - extensions

server to client packet:

- Server Hello
  1. server TLS version
  2. random number
  3. selected cipher suite
  4. selected compression method
- Certificate
  1. trust chain of server
     - first certificate is server's certificate
     - last certificate is certificate issued by root certificate
     - because root certificate can be omitted (browser must have it)
- Server Key Exchange
  - Only if key exchange protocol requires data exchange (eg. ECDH)
  - Mostly data is already in certificate
- Certificate Request (skipped in most cases)
- Server Hello Done

client to server packet:

- Certificate (if requested, return certificate)
- ClientKeyExchange
  - Client generates 48 random bytes (premaster secret)
  - PreMasterSecret encrypted with public key of server certificate
  - Server decrypts PreMasterSecret with private RSA key
  - Master secret = PRF(PreMasterSecret, "master secret", ClientHello.random + ServerHello.random)[0..47]
- CertificateVerify (verify server's certificate)
- ChangeCipherSpec ("everything is encrypted now")
- Finished (sending MAC of previous handshake messages)

server to client packet:

- ChangeCipherSpec ("everything is encrypted now")
- Finished

9 Which ciphersuites exist (for example)?

Structure: `[SSL | TLS]_[key exchange]_[authentication]_[bulk cipher]_[message auth]`

Key exchange / agreement
RSA, DH, DHE, ECDH, ECDHE (confidentiality, integrity)

Authentication
RSA, DSS, ECDSA (authenticity)

Bulk ciphers
AES, 3DES, RC4 (confidentiality)

Message authentication
SHA256, SHA384, MD5 (integrity)

Examples:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA

10 What is Certificate Pinning?

The certificate trust chain is ignored and a specific set of certificates is whitelisted.

11 How does the renegotiation attack work?

1. Attacker establishes a TLS connection to the server
2. Attacker and server communicate privately
3. Attacker renegotiates a new connection meaning that a new handshake is done via the existing encrypted channel
4. Attacker tricks server
5. Server has built up a secret connection to a different client than the attacker

The attacker cannot read from the new secret connection[2] but can inject data which will be read and processed at the client.

12 How does the BEAST attack work?

BEAST (Browser Exploit Against SSL/TLS) injects javascript in the same-origin using a broken Java Same Origin Policy implementation. Then the attacker sniffs the traffic between the victim and the server. He injects updated crafted data and can eventually cookies (even with httpOnly flags).

13 How does the Padding Oracle attack work?

During decryption of symmetric ciphers in CBC mode data is leaked about whether the padding of an encrypted message is correct or not. This can allow attackers to decrypt (possibly also encrypt) messages through the server ("oracle") using server's key, without knowing the encryption key.

This attack is a predecessor of Lucky Thirteen.

14 How does the Lucky Thirteen attack work?

The lucky thirteen attack uses a timing attack against the MAC check stage in the TLS algorithm. The attacker uses the input ciphertext and forms a message of 20 AES blocks. He copies a block (which content he wants to extract) and its predecessor as the last two encrypted blocks (which contain the MAC and padding).

Then on every different user connection it XORs the last byte of the penultimate block with a byte named Delta of his choice. He tries various Delta values and awaits the server response (a TLS server notifies the client of decryption failure).

Plotting the response time we observe that different Delta require different time to receive a reply.

15 How does the CRIME attack work?

CRIME (Compression Ratio Info-leak Made Easy) has been demonstrated with the HTTPS and SPDY protocols and attacks data compression. The attacker observes the size of compressed, encrypted data sent from the browser to the server. The attacker also makes the user to send multiple carefully crafted web connections to some attack sites, which contain various strings. If the data size becomes smaller, we can assume that the website contains a string which is also part of the cookie. Apply divide and conquer to retrieve the whole content of a cookie.

16 How does the BREACH attack work?

BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext) is an instance of the CRIME attack specifically for HTTP compression. Many browser and servers use gzip or DEFLATE data compression algorithms via the content-encoding option within HTTP, which is exploited by this attack.

There are no mitigations implemented against this attack.

17 What is the Heartbleed bug?

Heartbleed is an severe implementation in OpenSSL. The TLS heartbeat extension lacks proper input validation and returns as much main memory content as requested.

18 Where could passwords possibly come from?

- User password → Key Derivation Function
- Device-integrated chip
  - Secure Element
  - Trust Zone
  - Hardened CPU

[2] Hence, it's not a Man-In-The-Middle attack.

- Chip on external token via NFC, cable, etc
    - SIM card
    - Secure SD card
    - Smartcard
- Operating System Store
    - Software
    - Hardware
- Cloud Computing
    - Hardware Security Module
    - Mobile Phone Signature

19 Give statistics about Android malware

- Market shares: Android 84.7%, iOS 11.7%, Windows Phone 2.5% (as of 2014 Q2)
- 92% of all known mobile malware is written for Android.
- ∼70% of all smartphones in 2012 were Android devices.
- 77% of all Android threats can be mitigated with a migration to the lastest OS.

Reasons to attack Android:

- Market dominance
- Open platform
- Existence of many third-party app stores
- Anonymity of developers

Kinds of malware:

- Rootkits
- Worms
- Crimeware
- Trojans
- Viruses
- Spyware
- Adware

20 How does the Eurograbber trojan work?

1. Infect user's computer.
2. Intercept web communication between user and bank (offer "new banking software").
3. Attacker retrieves user's mobile number and infects the mobile device.
4. Next time user logs into bank, a transfer to a "mule" account is initiated.
5. A TAN is sent to the user's mobile. Attacker intercepts it and completes illicit transaction.

21 Which circumstances support phishing attacks on mobile devices?

- User cannot hover over link to see true URL
- Users expect mobile websites to look different than desktop versions

22 Which problems do user passwords on mobile devices have?

- User passwords have very low entropy [key derivation required]
- Passwords stored in plaintext [hashing required]
- Low-power mobile devices with little performance [little power requirements needed]
- Hashes tuned for performance [security problems]
- Attacker with high performance device(s) [HSM required]

23 What are mobile Botnets?

- Network of smartphones controlled by a botmaster
- Used for spam delivery, DDos attacks, theft of personal data
- Examples: Geinimi, Pjapps, DroidDream, DroidKungFu, Nickispy, SMSspacem

24 Name applications for electronic signatures?

E-Banking
User authentication, transaction authorization

E-Government
User authentication, Sign request data, Sign official notifications

Private affairs
Sign contracts

25 What is two-factor authentication?

An authentication requiring presence of two independent authentication factors such as

knowledge something only the user *knows*

possession something only the user *has*

inherence something only the user *is*

26 Was ist eine qualifizierte Signature (Austrian national signature law)?

Eine qualifizierte elektronische Signatur ist eine fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt wird. Eine fortgeschrittene Signatur ist eine elektronische Signatur, die

- ausschließlich dem Signator zugeordnet ist,
- die Identifizierung des Signators ermöglicht,
- mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann, sowie
- mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Veränderung der Daten festgestellt werden kann

Eine sichere Signaturerstellungseinheit (Secure Signature Creation Devices, SSCD) ist eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturerstellungsdaten verwendet wird und die den Sicherheitsanforderungen dieses Bundesgesetzes sowie der auf seiner Grundlage erlassenen Verordnungen entspricht (Signaturgesetz § 2).

27 How does the Austrian Mobile Phone Signature work?

For Mobile Phone Signatures a central HSM is assumed as SSCD. The Estonian signature system (in contrast) uses the SIM card as SSCD. It stores user's personal signature keys and creates signatures. Access to personal signature keys are protected by a two-factor authentication. A password is required for the signature process (authentication factor "knowledge") and a TAN is sent to the mobile phone (factor "possession").

1. User initiates signature creation in some application.
2. Application sends signature request to A-Trust.
3. User enters telephone number and password in web form and sends it to A-Trust.
4. A-Trust sends TAN and hash to mobile communication provider.
5. Mobile communication provider sends SMS to user.
6. User enters TAN into web form and sends it to A-Trust.
7. A-Trust signs document using HSM and sends signature response to application.
8. Application offers user signed document.

It is crucial that signed data (SD) is kept confidential and unmodified. Credentials (CRE) must only be kept confidential.

28 Why is encryption of the file system necessary for Remote Wiping?

Remote Wiping deleting all files on the filesystem is not an option, because it takes too much times. Hence it is convenient to encrypt all files and delete the key if remote wipe is desired.

29 What is crypto-shredding?

Crypto-shredding is the deliberate destruction of all encryption keys for the data; effectively destroying the data (unless the crypto scheme is broken some day).

30 In what regards do encryption systems differ?

- Purpose (remote wipe, encryption of data)
- Encryption scope (application data, system data, user data, how many keys are used)
- Key properties (length, storage, derivation)
- Locking (Encrypted when phone only locked?)
- Implementation (hardware / software support)
- Weaknesses (various attacks possible)

31 What does Mobile Device Management mean?

Mobile Device Management refers to rules established in a company to keep business data secure.

32 When were the two encryption systems introduced in iOS?

Device encryption (whole file system)
Introduced with iOS 3 and iPhone 3GS, based on a chip

Data protection (individual files and credentials)
Introduced with iOS 4, improved with iOS 5 (new classes, better keychain protection)

33 Where are data protection class keys derived from?

The PIN / passcode is entered by the user. Data protection class keys use derived keys from the key derivation algorithm which in turn uses the PIN.

34 Where are filesystem keys derived from?

The filesystem key originates from the Secure Element AES Key and is therefore independent from the PIN. If PIN would be used, a jailbreak can be used to circumvent PIN protection and the system decrypts the data for you. Hence filesystem encryption enables remote wiping, but data is accessible unless the device is shut off.

35 How does data protection in iOS work?

Protects specific application files (emails, PDF files, ...). The developer defines the protection class and unique file keys are generated and stored encrypted in extended file attributes. Protection classes (key derived from device's UID key and PIN/passcode):

NSProtectionNone
by device key, storage in EffaceableArea (small blobs of data with secure erasure)

NSProtectionComplete
by device key and passcode/PIN, decryption key is only available when device is unlocked

NSFileProtectionCompleteUnlessOpen
by device key and passcode/PIN, uses ECDH over D. J. Bernstein's Curve25519, file readable only if device unlocked or file still in memory

NSFileProtectionCompleteUntilFirstUserAuthentication
by device key and passcode/PIN, encrypted until first user auth (reboot loses key)

It's the developer's responsibility to select the correct protection class. The user relies on appropriate security decisions.

36 How does key derivation happen on iOS?

Screen lock passcode and hardware element are used for key derivation. Derivation takes 80 ms per derivation. The derived key finally results in the Data encryption key. Because the hardware element is involved, only on-device brute-force attacks are possible.

37 What is the iOS keychain?

The *keychain* is used to store passwords, credentials and keys (SQLite database). iOS has only one keychain. Database is stored in NSProtectionNone environment on device. `securityd` daemon handles access to database. Only apps from the same developer may access some keychain item.

38 Are iOS backups encrypted?

There are three types of backups:

Plain iTunes Backups
Credentials are stored encrypted with key stored on the iOS device. Hence credentials cannot be restored on other device.

Encrypted iTunes Backups
Files and credentials are protected via the derived key. Credentials can be restored on other iOS devices. But off-device brute-force attacks are possible for weak passwords when backup is stolen. Protection for keys is weaker than in plain iTunes Backups

iCloud Backups
somehow encrypted, protection via user passcode

The software developer has to choose whether files are in backup. For keychain entries he needs to chose the right protection class.

39 Which two keys are secured within chips of iOS devices?

- the *GDI key* is a globally shared key for decrypting Apple's firmware images
- the *UID key* works on a per-device basis. It is used to derive AES keys which are used to encrypt data (keychain, files, filesystem metadata)

The UID key is used to derive further keys (filesystem encryption key, keychain, etc)

40 How does the iOS Secure Boot Chain look like?

1. ROM is signed by *Apple Root CA Public Key* (verification needed)
2. LLB (Low Level Bootloader) is started (verification needed)
3. iBoot (Bootloader) is started (verification needed)
4. iOS kernel is running

41 What are tethered jailbreaks?

Tethered jailbreaks (unlike untethered jailbreaks) need to patch the system every time it boots (using a desktop computer).

42 Name a few iOS jailbreaks

- 0x24000 Segment Overflow
- Corona (limera1n)
- Pwnage

43 How can we mitigate buffer overflows attacks?

- Address space layout randomization
- Data Execution Prevention
- Compiler-based mitigation

44 What are characteristics of the Apple App Store?

- the *only* source for apps
- preinstalled on all iOS devices, not removable
- only reviewed apps offered

45 How does the Apple app publishing process look like?

- User uploads app
- Enter review queue
- App gets reviewed: Reject with reason or user is allowed to release

In 2009 40 reviewers were reported to be working on app reviews. At least 2 reviewers confirm one app. 8500 iPhone apps per week released. Reasons for rejection include bugs, instabilities, privacy violations, porn, ...

46 What are properties of the Android OS?

- Patched Linux kernel
- `libc` replaced with custom `Bionic` implementation
- `X11` replaced with `SurfaceFlinger`
- Until Android 4.3 single-user
- Managed code for user apps, well-defined execution environment
- Android Runtime (ART, Dalvik VM is deprecated since Android 4.4) to run Java software

47 How does filesystem encryption on Android work?

- `dm-crypt` is used as disk encryption system (since Android 3.0, Linux kernel feature)
- No hardware module (not entirely true any more) used unlike iOS. Hence off-device brute force attack is possible.
- After entering PIN, device is decrypted for 128 bit AES with CBC
- Android shares complexity of PIN to everyone (DevicePolicyManager property)
- PBKDF2 is used to derive master key from PIN. Device admin can set password complexity
- Master key is encrypted with 128 bit AES using OpenSSL

48 What is the Android KeyChain?

- public API since Android 4.0
- is a storage for credentials
- backed by secure element hardware, TPM or ARM TrustZone
- keys are not extractable

49 How does Sandboxing on Android work?

- individual user runs an app (like Linux kernel)
- apps are separated (process with its own address space, user permissions)
- applies to native code as well as java code on Dalvik
- SELinux is used to manage permissions for individual apps (invisible to app devs)

50 Which feature of Android can be used to mitigate buffer overflow attacks?

- `FORTIFY_SOURCE` is a compiler flag (can be used since Android 4.2)
- compiler adds checks for buffer size (if known at compile-time)

51 How does Secure Boot take place on Android?

- Kernel verification (key is in hardware of manufacturer)
- Used to verify first boot loader
- `dm-verity` kernel module creates and signs hash tree
- No protection classes - once phone is booted, everything is unencrypted

52 How does the Android permission system work?

- Android app requires a set of permissions to run
- User has to accept before installation
  - Cannot deselect individual permissions
  - Can turn off some functionality globally (GPS, WiFi, network, . . .)

53 Which application sources exist for Android?

- Google Play Store
  - Official store with free & commercial apps, ¿1 mio. apps
  - performs “application security scanning”
- Third Party Store (eg. Amazon Appstore)
- File System
  - Put `.apk` file on file system. Run it to install application.
  - `.apk` files can be downloaded from the web
  - “Untrusted Sources” must be allowed

Applications are signed with developer’s key. Two apps of same dev may share resources. Application encryption is possible with a device-specific key. Some information keeps world-readable (permissions, etc) but the code is encrypted (since Android 4.1). Since Android 4.2 / 2.3 apps are verified before installation (data is sent to google server).

54 What changed in regards of SMS handling with Android 4.4?

- User has to choose a “default app” for SMS
- Only this app can receive `SMS_DELIVER_ACTION` broadcast
- Other apps are still able to send simple SMS

55 Which IPC mechanisms does Android offer?

IPC mechanisms give Android applications the ability to

- run processes in background
- offer services consumed by other applications
- safely share relational data
- start other programs
- reuse components from other applications safely

56 Which backup system are available on Android?

Android Backup Service
since Android 2.2, enabled per default, access only via Google account, unknown encryption, Backup Service Key for each app, includes SMS, MMS, apps, wifi pwds, bookmarks, . . .

Dropbox, Carbon, SkyDrive
synchronization with cloud

Titanium Backup, NANdroid, App Backup & Restore

root permissions required

57 How do Windows Phone backups work?

- Builtin
- List of apps installed, setting, call history, sms, photos, etc

58 What is Blackberry?

- BlackBerry Limited (formerly Research In Motion) is a telecom and wireless equiment company
- BlackBerry Limited develops wireless handheld devices and smartphones as “BlackBerry deivces”
- Since 1999 (email pager), 40% smartphone market share in 2010
- Today below 10%, mostly known for still using physical keyboards on most products

59 Which operating system is used by BlackBerry devices?

- QNX, minimal unix-like microkernel
- designed for embedded systems
- kernel runs many small tasks (called “servers”) which can simply turned off (to turn off functionality)
- for mobile BlackBerry devices: strong separation between “work” and “personal” area
- focus on business usecases

60 What is BlackBerry Protect?

- Is integrated in OS
- Offers management services
  - Lock your device (if lost)
  - Delete data in it (if stolen)
  - Find it (if misplaced)
  - Wireless backup
  - Restore settings (if switched)

61 Which development platforms exist for BlackBerry?

- Native (Cascade / Core / Gaming)
- HTML 5
- Adobe Air
- Runtime for Android

62 Which security features does BlackBerry offer?

- Position Independent Code/Executable (PIC/PIE, equivalent to ASLR, compiler flag)
- Password Keeper
  - Previous versions: native app, now installation via BlackBerry World (app store)
  - stores all passwords
  - records encryption with AES 256
  - single password
  - generates very strong random passwords
- Memory cleaning (clear temporary data in memory)
- Content protection (app data protection with smartphone password, decrypted when unlocked)
- RIM cryptographic API (Java) (encrypt/decrypt/sign/verify, establish secure connections, key management)

63 Which mobile operating systems support certificate revocation?

Android
OCSP and CRL supported, must be explicitly enabled by developer

iOS
OCSP support, only enabled for Extended Validation certificates, certificate check passes if server unreachable

64 How do cold boot attacks work?

- Freeze (well, at least −15° C) mobile device when its running
- Charged memory cells in RAM do not drain immediately
- Recover data from frozen chip using a minimal OS

65 Describe how data-flow analysis can take place.

- Per function / method apply forward & backward slicing
- Define taints for data to analyze (taints are transitive)
  - sources are parameters, globals, instance members
  - sinks are return values, by-ref arguments, globals, instance members
- Possibly state explosion (everything is tainted)

66 What does MDM and MAM stand for?

Mobile Device Management and Mobile Application Management

67 What are possible deployment scenarios?

Managed devices
handing out dedicated devices to employees, company has control over hard-/software, enforce password rules / remote wiping / forbid installation sources / tracking

COPE Corporately-Owned, Personally-Enabled, unlike managed devices allows private usecases

BYOD Bring your own device, various approaches (MDM and MAM applied to whole smartphone, Container App Management, Application Wrapper Management, MDM and MAM only applied to “business area” as in BlackBerry Balance)

Consumer Little security-critical consumer application usecases (eg. banking)

68 How do key derivation functions work?

1. Use salt and shared secret as input for key establishment scheme (like HMAC, AES-CMAC). Use output as key derivation key
2. Use key derivation key as input to derive actual key. Derivation happens by applying cryptographic primitive multiple times in some mode of operation (like PBKDF2, scrypt, mcrypt).

69 How does PBKDF2 work?

Input parameters:

- iteration count
- salt
- required output length

- underlying PRF

Output:

- derived key

70 Which implementations use PBKDF2?

- WPA2
- TrueCrypt
- Mac OS X Mountain Lion

71 What is bcrypt?

- key derivation function
- iteration count is a power of two (hence less configurable than PBKDF2)

72 What is scrypt?

- key derivation function like PBKDF2
- strength is the usage of RAM (uses a lot of RAM, mathematically proven); hence difficulty to parallelize attack

73 Which side-channels of mobile devices do you know?

- Power consumption
- Sound
- Heat
- Execution time
- EM emission