ANDROID SECURITY CONSIDERATIONS

Reading Material:

Android Forensics Andrew Hoog

- Android as an attack vector
- Security strategies
- EDRM & BYOD

DATA THEFT TARGETS & ATTACK VECTORS

- easy to lose, easy to steal, short life usage span
- lots available second hand online
- increase in malware to target mobile devices
- information leakage
- data at rest
- data in transit

DATA AT REST

- non volatile data not stored in RAM or on a network
- SMS/MMS
- Call logs
- Voice Mail
- Financial apps

- Personal mail
- Web history
- Google search history
- YouTube
- pictures & videos
- Geo location
- Game history & interactions

DATA AT REST

- corporate email & attachments
- voice mails and faxes sent via mail
- user names, passwords, domain info

- wifi access points, information and passwords
- calendar items
- |M
- Corporate files
- Corporate cloud access

DATA AT REST EXAMPLE

 Android built in email app stores credentials for MS EAS in plaintext!!!!!!

located in EmailProvider.db

```
ahoog@ubuntu:~$ sqlite3 com.android.email/databases/EmailProvider.db
SQLite version 3.6.22
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .mode line
sqlite> select * from HostAuth;
    _id = 1
protocol = eas
address = owa.CorpExchangeServerExample.com
    port = 0
    flags = 5
    login = thisIsTheirUserNameInPlainText
password = thisIsTheirPasswordInPlainText-Seriously
    domain = NeverHurtsToHaveTheDomainInfoToo
accountKey = 0
```

DATA AT REST ACCESS TECHNIQUES

- physical access
- malicious code

DATA IN TRANSIT

- on a network
- or in RAM
- susceptible to
 - man in the middle
 - DNS Spoofing
 - TMSI overflow (baseband attack on GSM networks)

ANDROID DEVICES AS AN ATTACK VECTOR

- Data Stroage mass USB mode
- Recording Device audio, video, photo
- Circumventing network controls
 - Connected via USB to a workstation
 - Wireless access point

SECURITY CONSIDERATIONS

- very difficult
- h/w and s/w created and maintained by a broad group incl manufacturer and carrier
- custom apps installed by user
- device may be rooted
- · connects to many networks none of which are fully trusted

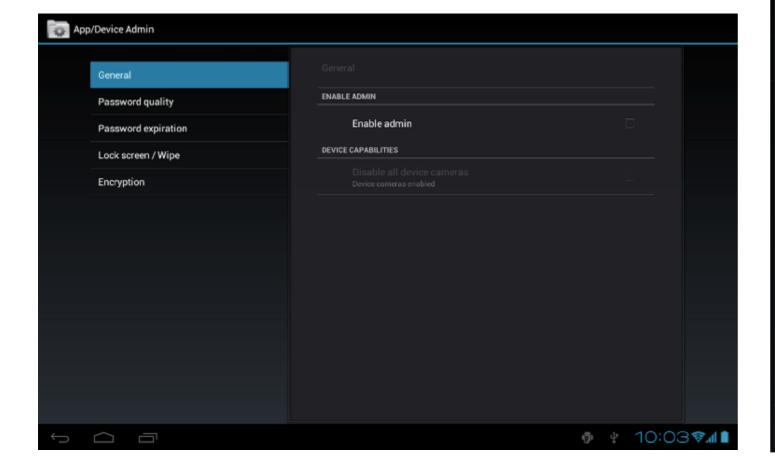
INDIVIDUAL SECURITY STRATEGIES

- Always use a data network you trust, cellular less susceptible to rogue access points
- Use a device passcode, wipe if entered incorrect
- Check services such as the appWatchdog
- Beware of link in SMS and emails, harder to identify fraudulent sites on a mobile device, three times more likely to click than a PC user
- Use an alternative browser
- Beware of the permissions required by a phone app

CORPORATE SECURITY STRATEGIES

- Policies are the phones covered in corporate policies in for example, Acceptable Usage, Data Security, Backups and Data Retention, E-Discovery
- Password/Pattern/Pin Lock max attempts to lock device
- Remote Wipe important but problematic if device set to airplane mode, employees cell plan disabled or if the device has been rooted. A countdown app can be used instead of this
- Upgrade to latest software
- Remote device management allows devices to be made adhere to policies eg: password enabled, min password length, max failed attempts, max inactivity timelock, prompt user for new password, lock device, wipe device

http://developer.android.com/guide/topics/admin/device-admin.html



Activate device administrator?



Sample Device Admin



Additional text explaining why this needs to be added.

Activating this administrator will allow the app API Demos to perform the following operations:

Erase all data

Erase the tablet's data without warning, by performing a factory data reset

Change the screen-unlock password

Change the screen-unlock password

Set password rules

Control the length and the characters allowed in screen-unlock passwords

Monitor screen-unlock attempts

Monitor the number of incorrect passwords entered when unlocking the screen, and lock the tablet or erase all the tablet's data if too many incorrect passwords are entered

Lock the screen

Control how and when the screen locks

Set lock-screen password expiration

Control how frequently the lock-screen password must be changed

Set storage encryption

Require that stored application data be encrypted

Disable cameras

Prevent use of all device cameras

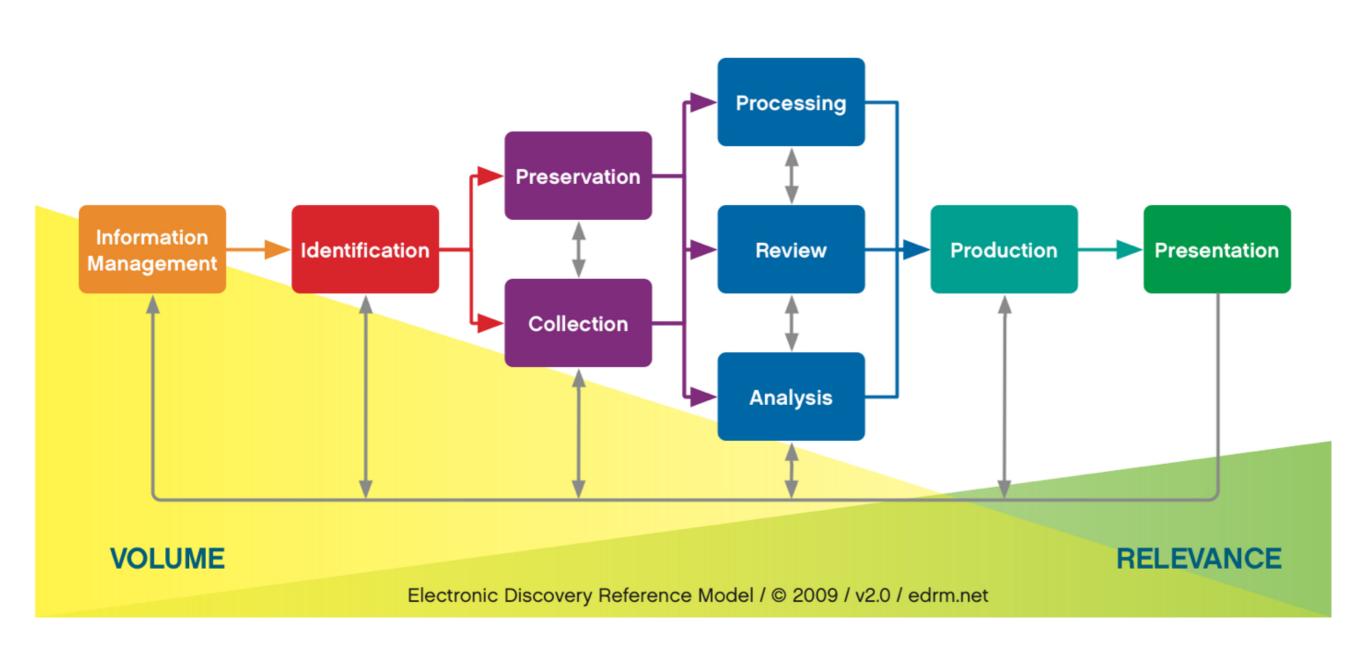
Cancel Activate

APP DEV SECURITY STRATEGIES

- Usernames should not be stored in plaintext
- Passwords should not be stored in plaintext, alternatives include token systems
- Read the AppWacthdog whitepaper

BYOD has big implications for EDRM

Electronic Discovery Reference Model



HANDLING AN ANDROID DEVICE

- Passcode increase timeout or enable stay awake
- Network isolation
- Power and Data Cables
- Powered off devices