Mobile devices – boon or curse

- **Oliver Ng -** Director of Training
- **Kishor Sonawane -** India Lead

Security Compass

Consulting & Training

Consumerization

- "According to Apple's chief operating officer, 65 percent of Fortune 100 firms are already deploying the iPad or piloting projects, and many analyst firms are predicting an explosion of tablet devices in the enterprise in 2011."
  http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf

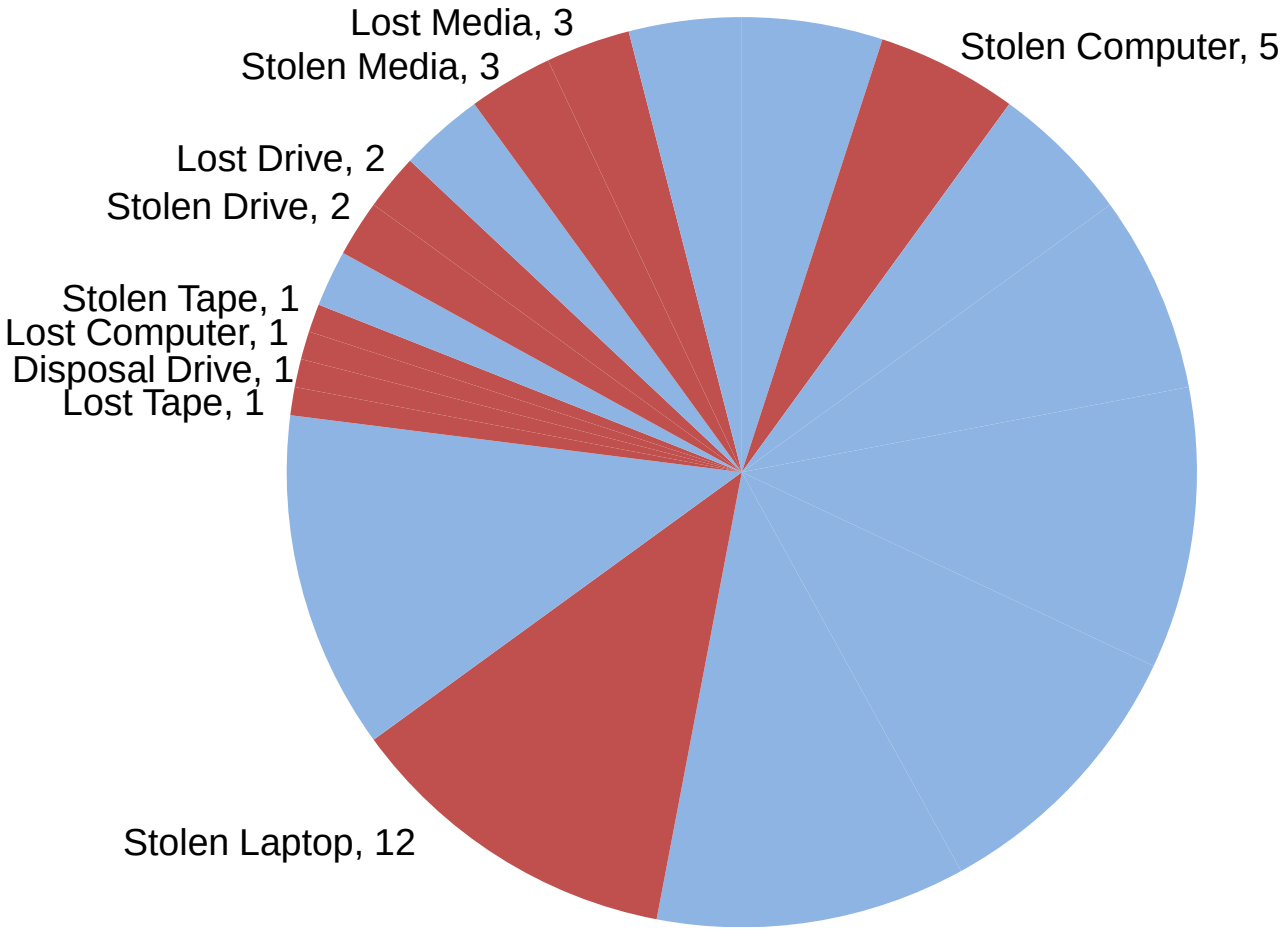
Consumerization

- Blurring the line between *work* and *personal*
- As a company, you have choices:
  - Provide employees with consumer-level devices
  - Allow access to corporate assets from their personal devices
- But what are the implications?

What are the risks?

- Emails (personal or work)
  - Archive
  - Ability to send as employee
- Credentials to and locations of corporate assets
- Sensitive documents, contracts, agreements
- Contact lists
  - Important for phishing , competitive risks

Lost Data



2010 incidents by breach type

Source: datalossdb.org

n:scenario for miwf

The situation

technolust

- CXO's sees the latest Android device launched, and he's a busy one.
- Loves the device and connects it for business and pleasure for:
  - gmail.com
  - company.com
  - Secure document storage app

What are mobile threats?

Lost or stolen phone

Weakly programmed applications

Malware

Man in the middle attacks

Cases we've seen

1. Case of the lost phone
   - Default Email Client

2. Case of the broken app
   - Encrypted document app

3. Case of the broken safe
   - Custom email app for corporate

Case of the lost phone

Lost or stolen phone

- CXO loses phone 2 days later after setting it all up
  - More likely to lose phone than a computer
- How do we normally mitigate against lost computers?
  - Strong passwords
  - Encryption (TrueCrypt, PGPDisk)

Strong Local Passwords

- Passwords can be circumvented with rooting or jailbreaking
- A phone can be compromised and returned (cloned)

Video

- Lockscreen bypass

File System Encryption

- Available on Blackberry
- Available as of iOS 4, kind of
  - API is for apps, not full disk encryption
- Available in Android 3.1+
  - 3.1 is for tablets only, not phones!

Case of the lost phone – Android Email Client

- CXO didn't set lock screen, Uh oh.
  - Easy access to data on phone
  - At mercy of app security, this is still important!

- Android Gmail client does not require added authentication
  - Gmail, GoogleApps mail could be compromised

Case of the lost phone – Android Email Client

- Attacker finds out CXOs personal info and website credentials, easily searchable in the Android mail interface

Defense: At minimum have keyguards, but still, not 100% solution

Case of the bad app

- How well is that app made? Can you trust it?

Mobile app development weaknesses

- Developers still have to learn secure code
- Why do we seem to forget web app security basics?
- Trust issues
  - We trust apps too much because we trust our mobile

Case of the bad app – Secure Doc App

- CXO needs to store documents. Buys a vendor app to “securely” download docs.
- App automatically “expires” document after a couple hours

- Vendor tells CXO that app only lets you read documents for predetermined time

Case of the dumb app – Secure Doc App

- We gain file system access, look at "expired" document's last modified date

- Reset clock back to that date… access granted to secure document!

Defense: Can you trust vendor applications? Test.

Case of the broken safe

- Storage of information by apps, is it secure?

Case of the broken safe – Custom email app

- Enterprise mail client requires the user to enter their credentials to check e-mail
  - Must be kept somewhere, how?

- Look for shared preferences XML (rooted phone)

```
# adb shell
# cd data/com.<productname>/shared_prefs
```

Case of the broken safe – Custom email app

- We found the credentials stored in the XML file, unencrypted

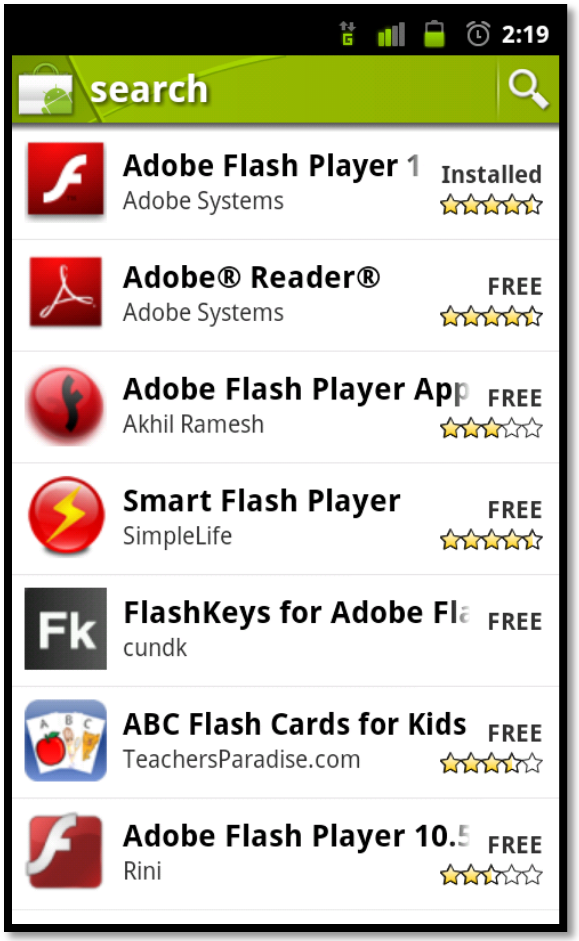
```
# cat preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<string name="serverpass">password</string>
<string name="localpasssalt">KKIEIrZeeN1+bDh6Zzy8luKyiXnGDkIkGt6sRpVmzCY=
</string>
<string name="serveruser">jdoe</string>
<boolean name="firstrun" value="false" />
<string name="localpasshash">L2EZX2oc7y0rrb4wxc9ex/UHtfBggN7OQLGkmJSY+uQ=
</string>
```

- *Defense: Don't trust apps to protect your most sensitive credentials*

Mobile Malware

Malware

- Android market, not checked
  - This is a problem
- iPhone app store, checked
  - But nobody knows how



Malware

- Emerging threat… but not clear yet
- 76% = increase in malware Q2 vs Q1 2011 (Mcafee)
- We see the most on Android
  - Pirated apps / alternative markets
  - Some has crept into the official Android Market, but quickly stamped out

Typical Android Malware

- Legitimate application is repacked to contain malware
- Attempts to root the device with exploit
- Sends phone data to command and control
  - can grab data, send messages, make calls

Defense!

- Install from legitimate sources & trusted developers
- Spot the cues such as evil permissions
- Mobile antivirus such as Lookout Security
- Solutions like Mobile Active Defense (MAD) can help you to limit apps

Man in the Middle

Man in the Middle

- MITM happens in mobile!
- Funnel traffic through corporate VPN
  - Now you have VPN credentials stored on phone
- MAD automatically routes traffic through their own VPN
  - They may do some deep packet inspection on your traffic
  - Is this a good thing?

Final thoughts

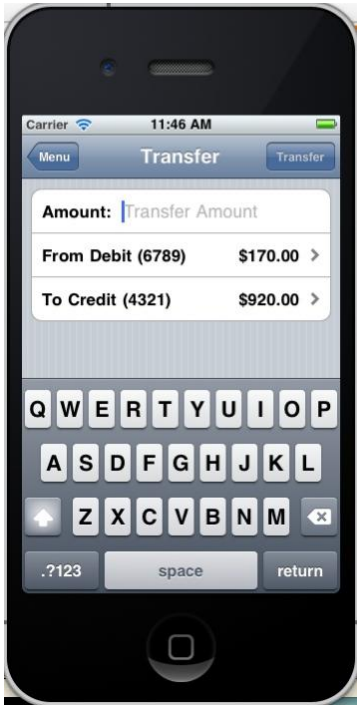
Final thoughts

- Assess risks as required for your business
- At minimum have key lock on the device
- Promote device policies and mobile management policy
- Don’t forget, we learned all these issues before in web apps!

Final thoughts

- Have your security team review vendor apps
  - As with desktop software, ask questions before purchasing for corporate deployment

iPhone and Android ExploitMe Mobile Labs are here



Will be out soon!

http://labs.securitycompass.com

Questions?

Oliver Ng - Director of Training
Kishor Sonawane - India Lead

Security Compass:
http://www.securitycompass.com

Contact us:
training@securitycompass.com

Follow:
@securitycompass