# iPhone Insecurity:

## Security issues for enterprises to consider

SANS Information Security Webcast

18 May 2010
Geneva, Switzerland

Jim Herbeck
Managing Partner, Nouvel Strategies
JHerbeck@NouvelStrategies.com

Member of Faculty, SANS Institute
JHerbeck@sans.org

Webcast archive may be viewed at:
https://www.sans.org/webcasts/iphone-insecurity-93463

NOUVEL

# Agenda

- The risks
- The threats
- The vulnerabilities
- The future

# Understanding the risks

- The iPhone is **not**:
  - a telephone
  - an iPod.
- The iPhone:
  - **is** a portable computer.
  - **has** an enormous amount of stored data.
  - **needs** to be secured.

Wikimedia Commons: public domain image/copyright expired



# Specific risks

- Tangible risk:
  - Loss of the iPhone due to theft.
    - Loss of availability.
  - Loss of information assets on the iPhone due to theft.
    - Loss of confidentiality.
  - Impersonation or fraud by masquerading using stolen iPhone.
    - Loss of integrity.
- Intangible risk:
  - Bad publicity.
  - Loss of trust, reputation.
  - Loss of clients.

# Understanding the threats

- Who in the organization carries iPhones:
  - Executives, with confidential Emails about financial data or mergers and acquisitions.
  - Sales people, with sensitive information about upcoming sales, and an Address Book filled with current customers.
  - Workers, with proprietary information about products, services, or customers.

- Characterize the threat:
  - Threat based on random loss or theft of a popular, trendy smartphone.
  - Threat based on random attack by malicious software.
  - Threat based on targeted, industrial espionage.




# Top 10 iPhone vulnerabilities

**Technical Vulnerabilities:**

1. iPhone OS
2. App store
3. Jailbreaking
4. Passcode
5. Data encryption
6. System data

**Organizational vulnerabilities:**

7. Security policy
8. Configuration control

**Human vulnerabilities:**

9. Personalization
10. Physical security

# 1. iPhone OS vulnerabilities

- iPhone OS software vulnerabilities exist.
  - Flaws or weaknesses in iPhone OS.
  - Gateway for malicious app or malware.
- iPhone OS 3.0 fixed 46 security vulnerabilities.
  - How many more are there?
- iPhone/Linux vulnerability discovered yesterday by Bernd Marienfeldt.

http://marienfeldt.wordpress.com/2010/03/22/iphone-business-security-framework/



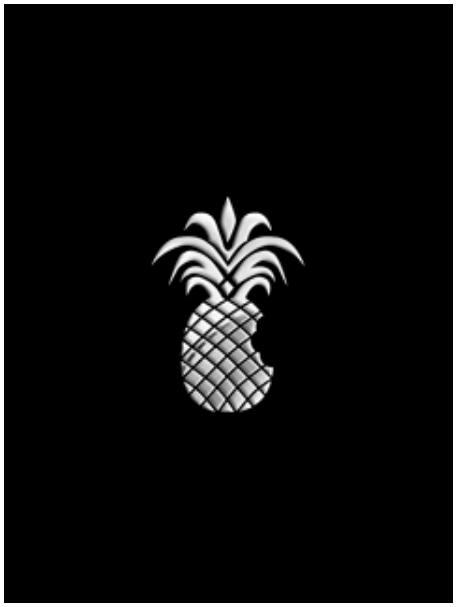

# 2. App store

- iPhone apps are “safe” because they can only be downloaded from the App store.
  - Apple approves the apps, to ensure they’re safe for you.
  - 234,266 Apps have been approved to date.
- But, Apple acknowledges that there are bad apps that have been submitted.
  - Apple VP Phil Schiller said, “There have been applications submitted for approval that will steal data”
- Nicolas Seriot has theorized how to create an app call SpyPhone and distribute it through the App store.

http://seriot.ch/

# 3. Jailbreaking

- iPhone can be “jailbroken:”
  - Process to modify iPhone OS to permit non-Apple authorized code to be installed and executed.
  - Creates new vulnerabilities.
- An estimated 6-8% of 50+ million iPhones are jailbroken.
  - Are 3-4+ million jailbroken iPhones securely configured?
- Jailbreaking is of questionable legality and voids your warranty.






# 4. Passcode

- Smartphone passcodes by default are usually weak, 4-digit numeric passwords.
- iPhone passcodes are even weaker.
  - With physical access to the device and a USB cable, an iPhone passcode can be trivially removed.
- Jonathan Zdziarski has a YouTube video demonstrating how to bypass the iPhone passcode.
  - Author of “iPhone Forensics”.
  - There is some complexity in technique (and variation depending upon iPhone OS version).

http://www.youtube.com/watch?v=5wS3AMbXRLs

# 5. Data encryption

- iPhone models prior to the iPhone 3GS did not encrypt any stored data.
  - A serious issue for business users.
- With the iPhone 3GS, all data store on the iPhone is encrypted.
  - Business issue solved, except…
- It's relatively trivial to trick the iPhone into making an unencrypted copy of all the data on the phone:
  - Jonathan Zdziarowski has a helpful YouTube video called "What Data Can You Steal From an iPhone 3GS in 2 Minutes."

http://www.youtube.com/watch?v=34f47m-lYSg




# 6. System data

- The iPhone store a lot of data you may not think about:
  - Email parameters, including name and Email address, but…
    - Not the mail server password.
    - Not messages, though they can be retrieved using previous method.
  - Keyboard cache:
    - All characters entered, except passwords.
  - Address book contents.
  - Safari history (last 20 entries).
  - YouTube history.
  - Wifi network history.
  - Digital photo geotags and EXIF tags:
    - Time/date and location of the iPhone when photos were taken.
  - Automatic screenshots, taken every time the "home" button is pushed.
- If someone has physical access to your iPhone, they can get a copy of all the system data.

# 7. Security policy

- Many organizations “exempt” the iPhone from compliance with the established information security policy.
- Usually, there are two possible misconceptions:
  - Apple says the iPhone is secure, so it’s OK, right?

  or
  - It’s just a phone, so we don’t have to worry about InfoSec.
- Because VIP’s often are the ones “demanding” iPhones, Information Security Officer’s may be afraid to say, “No.”




# 8. Configuration control

- Many organizations permit users to control their iPhone configurations.
- The only secure way to manage smartphones is by using a centralized configuration application, with a security template.
- Apple created the free iPhone Configuration Utility. Many organizations either aren’t using it, or don’t understand what to do:
  - Create longer, alpha-numeric passcodes.
  - Restrict downloads from the App store.
  - Lock Email to only check a corporate account.
  - Block explicit content.
  - Block the use of the camera
  - Block web browsing

# 9. Personalization

- Many users like to “personalize” their iPhone.
  - For your personal iPhone, that’s OK.
  - For your business iPhone, that exposes the organization to risk.
- Using a cute photo for the background rather than a flash screen with a warning banner on a business iPhone is inappropriate. (sample warning banner->)
- Jailbreaking a business iPhone is inappropriate.
- Downloading lots of non-business apps on a business iPhone is inappropriate.





# 10. Physical security

- Perhaps the biggest risk for any smartphone is the loss or theft of the mobile device.
- As the iPhone is a popular, trendy device, this is a real problem.
  - This is even a problem for Apple, as an iPhone Engineer recently left an iPhone prototype at a bar.
- It’s not practical to use cable locks with iPhone’s

## iPhone vulnerability management

- Some of the iPhone vulnerabilities can be mitigated.
- As you'll see, some crucial vulnerabilities cannot…




## 1. iPhone OS vulnerabilities: Risk mitigation

- Keep iPhone OS software current.
- Apply iPhone OS security patches promptly.
- Hope security researchers keep finding iPhone OS vulnerabilities
- Hope Apple does a good job fixing security vulnerabilities—promptly.

## 2. App store: Risk mitigation

- Update security policy: only install authorized apps from trusted sources.
- Use the iPhone Configuration Utility to prevent user visits to or downloads from the App Store.
- Periodically audit devices to ensure compliance.




## 3. Jailbreaking: Risk mitigation

- Update security policy: prohibit jailbreaking iPhones (installing unauthorized modifications to the OS).
- Include a “no jailbreaking” message in the next Awareness program.
- Periodically audit devices to ensure compliance.
- Hope Apple includes something like Intel’s TPM and Microsoft’s BitLocker in a future release.

Note: with physical access and a USB cable, this vulnerability still exists.

## 4. Passcode: Risk mitigation

- Update security policy: iPhone passcodes must comply with established password policy.
- Use the iPhone Configuration Utility to enforce password policy.
- Periodically audit devices to ensure compliance.

Note: with physical access and a USB cable, this vulnerability still exists.




## 5. Data encryption: Risk mitigation

- Update security policy: require iPhone models that support data encryption (iPhone 3GS).
- Keep iPhone OS software current.
- Wait for the improved encryption features promised with iPhone OS 4.

Note: with physical access and a USB cable, this vulnerability still exists.

## 6. System data: Risk mitigation

- Vulnerability fixed with:
  - Data encryption (see previous risk mitigation).
  - Improvements in Apple's sandbox security.

Note: with physical access and a USB cable, this vulnerability still exists.




## 7. Security policy: Risk mitigation

- Enforce security policy on iPhones.
- Depending upon the organization's security policy, this may involve getting rid of iPhones.
- Many have already noted that it's presently difficult to justify using the iPhone in "regulated" industries:
  - Banking
  - Healthcare
  - Pharma

## 8. Configuration control: Risk mitigation

- Update security policy: require configuration control using secure profiles for the iPhone.
- Use the iPhone Configuration Utility:
  - http://www.apple.com/support/iphone/enterprise/
- Periodically audit devices to ensure compliance.

Note: with physical access and a USB cable, this vulnerability still exists.




## 9. Personalization: Risk mitigation

- Update security policy: prohibit personalization of business iPhones.
- Use the iPhone Configuration Utility to prevent personalization.
- Periodically audit devices to ensure compliance.

Note: with physical access and a USB cable, this vulnerability still exists.

## 10. Physical security: Risk mitigation

- Update security policy: make users responsible for reporting lost or stolen iPhones.
- Use the iPhone Configuration Utility to enforce automatic wiping after 10 bad access attempts.
- Use “Remote Wipe” for missing iPhones:
  - Via MobileMe for personal users (can take 2+ hours).
  - Via an Exchange Server for business users.




## iPhone risk management

- Recognize what the security requirements are for your organization.
- Recognize what the unfixable vulnerabilities are on the iPhone.
- Recognize what kind of data your potential iPhone users will risk exposing by using an iPhone.
- Make an informed risk management recommendation to management.

# The future: iPhone OS 4

- Announced April 8, 2010; to be delivered “this summer.”
- Most of the security-related improvements come under the heading of “New enterprise features:”
  - New data protection APIs
  - Email messages and attachments encrypted using device passcode
  - New mobile device management APIs, for improved configuration control

http://www.apple.com/iphone/business/preview-iphone-os/




# Agenda

- The risks
- The threats
- The vulnerabilities
- The future

# iPhone Insecurity:

## Security issues for enterprises to consider

SANS Information Security Webcast

18 May 2010
Geneva, Switzerland

Jim Herbeck
Managing Partner, Nouvel Strategies
JHerbeck@NouvelStrategies.com

Member of Faculty, SANS Institute
JHerbeck@sans.org

Webcast archive may be viewed at:
https://www.sans.org/webcasts/iphone-insecurity-93463

NOUVEL