iPhone Insecurity

2011 UPDATE

SANS Information Security Webcast

19 Apr 2011
Geneva, Switzerland

Webcast archive:
https://www.sans.org/webcasts/iphone-insecurity-2011-update-94443

Annotated slides:
http://nouvelstrategies.com/iPhone-insecurity

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

Member of Faculty, SANS Institute
JHerbeck@sans.org

Agenda

- Review: risks, threats, and vulnerabilities
- Updating the top 10 iPhone vulnerabilities
- Smartphone security
- The bigger iOS picture
- The future

Reviewing the risks

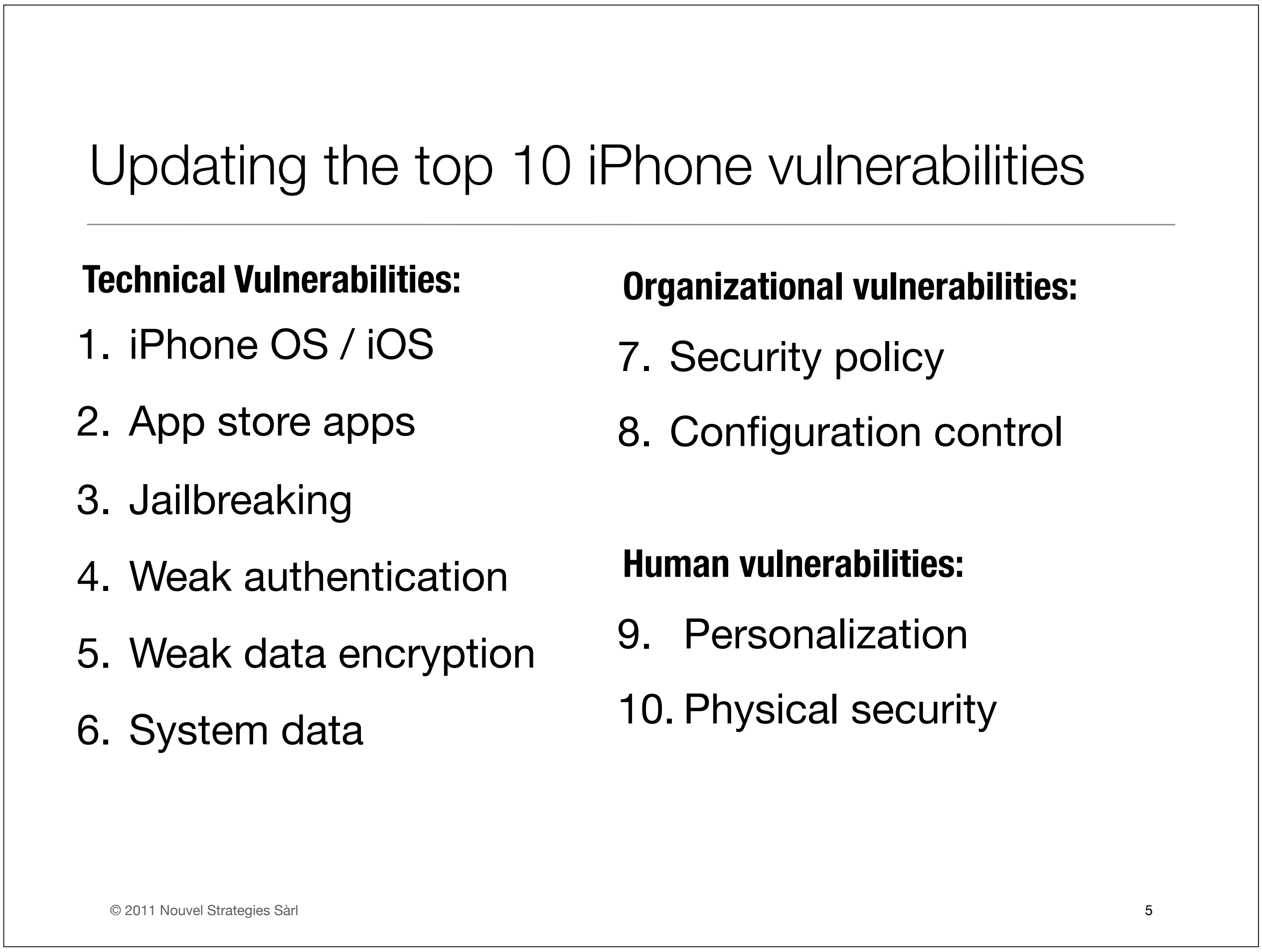
- The iPhone:
  - **is** a portable computer
  - **has** an enormous amount of stored data
  - **needs** to be secured
- Tangible risk:
  - loss of phone or data
- Intangible risk:
  - bad publicity, loss of reputation or clients

Wikimedia Commons: public domain image/copyright expired

Wikimedia Commons: public domain image/copyright expired

Reviewing the threats

- Who carries iPhone’s:
  - VIP’s? (sensitive data)
  - sales people? (customer data)
  - workers? (corp data)
- Types of threats:
  - random theft of trendy device
  - random attack by malware
  - advanced persistent threat



Updating the top 10 iPhone vulnerabilities

Technical Vulnerabilities:

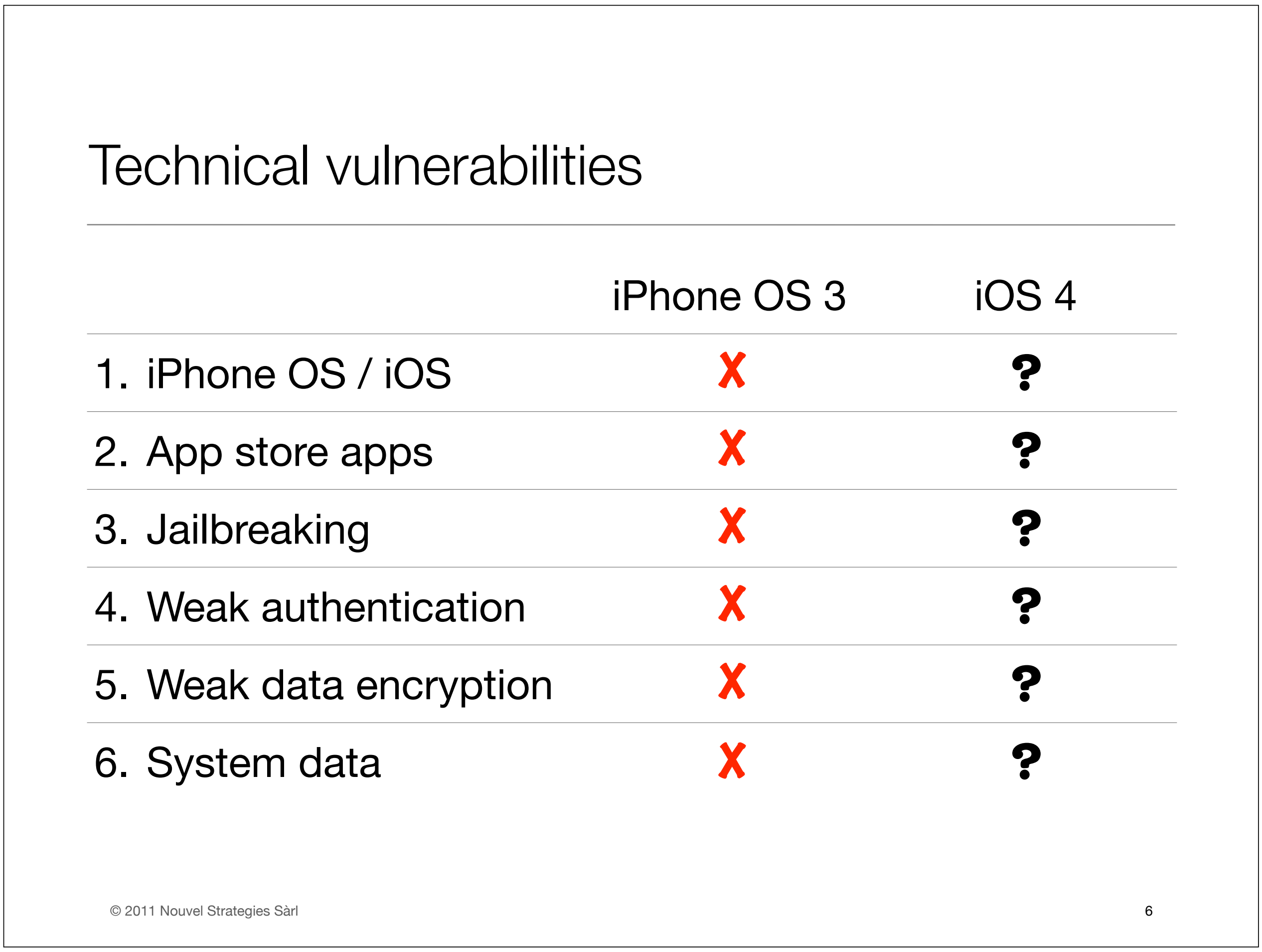
1. iPhone OS / iOS
2. App store apps
3. Jailbreaking
4. Weak authentication
5. Weak data encryption
6. System data

Organizational vulnerabilities:

7. Security policy
8. Configuration control

Human vulnerabilities:

9. Personalization
10. Physical security



Technical vulnerabilities

	iPhone OS 3	iOS 4
1. iPhone OS / iOS	✗	?
2. App store apps	✗	?
3. Jailbreaking	✗	?
4. Weak authentication	✗	?
5. Weak data encryption	✗	?
6. System data	✗	?

STILL VULNERABLE

1. iPhone OS / iOS vulnerabilities

- OS vulnerabilities exist:
  - flaws or weaknesses in iPhone OS / iOS
  - gateway for malicious app or malware
- iOS 4 fixed many security vulnerabilities:
  - how many more are there? Security update iOS 4.3 was released Mar 9, 2011

Risk Management:

- apply iOS 4 updates/security patches promptly
  - unfortunately, updates are made through iTunes, when the user connects and decides to update
- periodically audit iPhones to ensure compliance

STILL VULNERABLE

2. App store apps

- 3rd party apps may be malicious or vulnerable:
  - confidentiality, integrity, or availability could be compromised
  - Apple reviews/approves 3rd party apps to ensure quality/security
  - 350,000+ apps have been approved to date—with no errors?

Risk Management:

- update security policy: only install authorized apps from trusted developers
- use the iPhone Configuration Utility to disable “Allow installing apps”
- periodically audit iPhones to ensure compliance

STILL VULNERABLE

3. Jailbreaking

- "Jailbreaking" is a form of hacking:
  - modifies iOS to bypass normal app installation process
  - permits the installation of unauthorized, "rogue" apps
  - permits unauthorized configuration modification
  - creates new vulnerabilities: worms that target jailbroken iPhones

Risk Management:

- 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

STILL VULNERABLE

4. Weak authentication

- iPhone passcodes are usually weak, 4-digit numeric passwords:
  - With physical access to the device and a USB cable, an iPhone passcode can be removed via the "Zdziarowski Method"
- In Feb 2011, researchers at Fraunhofer Institute for Secure Information Technology (SIT) in Germany discovered a way to access passwords directly from the iOS password keychain

Risk Management:

- update security policy: iPhone passcodes should be consistent with established password policy
- use the iPhone Configuration Utility to disable "Allow simple password" and enforce the company's password policy
- periodically audit devices to ensure compliance

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

STILL VULNERABLE

5. Data encryption

- iPhone 3G and earlier did not encrypt any stored data
- iPhone 3GS and iPhone 4 running iOS 4 feature “data protection”, with hardware data encryption:
  - only if it’s enabled and only if 3rd party apps implement feature
  - iOS 4 uses this feature to protect Email and attachments

Risk Management:

- update security policy: require iPhone models that support data encryption and current iOS software
- use the iPhone Configuration Utility to disable “Allow simple password”, enforce the company’s password policy, and force encrypted backups
- periodically audit devices to ensure compliance

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

STILL VULNERABLE

6. System data

- The iPhone stores a lot of data you may not think about:
  - email parameters, keyboard cache, address book contents
  - history file (Safari, YouTube, Wifi networks)
  - digital photo geotags and EXIF tags
  - automatic screenshots, taken every time the “home” button is pushed
- If someone has physical access to your iPhone, they can potentially get a copy of all the system data

Risk Management:

- data encryption (see previous risk mitigation)
- hope for more improvements in Apple’s sandbox security

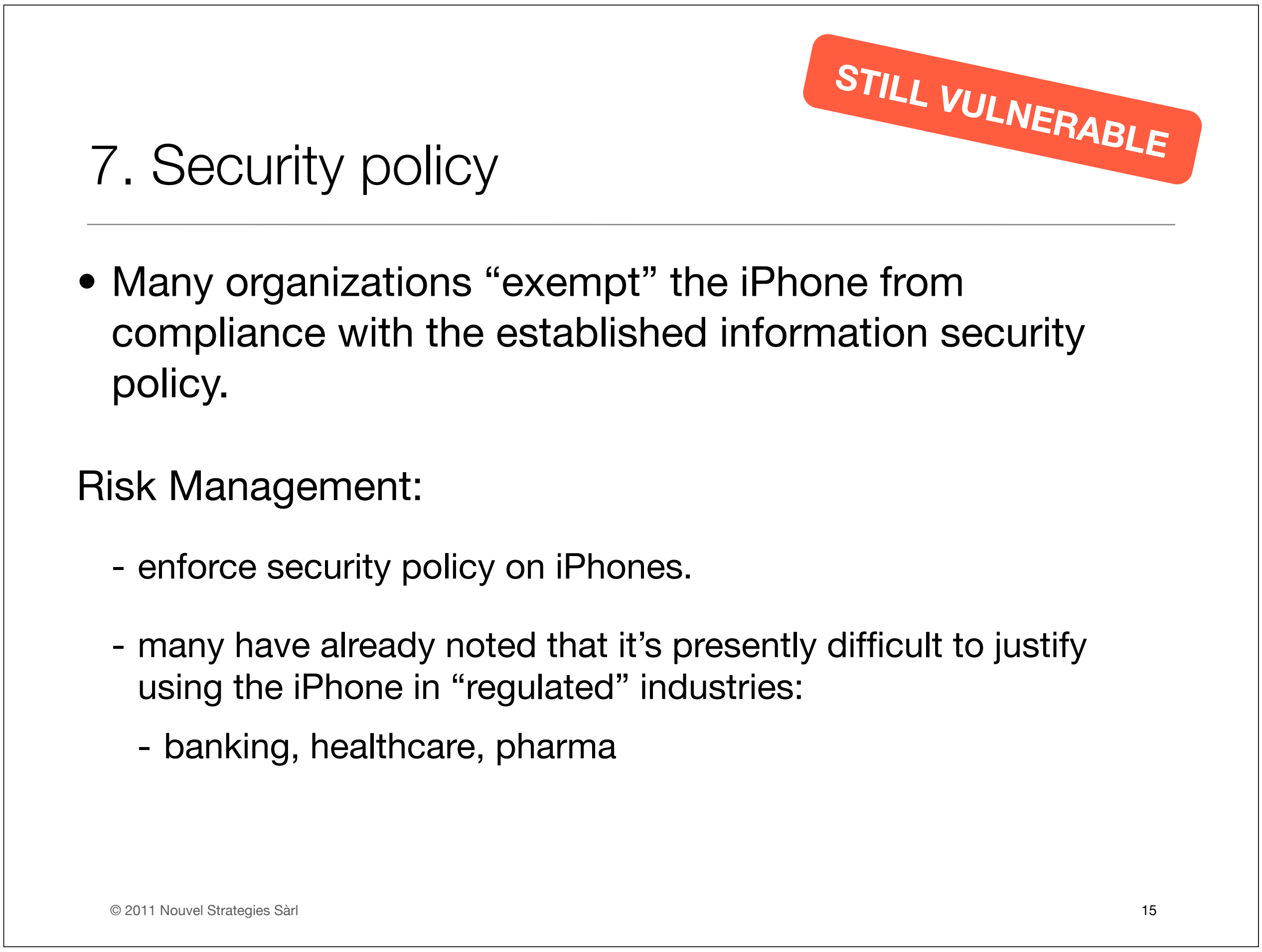
Note: with physical access and a USB cable, this vulnerability still exists

Technical vulnerability summary

	iPhone OS 3	iOS 4
1. iPhone OS / iOS	✗	STILL VULNERABLE
2. App store apps	✗	STILL VULNERABLE
3. Jailbreaking	✗	STILL VULNERABLE
4. Weak authentication	✗	STILL VULNERABLE
5. Weak data encryption	✗	STILL VULNERABLE
6. System data	✗	STILL VULNERABLE

Organizational and human vulnerabilities

	iPhone OS 3	iOS 4
Organizational vulnerabilities		
7. Security policy	✗	?
8. Configuration control	✗	?
Human vulnerabilities		
9. Personalization	✗	?
10. Physical security	✗	?



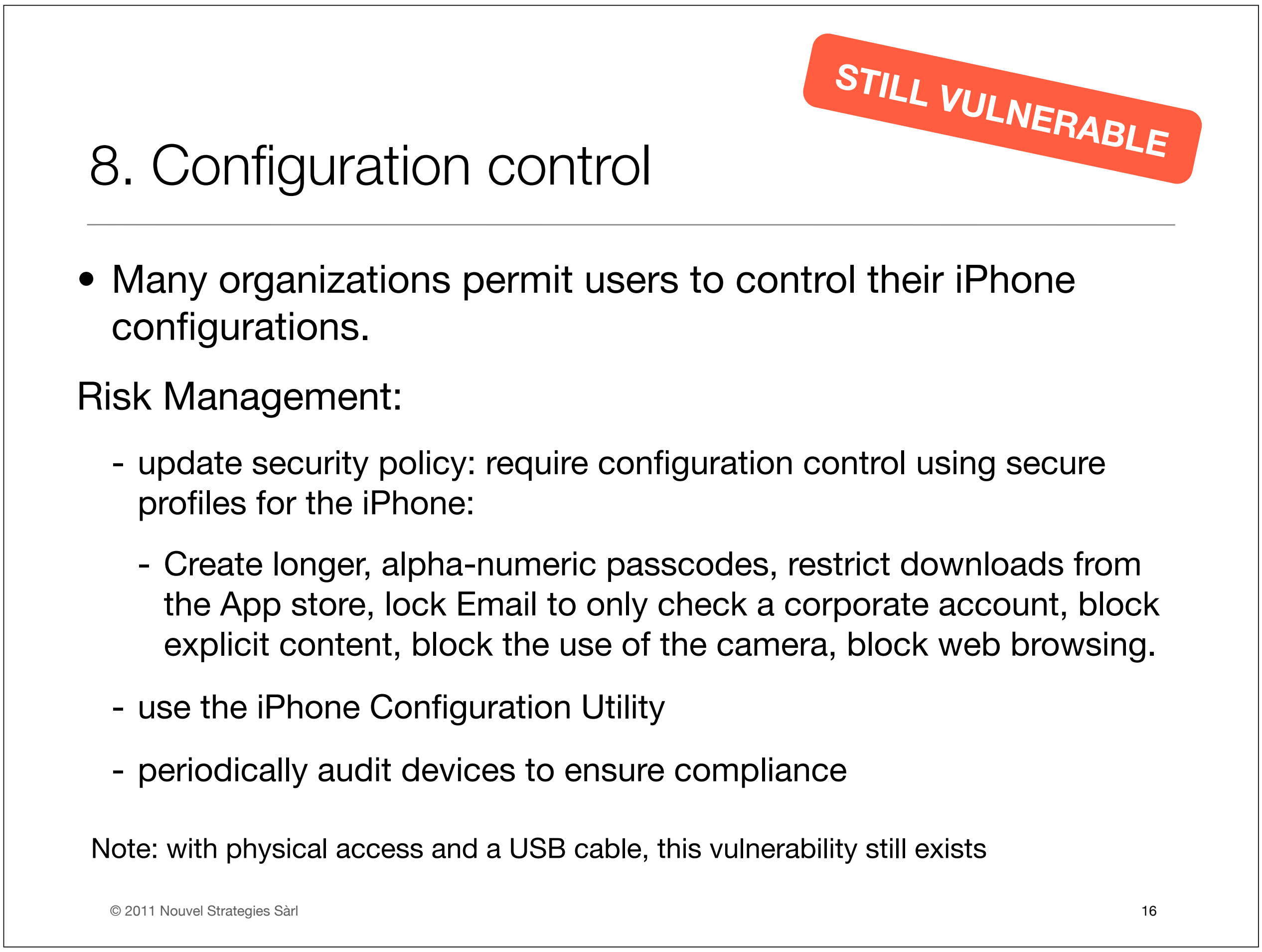
STILL VULNERABLE

7. Security policy

- Many organizations “exempt” the iPhone from compliance with the established information security policy.

Risk Management:

- enforce security policy on iPhones.
- many have already noted that it’s presently difficult to justify using the iPhone in “regulated” industries:
    - banking, healthcare, pharma



STILL VULNERABLE

8. Configuration control

- Many organizations permit users to control their iPhone configurations.

Risk Management:

- update security policy: require configuration control using secure profiles for the iPhone:
    - 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.
- use the iPhone Configuration Utility
- periodically audit devices to ensure compliance

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

STILL VULNERABLE

9. Personalization

- Many users like to “personalize” their iPhone.
  - cute background photos, different user interface “themes”
  - downloading non-business apps
  - jailbreaking often required to bypass “cumbersome IT restrictions”

Risk Management:

- update security policy: disallow 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

STILL VULNERABLE

10. Physical security

- Perhaps the biggest risk for any smartphone is the loss or theft of the mobile device
- It’s not practical to use cable locks with iPhones

Risk Management:

- 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 for older iPhones)
  - via an Exchange Server for business users

Organizational and human vulnerabilities

	iPhone OS 3	iOS 4
Organizational vulnerabilities		
7. Security policy	✗	STILL VULNERABLE
8. Configuration control	✗	STILL VULNERABLE
Human vulnerabilities		
9. Personalization	✗	STILL VULNERABLE
10. Physical security	✗	STILL VULNERABLE

Reviewing 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 the appropriate risk management recommendation so management can make an informed decision regarding iPhone usage

Smartphone security: the competition?

- There are competing smartphone operating systems:
  - Android (Google)
  - Blackberry OS (RIM)
  - Symbian (Nokia)
  - Windows Phone (Microsoft)
- How does iOS 4 compare?

Smartphone security: Android (Google)

- The recent, open-source alternative to the iPhone and iOS:
  - recently #1 in smartphone sales (depending upon whose data and what region in the world)
  - projected to have as much as 45% market share by 2016
  - works on multiple vendor hardware
  - apps distributed via Android Market (150,000+ apps) – and others
- Already has security issues:
  - Google has had to use their app removal capability to eliminate DreamDroid in March, 2011, after 50,000+ downloads
  - reports estimate 1 in 5 Android apps may have security problems
  - Android security may vary by vendor implementation

Smartphone security: Blackberry OS (RIM)

- Original business smartphone (since 2002):
  - strong in business environment
  - less popular in consumer environment—not as sexy
  - only works on Blackberry hardware
  - apps distributed via Blackberry App World (25,000+ apps)
- Has the strongest security reputation:
  - often cited as the "gold standard", most secure mobile device
  - recent problems in a few countries as the encryption was "too good" for the government to intercept communications
  - but, vulnerability exploited at the Pwn2Own 2011 Contest required RIM to advise users to disable Javascript in browser (Mar 14, 2011)

Smartphone security: Symbian (Nokia)

- The original multi-vendor smartphone OS:
  - largest installed base (estimated at 385+ million Q210)
  - recent sales indicate sharply falling market share
  - future uncertain after Feb 2011 agreement with Microsoft
  - apps distributed via Nokia Ovi Store (40,000+ apps)
- Security issues:
  - Symbian has been attacked by malware numerous times in the past 10 years
  - many Bluetooth attacks compromise smartphone and data:
    - Snarf, Backdoor, Bluebug, Bluejacking, ...

Smartphone security: Windows Phone (MS)

- Microsoft’s latest attempt at smartphone domination:
  - popular in corporate, Microsoft environments
  - less popular anywhere else
  - lowest sales figures and installed base (by an order of magnitude)
  - apps distributed via Windows Phone Marketplace (13,000+ apps)
- Has Windows security infrastructure—and issues:
  - Microsoft patch Tuesday for your smartphone’s “issues”
  - Great Microsoft security infrastructure—that requires a skilled IT staff to design, deploy, and maintain

The bigger iOS picture

- iOS 4 is now Apple’s OS for non-PC devices:
  - iPod Touch
  - iPad
  - Apple TV
- Businesses and organizations have started using these devices
- Security issues for iOS 4 on the iPhone apply to the other iOS devices:
  - Mail and apps are present on iPod Touch and iPad
  - Apple TV is probably less of a vulnerability
  - The dirty little secret of the lack of embedded system security

The future: iOS 5

- Under development, delivery date not yet announced.
  - Expected either in June or September, depending upon rumor website
- Should include new security features:
  - Not much is known today

Agenda

- Review: risks, threats, and vulnerabilities
- Updating the top 10 iPhone vulnerabilities
- Smartphone security
- The bigger iOS picture
- The future

iPhone Insecurity

2011 UPDATE

SANS Information Security Webcast

19 Apr 2011
Geneva, Switzerland

Webcast archive:
https://www.sans.org/webcasts/iphone-insecurity-2011-update-94443

Annotated slides:
http://nouvelstrategies.com/iPhone-insecurity

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

Member of Faculty, SANS Institute
JHerbeck@sans.org