

**McAfee®**



Protect what you value.

# Apple iPhone SDK Programming

Marius van Oers

McAfee Avert

© 2008 McAfee, Inc.

- Initially no regular **SDK**
- Safari browser based **Web 2.0 applications** – Ajax
- Instabilities in the mobile browser implementations, content attack exploits might be seen
- Less chance for malware
- Harder to patch
- No low level kernel hooking for AV/Firewall

The McAfee logo is displayed in a bold, red, sans-serif font on a black background.

10/9/2008



Protect what you value.

# ZiPhone

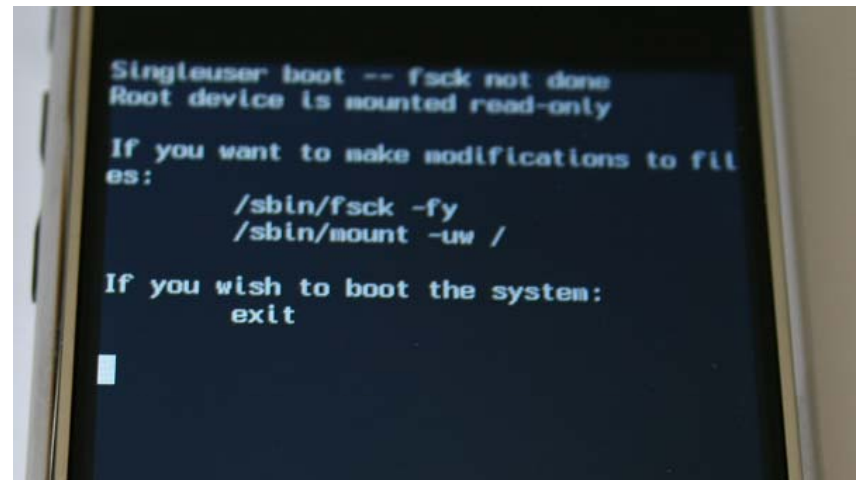
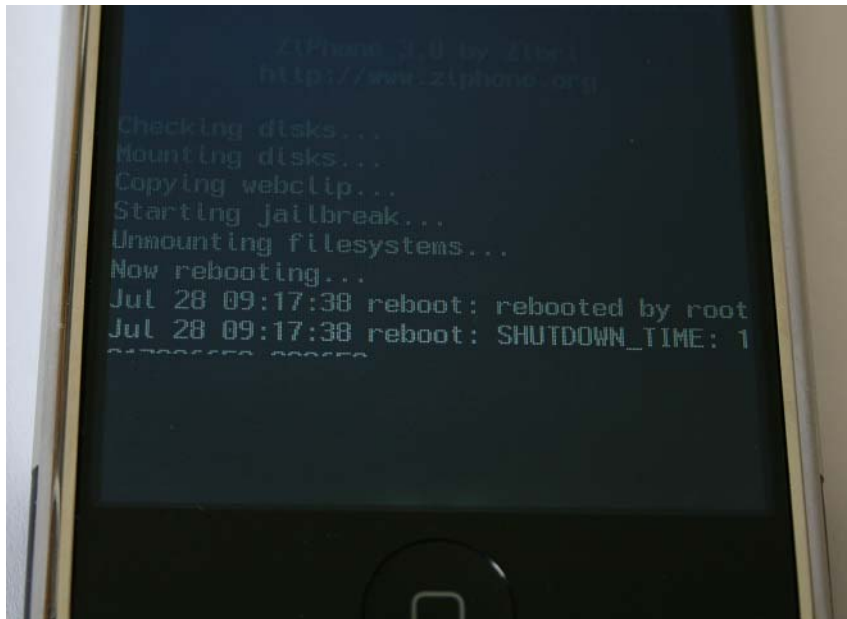


**McAfee**

10/9/2008



Protect what you value.



**McAfee**

10/9/2008



Protect what you value.

## Using “Jailbreak” like tools

- Possible to make a “disk” connection to the iPhone and see what files are onto the system.
- Change some background image or ringtone sounds but it was also possible to see and modify software on the iPhone.
- Security risk: trusting the crack program !

**McAfee**

10/9/2008



Protect what you value.

# Installing third party native applications



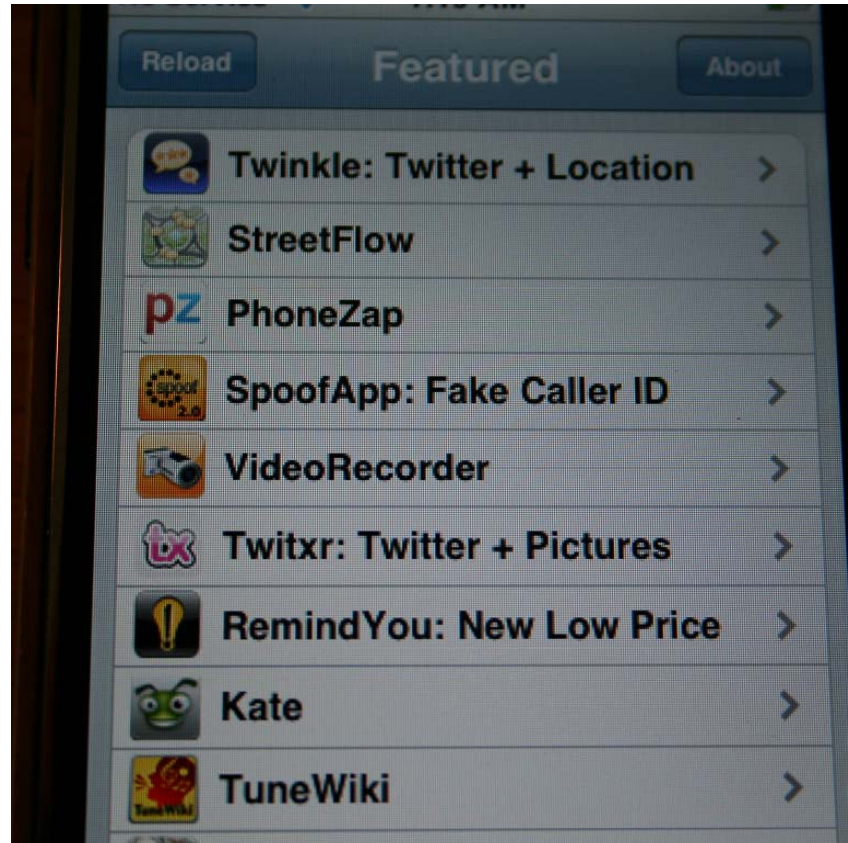
**McAfee**

10/9/2008



Protect what you value.

# Third party native applications



**McAfee**

10/9/2008



Protect what you value.

# iPhone SDK

- Early in 2008 beta versions of the SDK
- Native applications for the iPhone can now be build using the latest [Xcode](#) development environment.

**McAfee**

10/9/2008



Protect what you value.



# Xcode



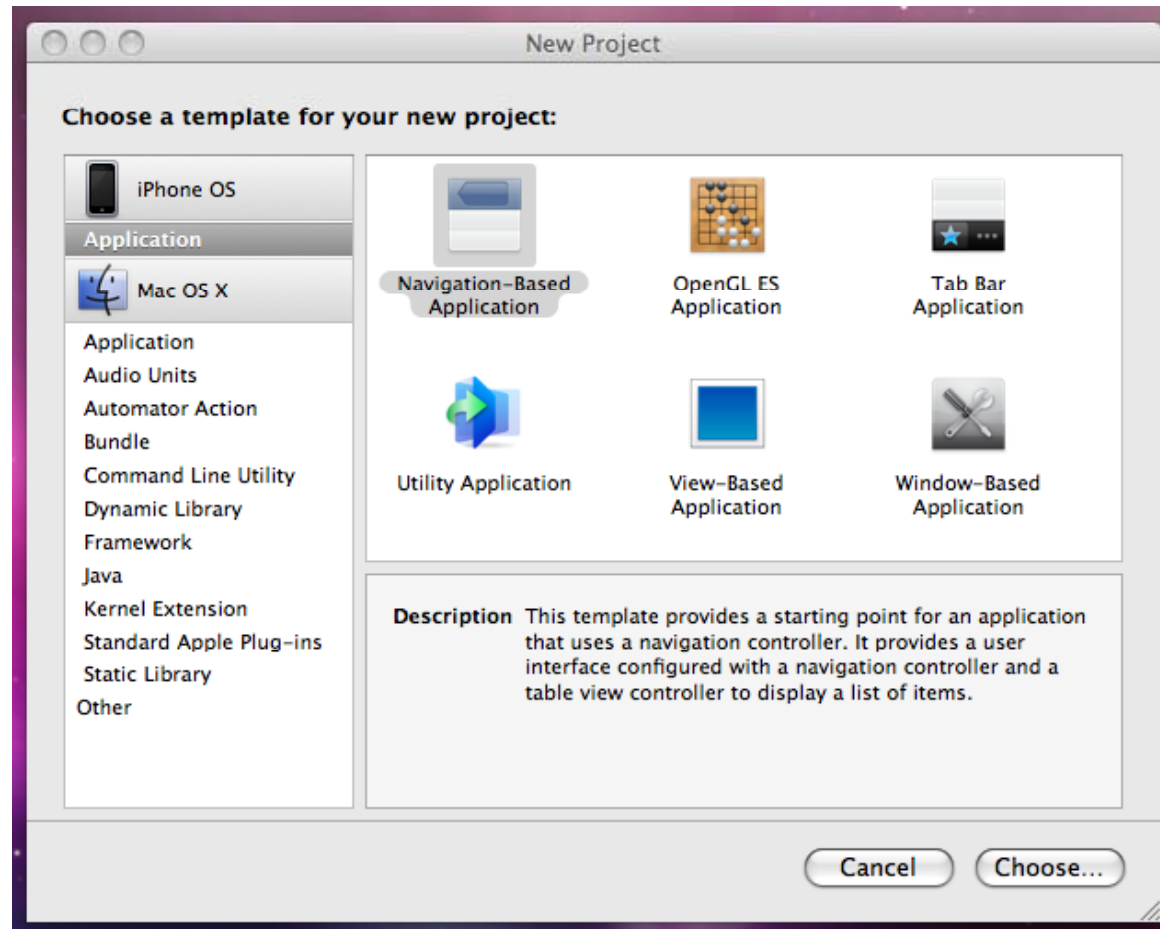
# McAfee

10/9/2008



Protect what you value.

# iPhone OS – New Xcode Project



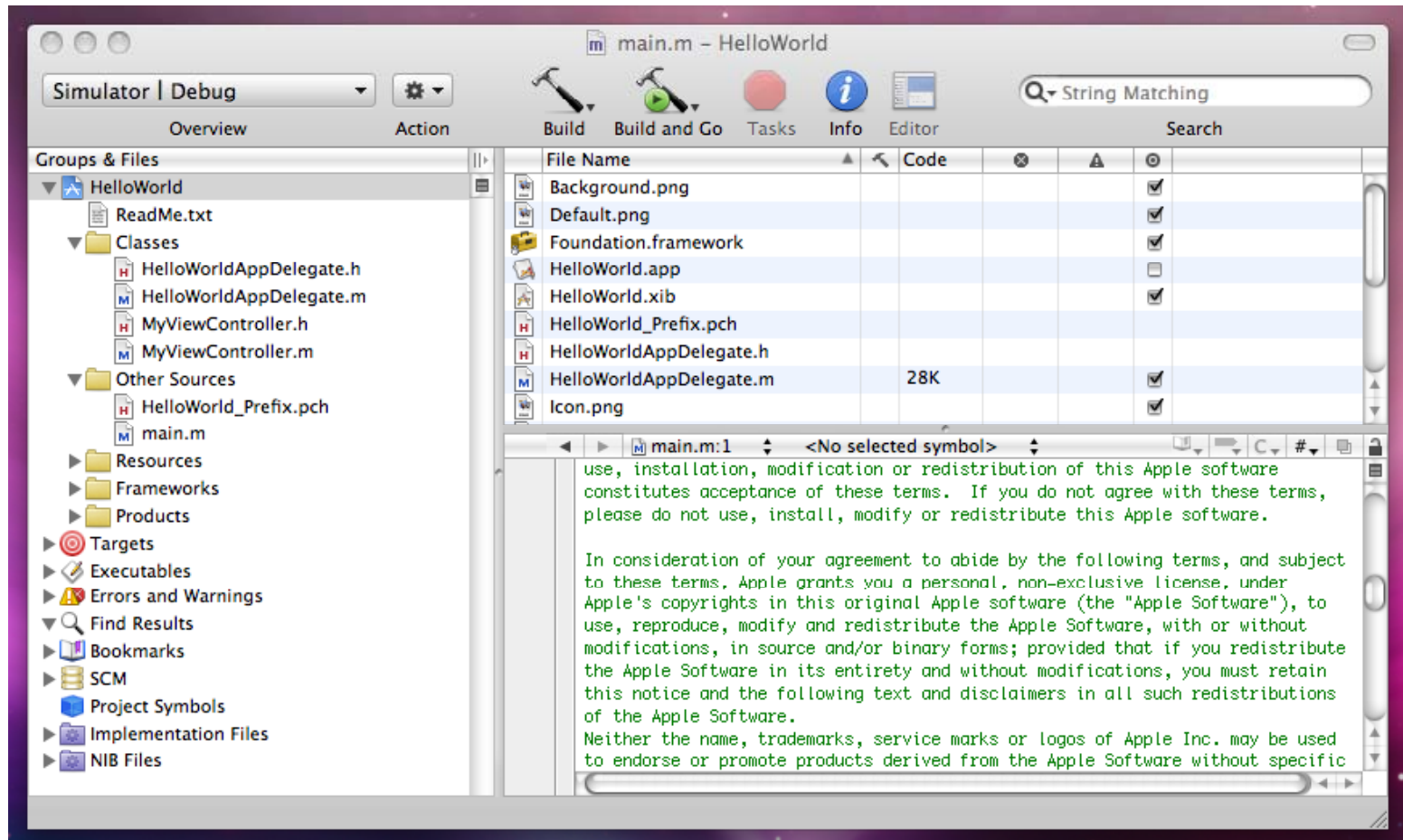
**McAfee**

10/9/2008



Protect what you value.

# Hello World



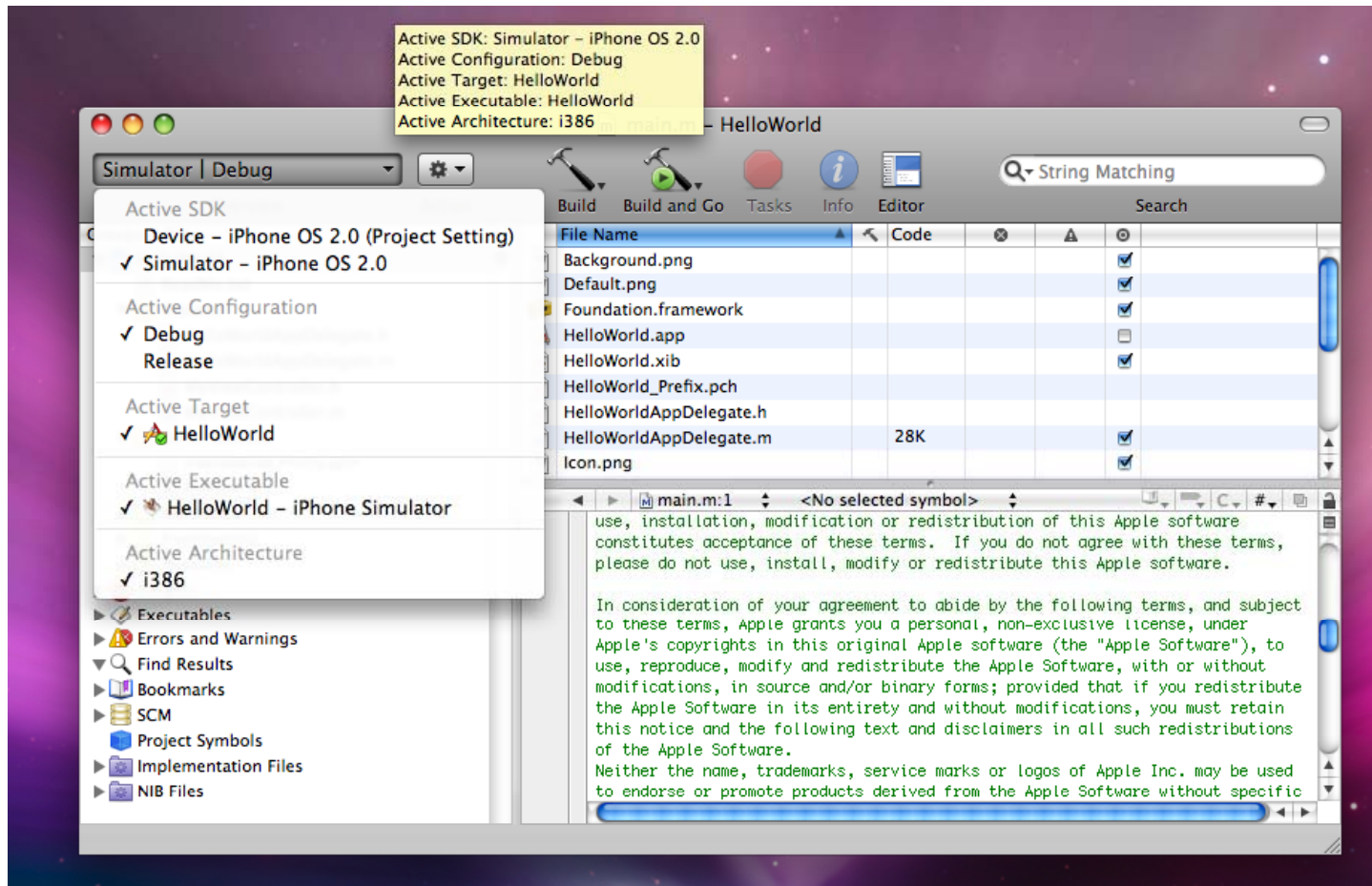
**McAfee**

10/9/2008



Protect what you value.

# Device or Simulator



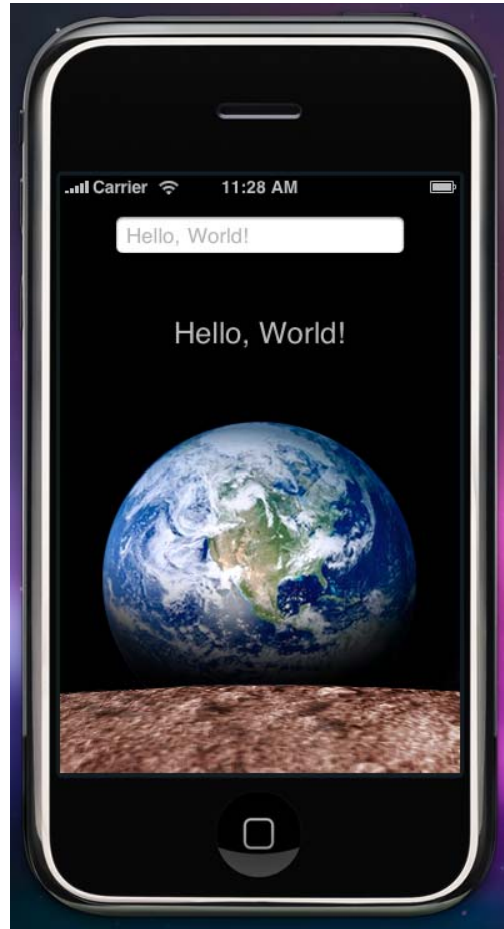
# McAfee

10/9/2008



Protect what you value.

# iPhone Simulator



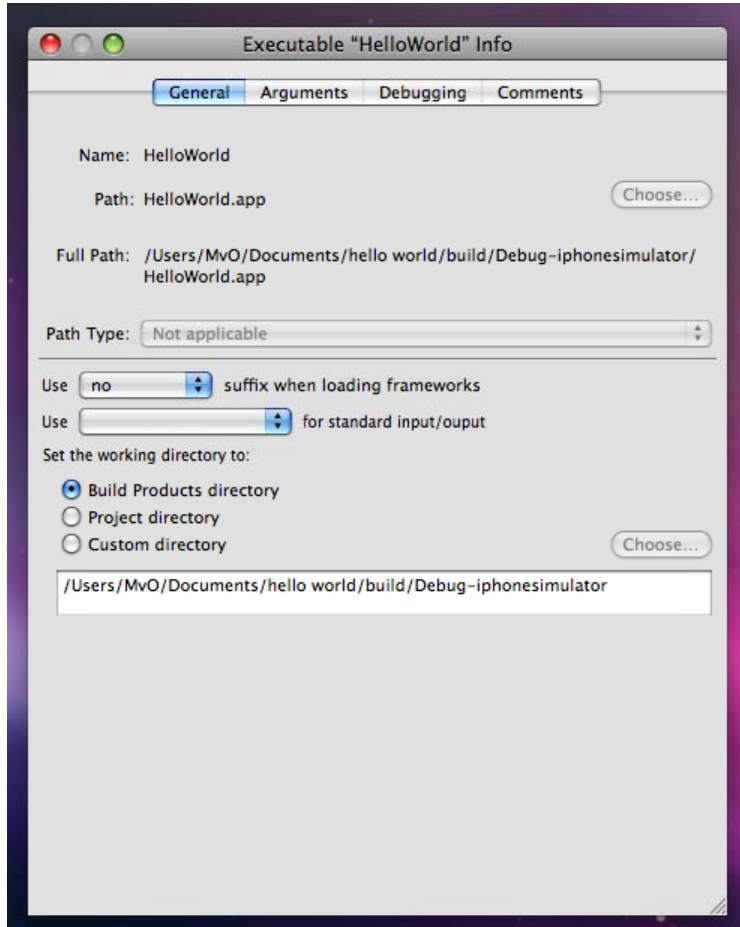
**McAfee**

10/9/2008



Protect what you value.

# Output Binary



C:\vb\conference\vb2008\_ottawa\demo code\001\hello world\build\Debug-iphonesimulator\HelloWorld.app\  
HelloWorld (24.208 bytes)

```

HelloWorld
00000000 CE FA ED FE 07 00 00 00 03 00 00 00 02 00 00 00  iuip.....
00000010 11 00 00 00 C4 09 00 00 85 00 00 00 01 00 00 00  .....A.....
00000020 38 00 00 00 5F 5F 50 41 47 45 5A 45 52 4F 00 00  8..._PAGEZERO..
00000030 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00  .....
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00000050 00 00 00 00 01 00 00 00 C0 00 00 00 5F 5F 54 45  .....A..._TE
00000060 58 54 00 00 00 00 00 00 00 00 00 00 00 10 00 00  XT.....
00000070 00 20 00 00 00 00 00 00 00 20 00 00 07 00 00 00  .....
00000080 05 00 00 00 02 00 00 00 00 00 00 00 5F 5F 74 65  .....te
00000090 78 74 00 00 00 00 00 00 00 00 00 00 5F 5F 54 45  xt.....TE
000000A0 58 54 00 00 00 00 00 00 00 00 00 00 FC 21 00 00  XT.....u!..
000000B0 86 06 00 00 FC 11 00 00 02 00 00 00 00 00 00 00  |...u.....
000000C0 00 00 00 00 00 04 00 80 00 00 00 00 00 00 00 00  |.....|.....
000000D0 5F 5F 63 73 74 72 69 6E 67 00 00 00 00 00 00 00  __cstring.....
000000E0 5F 5F 54 45 58 54 00 00 00 00 00 00 00 00 00 00  __TEXT.....
000000F0 84 28 00 00 79 07 00 00 84 18 00 00 02 00 00 00  |(.y...|.....
00000100 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00  .....
    
```



# AddressBook

- The Addressbook not only keeps records of a contact's name and address information, its framework can be called by **SMS** and **E-Mail** and also by custom third party applications.
- <http://developer.apple.com/iphone/program/>

**McAfee**

10/9/2008



Protect what you value.

# AddressBook access

- Possible to have direct access to the addressbook, so without having a need to build a gui to interact with the user.
- It is possible to read but also write directly to addressbook records: [Add/Replace/Remove](#)
- Very powerful functionality and could – in theory – open the door for direct actions performed by adware/malware

**McAfee**

10/9/2008



Protect what you value.



# AddressBook - Personal Information Properties

- const ABPropertyID kABPersonFirstNameProperty;
- const ABPropertyID kABPersonLastNameProperty;
- const ABPropertyID kABPersonMiddleNameProperty;
- const ABPropertyID kABPersonPrefixProperty;
- const ABPropertyID kABPersonSuffixProperty;
- const ABPropertyID kABPersonNicknameProperty;
- const ABPropertyID kABPersonFirstNamePhoneticProperty;
- const ABPropertyID kABPersonLastNamePhoneticProperty;
- const ABPropertyID kABPersonMiddleNamePhoneticProperty;
- const ABPropertyID kABPersonOrganizationProperty;
- const ABPropertyID kABPersonJobTitleProperty;
- const ABPropertyID kABPersonDepartmentProperty;
- const ABPropertyID kABPersonEmailProperty;
- const ABPropertyID kABPersonBirthdayProperty;
- const ABPropertyID kABPersonNoteProperty;
- const ABPropertyID kABPersonCreationDateProperty;
- const ABPropertyID kABPersonModificationDateProperty;

The McAfee logo is displayed in a bold, red, sans-serif font on a black background.

10/9/2008



Protect what you value.

# AddressBook - Getting Personal Information

```
//-----
NSString* name = (NSString *)ABRecordCopyValue(person, kABPersonFirstNameProperty);
self.firstName.text = name;
[name release];

//-----

name = (NSString *)ABRecordCopyValue(person, kABPersonLastNameProperty);
self.lastName.text = name;
[name release];

//-----

NSString* comp = (NSString *)ABRecordCopyValue(person, kABPersonOrganizationProperty);
self.companyname.text = comp;
[comp release];

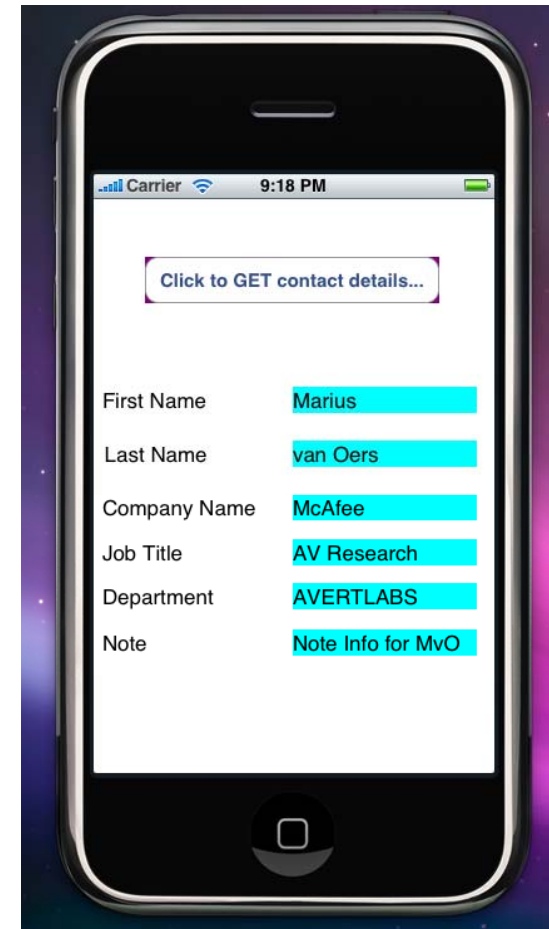
//-----

NSString* job = (NSString *)ABRecordCopyValue(person, kABPersonJobTitleProperty);
self.jobtitle.text = job;
[job release];

//-----

NSString* dep = (NSString *)ABRecordCopyValue(person, kABPersonDepartmentProperty);
self.department.text = dep;
[dep release];

//-----
```



**McAfee**

10/9/2008



Protect what you value.

## AddressBook - Phone Number Property

- const ABPropertyID kABPersonPhoneProperty;
  - const CFStringRef kABPersonPhoneMobileLabel;
  - const CFStringRef kABPersonPhoneMainLabel;
  - const CFStringRef kABPersonPhoneHomeFAXLabel;
  - const CFStringRef kABPersonPhoneWorkFAXLabel;
  - const CFStringRef kABPersonPhonePagerLabel;
- 
- ABMultiValueAddValueAndLabel(multi, @"123-456-1000", kABPersonPhoneMobileLabel)
  - ABMultiValueAddValueAndLabel(multi, @"123-456-1001", kABPersonPhoneMainLabel)

The McAfee logo is displayed in a bold, red, sans-serif font on a black background.

10/9/2008



Protect what you value.

# AddressBook - Instant Message Property

- `const ABPropertyID kABPersonInstantMessageProperty;`
- `const CFStringRef kABPersonInstantMessageServiceKey;`
- `const CFStringRef kABPersonInstantMessageServiceYahoo;`
- `const CFStringRef kABPersonInstantMessageServiceJabber;`
- `const CFStringRef kABPersonInstantMessageServiceMSN;`
- `const CFStringRef kABPersonInstantMessageServiceICQ;`
- `const CFStringRef kABPersonInstantMessageServiceAIM;`
- `const CFStringRef kABPersonInstantMessageUsernameKey;`

**McAfee**

10/9/2008



Protect what you value.

## AddressBook - URL Property

- const ABPropertyID kABPersonURLProperty;
- const CFStringRef kABPersonHomePageLabel;

**McAfee**

10/9/2008



Protect what you value.

# Problems

- Build\Debug-iphoneos\ .app ,didn't execute on “computer”, not supported on this architecture
- API's might not be equal OSX “computers” vs iPhone devices

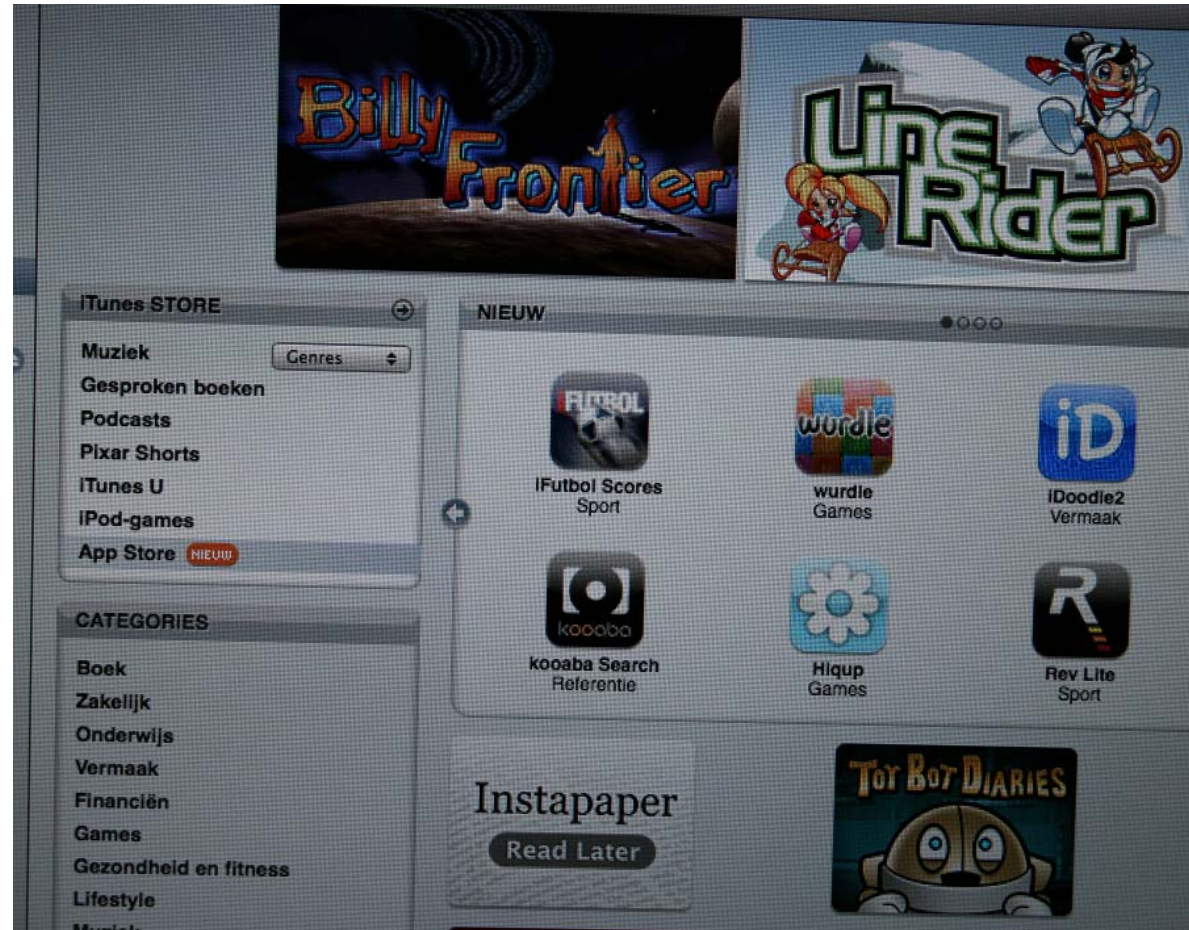
**McAfee**

10/9/2008



Protect what you value.

# iTunes App Store



**McAfee**

10/9/2008



Protect what you value.

# Conclusion

- Third party applications can directly access the Addressbook
- Create or Change the contact information
- Retrieving E-mail addresses & Telephone numbers might be abused

**McAfee**

10/9/2008



Protect what you value.



Thanks for attention !

# Questions?

E-mail: [marius\\_van\\_oers@avertlabs.com](mailto:marius_van_oers@avertlabs.com)

**McAfee**

10/9/2008



Protect what you value.