Attacking iOS Applications

iOS Uygulamaları Hedef Tahtasında

Sertan Kolat

Ajanda

- iOS İşletim Sistemi
- Donanım ve Mimari Bilgisi
- iOS Güvenlik Özellikleri
- iOS Uygulamaları ve Bileşenleri
- iOS Uygulama Denetimi Araç Kiti
- Kapalı Kutu Testleri
  - Statik Analiz
  - Dinamik Analiz
- Açık Kutu Testleri

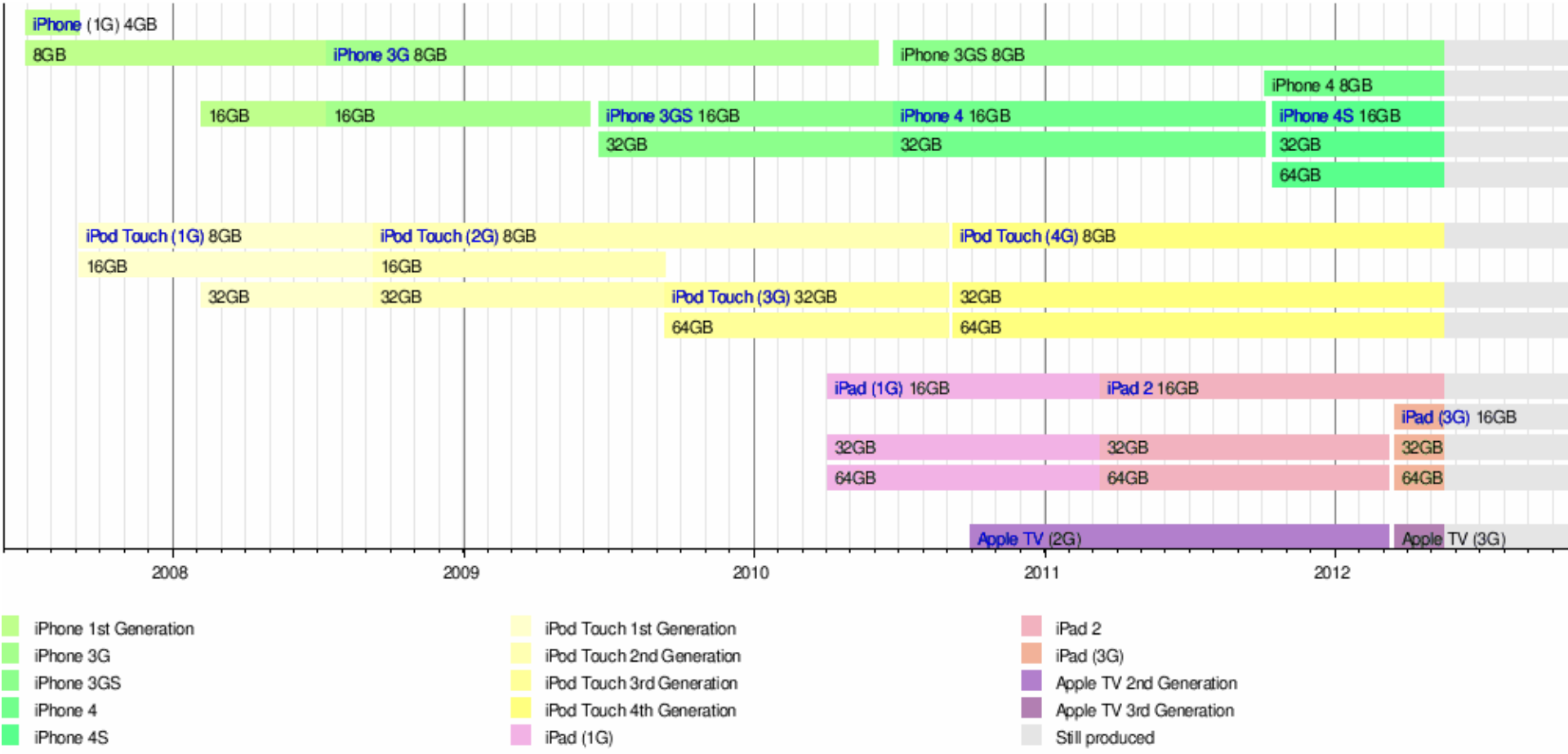
id

- Sertan Kolat
- Security Beast
- Avanteg – Güvenlik Denetimi & Servisler Yöneticisi
- Güvenlik TV – Yapımcı ve Sunucu
- CISSP, CISA, OSCP
- Blogger
  - SertanKolat.com
  - AutomatedScanning.blogspot.com

iOS İşletim Sistemi

- iPhone OS -> iOS != Cisco IOS
- OS X'ten türetilme
- iPhone, iPod touch, iPad, Apple TV
- Sadece Apple donanımlarında kullanılıyor

iOS Kullanan Donanımlar



** http://en.wikipedia.org/wiki/IOS*

Donanım Mimarisi

İşlemci	Mimari Jenerasyonu	Kullanılan Cihaz
ARM7TDMI	ARMv4	iPod
ARM9E	ARMv5	Airport Extreme N basestation
ARM 1176JZ(F)-S	ARMv6	iPhone, iPhone 3G, iPod touch
ARM Cortex-A8	ARMv7	iPhone 3GS
Apple A4 (ARM Cortex-A8 CPU + PowerVR GPU)	ARMv7	iPad, iPhone 4, iPod touch (4th gen), Apple TV (2nd gen)
Apple A5 (dual-core ARM Cortex-A9 MPCore CPU, NEON SIMD accelerator + dual core PowerVR SGX543MP2 GPU)	ARMv7	iPad 2, iPhone 4S, Apple TV (3rd gen)
Apple A5X (dual-core CPU + quad-core PowerVR SGX543MP4 GPU)	ARMv7	iPad 3

Donanım Mimarisi

İşlemci	Mimari Jenerasyonu	Kullanılan Cihaz
ARM7TDMI	ARMv4	iPod
ARM9E	ARMv5	Airport Extreme N basestation
ARM 1176JZ(F)-S	ARMv6	iPhone, iPhone 3G, iPod touch
ARM Cortex-A8	ARMv7	iPhone 3GS
Apple A4 (ARM Cortex-A8 CPU + PowerVR GPU)	ARMv7	iPad, iPhone 4, iPod touch (4th gen), Apple TV (2nd gen)
Apple A5 (dual-core ARM Cortex-A9 MPCore CPU, NEON SIMD accelerator + dual core PowerVR SGX543MP2 GPU)	ARMv7	iPad 2, iPhone 4S, Apple TV (3rd gen)
Apple A5X (dual-core CPU + quad-core PowerVR SGX543MP4 GPU)	ARMv7	iPad 3

iOS Güvenlik Özellikleri

- Code Signing
- Stack canaries
- Nonexecutable memory
- ASLR (full ASLR için uygulama PIE desteği ile derlenmeli)
- Sandboxing
- Data at rest encryption

* Apple IOS 4 Security Evaluation - http://www.trailofbits.com/resources/ios4_security_evaluation_slides.pdf

iOS Uygulamaları

- 550.000'in üzerinde iOS uygulaması, toplamda 25 milyarın üzerinde indirilmiş
- Xcode IDE kullanılarak geliştiriliyor
- Objective C geliştirme dili
  - Bir çok geliştiricinin Java veya C# geçmişi var
  - iOS uygulama geliştiricilerinin bir çoğu C kökenli olmadığından, C 'de yapılan hatalardan bir haber
  - Özetle her yeni platformda eski hatalar yapılıyor
  - Ancak Apple tarafından sağlanan kütüphanelerin kullanımı ve iOS güvenlik önlemleri, geliştirici hatasıyla oluşabilecek problemleri engelliyor(?)
- Tipik bir iOS uygulaması
  - Kullanıcının cihazında kurulu
  - Kullanıcıyla etkileşim,
  - Uygulama sunucusu ve/veya Internet'le iletişim içerisinde

Uygulamanın Cihaza Kurulması

- IPA paket formatı (iOS Package Format)
  - Sıkıştırılmış ZIP arşivi
  - Paket İçeriği
    - iTunesArtwork
    - iTunesMetadata.plist
    - Payload/
      - Uygulama.App/
        - SC_Info/
        - Info.plist
        - ...

```
pop-pop-ret:Mobile Applications warex$ file WhatsApp\ 2.6.10.ipa
WhatsApp 2.6.10.ipa: Zip archive data, at least v1.0 to extract
pop-pop-ret:Mobile Applications warex$
```

Uygulamalar nereye kuruluyor?

- Klasör yapısı ve dosyalar
  - Kullanıcı klasörü /private/var/mobile (/User, /var/mobile alias)
  - Varsayılan uygulamalar /Applications altında
  - Kullanıcı tarafından kurulan uygulamalar /User/Applications içerisine kuruluyor
  - Uygulama klasörü /User/Applications/<app GUID>/<appname.app>

iOS Uygulama Denetimi

- Kapalı kutu testleri (Blackbox testing)
  - Statik Analiz
  - Dinamik Analiz
- Açık kutu testleri (Whitebox testing)
  - Kaynak Kodu Analizi

iOS Uygulama Denetimi Araç Kiti

- Jailbreak'li cihaz
- otool, nm
- plutil
- sqlite3 veya favori SQLite görüntüleyici
- class-dump, class-dump-z
- cycript
- GNU Debugger
- Hex editor
- Favori intercepting proxy yazılımınız
- Xcode

KAPALI KUTU TESTLERİ

Dosya Analizi

- Uygulama nerede kurulu?
  find /User/Applications –iname <AppName>
  /User/Applications/<App GUID>/AppName.app/AppName

```
Padawan:~ root# find /User/Applications -iname evernote
/User/Applications/DF1D2C39-5675-48B6-A7C1-308759D2173C/Evernote.app/Evernote
Padawan:~ root# cd /User/Applications/DF1D2C39-5675-48B6-A7C1-308759D2173C
Padawan:/User/Applications/DF1D2C39-5675-48B6-A7C1-308759D2173C root# ls
Documents/  Evernote.app/  Library/  iTunesArtwork  iTunesMetadata.plist  tmp/
```

- AppName.app/ klasörü uygulamanın kendisi ve çalışması için gereken bileşenler
- Ek olarak Documents/ ve Library/Preferences/ dizinlerindeki dosyalar mutlaka incelenmeli
- Diğer dizinlerdeki cache dosyaları incelenebilir

Dosya Analizi II: Ayarlar ve Program Verileri

- Ayarlar ve program verilerinin saklandığı dosyalar
  - SQLite Veritabanı
    - sqlite3 komutu veya çeşitli SQLite görüntüleyicileri
    - sqlite> .tables (veritabanındaki tabloları listele)
    - sqlite> select * from tablo;
    - …
  - Property Lists (plist)
    - Property list utility, plutil
    - plutil –show dosya.plist (İçeriğini görüntüle)
    - plutil –convert xml1 dosya.plist (XML formatına çevir)
    - …
- Diğer dosyalar
  - "file *" komutuyla klasördeki dosya tipleri görülebilir

Dosya Analizi II: Ayarlar ve Program Verileri

warex — ssh — 147×29

```
AdvancedSearchButton.png:                    PNG image data, 805314562 x 284378236, 0-bit grayscale,
CodeResources:                               symbolic link to `_CodeSignature/CodeResources'
Default-Landscape.png:                       PNG image data, 805314566 x 396263525, 0-bit grayscale,
Default-Portrait.png:                        PNG image data, 805314566 x 396263525, 0-bit grayscale,
Default.png:                                 PNG image data, 805314566 x 396263525, 0-bit grayscale,
Default@2x.png:                              PNG image data, 805314566 x 396263525, 0-bit grayscale,
ENCaptchaViewController.nib:                 data
ENNativeRegistrationController.nib:          data
ENNoteEditor.css:                            ASCII C program text
ENNoteEditor.js:                             ASCII text, with very long lines
ENNotebookSharingViewController.nib:         data
ENPadAudioRecorder.nib:                      data
ENPadPasscodeBackgroundViewController.nib:   data
ENPadWelcomeScreenController.nib:            data
ENPhoneWelcomeScreenViewController.nib:      data
ENPremiumCommerceViewController.nib:         data
ENResetPasswordViewController.nib:           data
ENSanitizer.js:                              ASCII text, with very long lines
ENSignInViewController.nib:                  data
ENSplashScreenViewController.nib:            data
English.lproj:                               directory
Entitlements-Beta.plist:                     Apple binary property list
Entitlements-Enterprise.plist:               Apple binary property list
Entitlements.plist:                          Apple binary property list
Evernote:                                    Mach-O fat file with 2 architectures
FBDialog.bundle:                             directory
French.lproj:                                directory
FullScreenWebView.nib:                       data
--More--(byte 1995)
```

Dosya Analizi II: Ayarlar ve Program Verileri

- Neler bulunabilir?
  - Uygulama bileşenlerini daha iyi anlama
  - Uygulamaya ait özel veritabanları, bilgiler
  - Uygulamaya gömülü şifreler vb.
  - Kullanıcılara ait hassas bilgiler

```
# pwd
/User/Applications/4[redacted]B/Documents
# plutil *Options
(
    "sertan@gmail.com",
    [redacted],
    1,
    0
)
# 
# plutil *plist |grep -i user
    userName = warex;
    userPass = "[redacted]";
    userRealName = "Sertan Kolat";
# 
```

Şifre

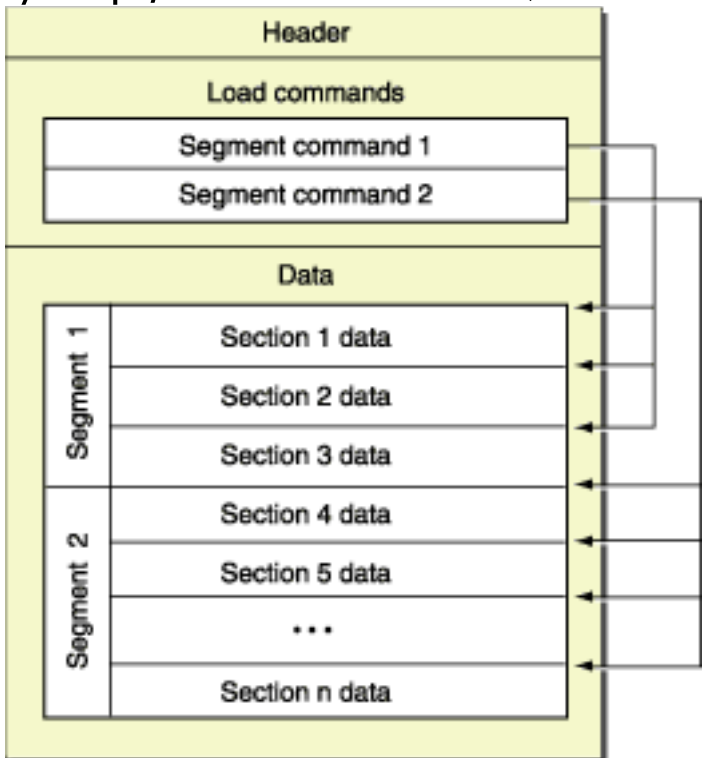
Dosya Analizi III: Binary Dosyalar

- Fat binary

```
Padawan:~ root# otool -f /Applications/Camera.app/Camera
Padawan:~ root# otool -f /User/Applications/DF1D2C39-5675-48B6-A7C1-308759D2173C/Evernote.app/Evernote
Fat headers
fat_magic 0xcafebabe
nfat_arch 2
architecture 0
    cputype 12
    cpusubtype 9
    capabilities 0x0
    offset 4096
    size 5760880
    align 2^12 (4096)
architecture 1
    cputype 12
    cpusubtype 6
    capabilities 0x0
    offset 5767168
    size 5708064
    align 2^12 (4096)
```

Dosya Analizi III: Binary Dosyalar

- Mach-O (Mach object) dosya formatı (Standart OS X program ve kütüphaneleri)
  - Temel olarak 3 ana bölümü bulunuyor
    - Header structure (dosya tipi, hedef mimari vs)
    - Load commands
    - Data

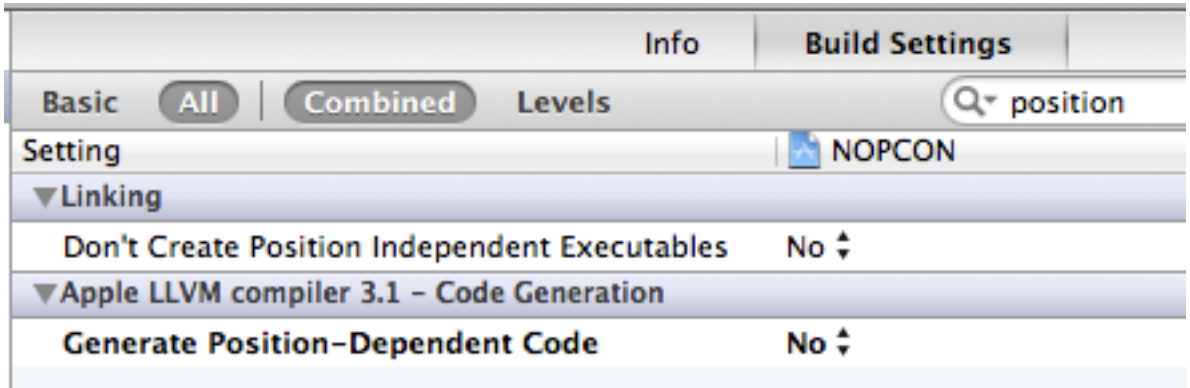


http://bit.ly/mach-o

Dosya Analizi III: Binary Dosyalar

- Full ASLR desteği var mı?

```
Padawan:~ root# otool -vh /Applications/Camera.app/Camera
/Applications/Camera.app/Camera:
Mach header
      magic cputype cpusubtype  caps    filetype ncmds sizeofcmds      flags
   MH_MAGIC     ARM          9  0x00     EXECUTE    34       3756  NOUNDEFS DYLDLINK TWOLEVEL PIE
Padawan:~ root# otool -vh /User/Applications/DF1D2C39-5675-48B6-A7C1-308759D2173C/Evernote.app/Evernote
/User/Applications/DF1D2C39-5675-48B6-A7C1-308759D2173C/Evernote.app/Evernote:
Mach header
      magic cputype cpusubtype  caps    filetype ncmds sizeofcmds      flags
   MH_MAGIC     ARM          9  0x00     EXECUTE    45       5080  NOUNDEFS DYLDLINK TWOLEVEL
Padawan:~ root# otool -arch armv6 -vh /User/Applications/DF1D2C39-5675-48B6-A7C1-308759D2173C/Evernote.app/Evernote
/User/Applications/DF1D2C39-5675-48B6-A7C1-308759D2173C/Evernote.app/Evernote:
Mach header
      magic cputype cpusubtype  caps    filetype ncmds sizeofcmds      flags
   MH_MAGIC     ARM         V6  0x00     EXECUTE    45       5080  NOUNDEFS DYLDLINK TWOLEVEL
```



Dosya Analizi III: Binary Dosyalar

- Şifrelenmiş Binary'ler
  - İndirilen uygulamalar şifrelenmiş olduğu için, nm, class-dump-z gibi uygulamalarla analizi mümkün olmuyor. Çözüm? Şifrelemeyi iptal etme
  - Araç kiti:
    - Jailbroken device
    - otool
    - GNU Debugger
    - dd
    - Hex Editor

Dosya Analizi III: Binary Dosyalar

```
/**
 * This header is generated by class-dump-z 0.2a.
 * class-dump-z is Copyright (C) 2009 by KennyTM~, licensed under GPLv3.
 *
 * Source: (null)
 */

@protocol XXEncryptedProtocol_52eb94 <XXEncryptedProtocol_52ebbc, XXEncryptedProtocol_52ebe4>
@property(assign) ? XXEncryptedProperty_459b60;
@property(assign) ? XXEncryptedProperty_4592de;
@property(assign) ? XXEncryptedProperty_42b49f;
@property(assign) ? XXEncryptedProperty_42b47f;
@property(assign) ? XXEncryptedProperty_42b45f;
@property(assign) ? XXEncryptedProperty_42b43d;
-(?)XXEncryptedMethod_3e7e53;
-(?)XXEncryptedMethod_3e79d2;
-(?)XXEncryptedMethod_3e7e37;
-(?)XXEncryptedMethod_3e7a29;
-(?)XXEncryptedMethod_3e77ba;
-(?)XXEncryptedMethod_3e7e14;
-(?)XXEncryptedMethod_3e7b45;
-(?)XXEncryptedMethod_3e7bea;
-(?)XXEncryptedMethod_3e7e0a;
-(?)XXEncryptedMethod_3e7bd4;
-(?)XXEncryptedMethod_3e7e00;
-(?)XXEncryptedMethod_3e7b33;
-(?)XXEncryptedMethod_3e7bba;
-(?)XXEncryptedMethod_3e7b3c;
-(?)XXEncryptedMethod_3e7bc7;
@end
```

Dosya Analizi III: Binary Dosyalar

- Deşifre edilmiş uygulama

```
# otool -l MyApplication |grep cry
 cryptoff  4096
 cryptsize 520192
 cryptid   0
```

Dosya Analizi III: Binary Dosyalar

```
/**
 * This header is generated by class-dump-z 0.2a.
 * class-dump-z is Copyright (C) 2009 by KennyTM~, licensed under GPLv3.
 *
 * Source: (null)
 */

typedef struct _NSZone NSZone;

typedef struct CGPoint {
        float x;
        float y;
} CGPoint;

typedef struct CGSize {
        float _field1;
        float _field2;
} CGSize;

typedef struct CGRect {
        CGPoint _field1;
        CGSize _field2;
} CGRect;

typedef struct _NSRange {
        unsigned _field1;
        unsigned _field2;
} NSRange;
```

Dinamik Analiz

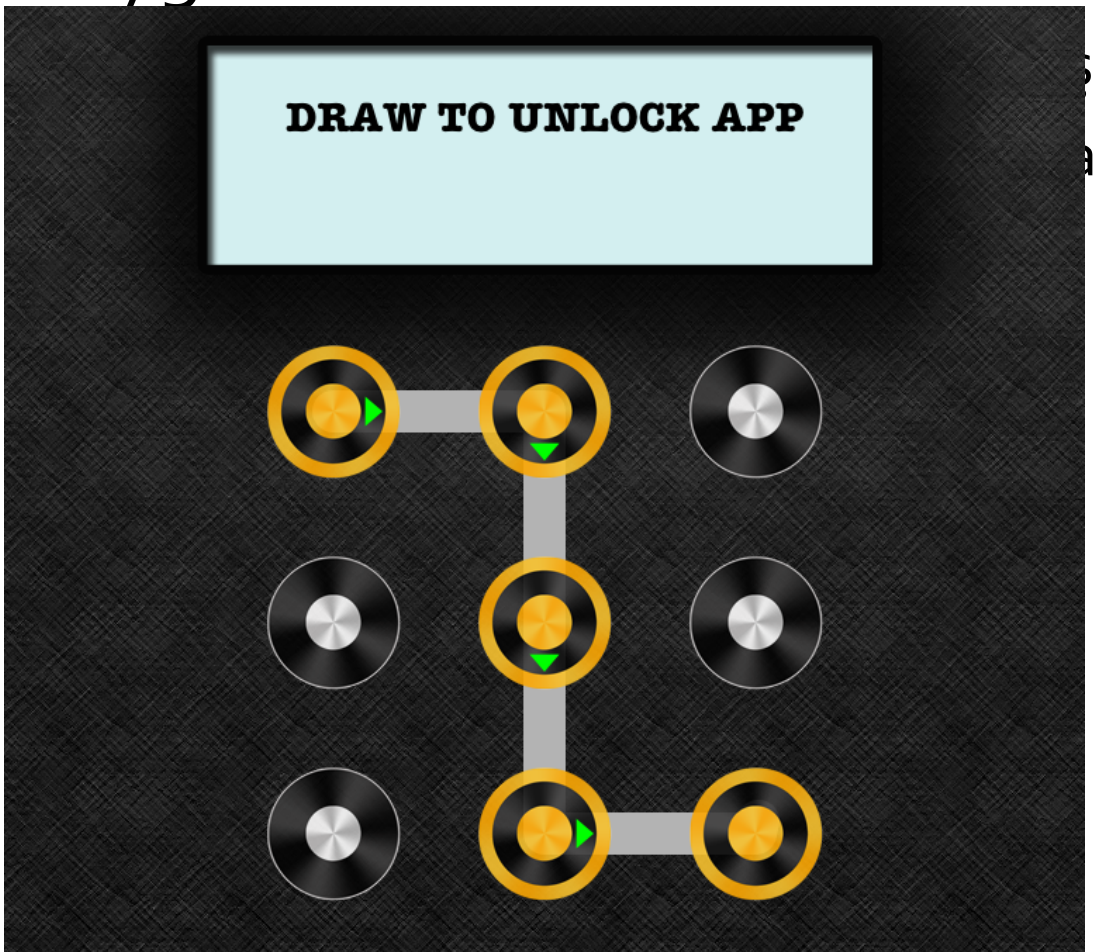
- GNU Debugger ile çalışan uygulama analizi
- otool (-tv, -tV) veya IDA Pro ile disassemble
- Uygulamaya gömülü şifreler, anahtarlar var mı?
- Kötü niyetli aktivite yapan kod bulunuyor mu?
- Cycript ile runtime manipulasyonu
  - Çalışan uygulamaya attach edip, mevcut metodlar değiştirilebilir, varolan metodlar çağırılabilir

Dinamik Analiz: Cycript ile Runtime Manipülasyonu

- Hedef Uygulama: **Dot Lock Photo**
  - Özel fotoğraflarınızı belirlediğiniz pattern ile şifreliyor
  - Doğru pattern girildiğinde gizli albümlerinizi açıyor

Dinamik Analiz: Cycript ile Runtime Manipülasyonu

- Hedef Uygulama: **Dot Lock Photo**
  - Öze şifreliyor
  - Doğ açıyor



Dinamik Analiz: Cycript ile Runtime Manipülasyonu

- Hedef Uygulama: **Dot Lock Photo**

(Deşifre edilmiş binary için class-dump-z çıktısından bir bölüm)

```
@interface SecurePhotoAppDelegate : NSObject <UIApplicationDelegate,
DotLockPasscodeViewControllerDelegate> {
        int wrongAttempt;
        int runMode;
        int loginPasscodeType;
… (kesilmiştir)
-(BOOL)doSaveNewPasscode:(unsigned)passcode;
-(BOOL)doCancelPasscode;
-(BOOL)isCorrectOldPasscode:(unsigned)passcode;
-(void)initNormalWindow;
-(void)initDecoyWindow;
```

Dinamik Analiz: Cycript ile Runtime Manipülasyonu

- Hedef Uygulama: **Dot Lock Photo**

```
# ps -ef |grep -i dotlock |grep -v grep
501  1674     1   0   0:00.95 ??         0:03.42 /var/mobile/
Applications/5B27EAD5-9646-48EA-99FB-1C2701349765/
SecureDotLockPhotoLite.app/SecureDotLockPhotoLite

# cycript -p 1674
cy#
cy# var app = [ UIApplication sharedApplication ]
"<UIApplication: 0x1a64d0>"

cy# [ app.delegate doCancelPasscode ]
1
cy#
```

Dinamik Analiz: Cycript ile Runtime Manipülasyonu

Bu bölümdeki video'lu, anlatım sunumdan çıkartılmıştır

Dinamik Analiz: Ağ Trafiği İzleme ve Manipülasyon

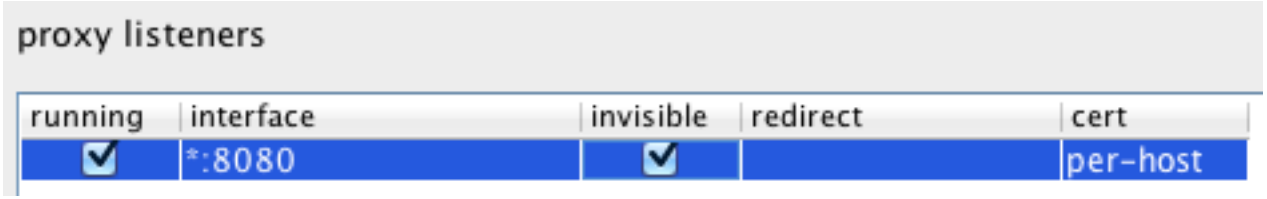
- Uygulama özel verileri dışarıya gönderiyor mu?
- İzinsiz gizlilik ihlali var mı?
- Değiştirilen paketler uygulama ve uygulama sunucusu tarafında ne gibi problemler yaratıyor?
- Veriler güvenli kanallar üzerinden mi gönderiliyor?
- Uygulamaya hizmet veren servislerin kontrolü
  - Test edilen uygulamaların çoğu web servisi ile haberleşiyor
  - Klasik web uygulamalarında yapılan hatalara devam… kullanıcı verileri değiştiremez zannedildiğinden daha az önemseniyor
  - Web sunucularında unutulmuş geçici dosyalar çoğunlukta
  - Uygulamalar mantıksal saldırılara, veya diğer kullanıcının yerine geçme durumlarına açık

Dinamik Analiz: Ağ Trafiği İzleme ve Manipülasyon

- Wireshark, tcpdump vb sniffer ile trafik analizi
- Driftnet: TCP bağlantılarından imaj ayıklama http://www.ex-parrot.com/~chris/driftnet/
- Burp Suite HTTP/S intercepting proxy yazılımı http://portswigger.net/burp/
- Canape gibi hazır veya özel yazılmış protokol spesifik proxy yazılımları ile paket değiştirme http://www.contextis.com/research/tools/canape/

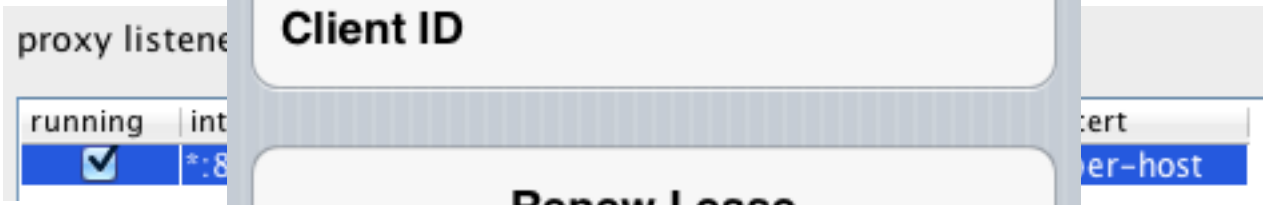
Dinamik Analiz: Ağ Trafiği İzleme ve Manipülasyon

- Burp Suite ve cihaz proxy ayarları



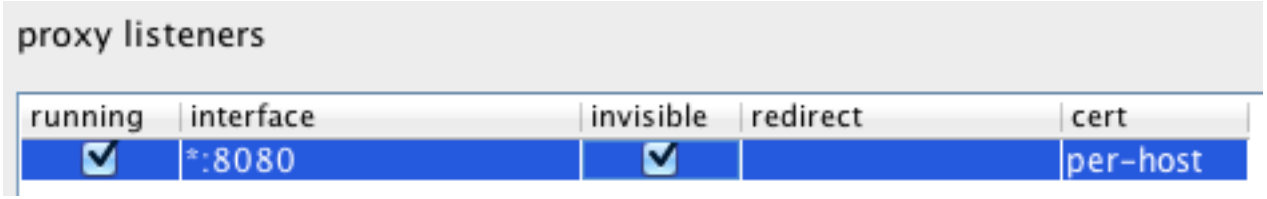
Dinamik Analiz:
Ağ Trafiği İzleme ve Manipülasyon

- Burp Suit



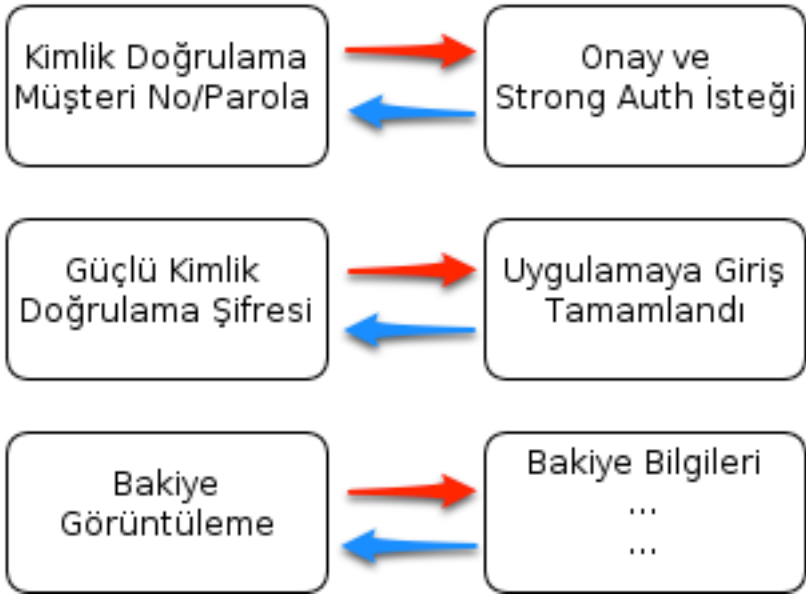
Dinamik Analiz: Ağ Trafiği İzleme ve Manipülasyon

- Burp Suite ve cihaz proxy ayarları



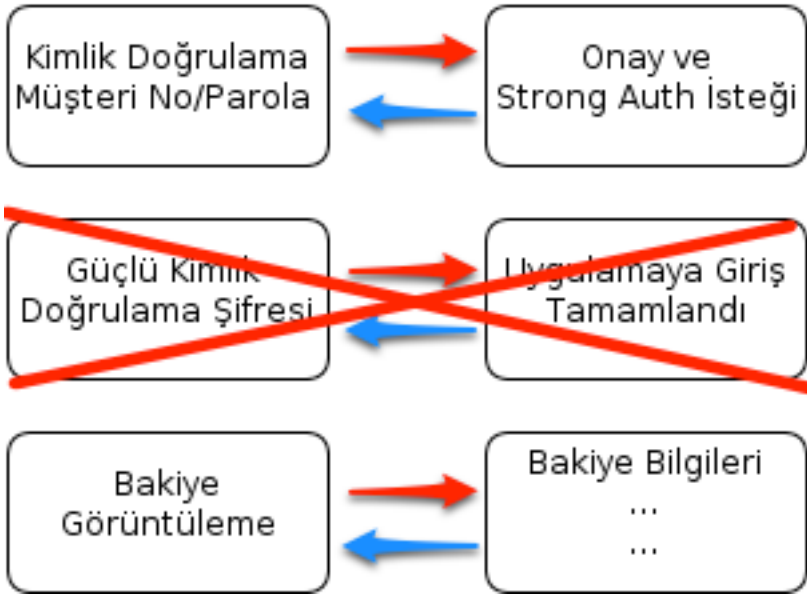
Dinamik Analiz: Ağ Trafiği İzleme ve Manipülasyon

- Mantıksal Saldırılar



Dinamik Analiz: Ağ Trafiği İzleme ve Manipülasyon

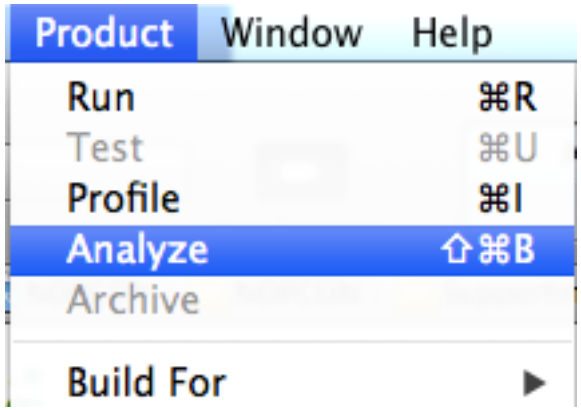
- Mantıksal Saldırılar



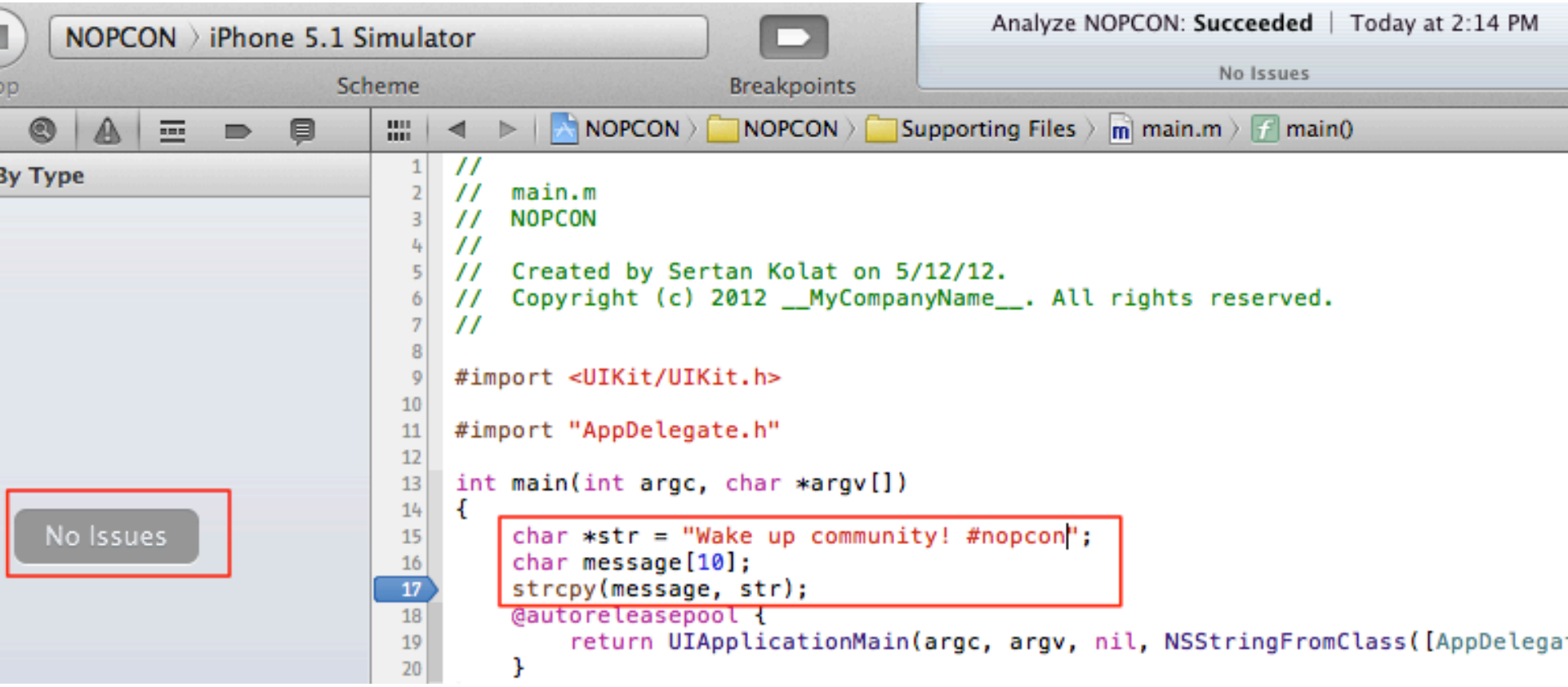
AÇIK KUTU TESTLERİ

Kaynak Kodu Analizi

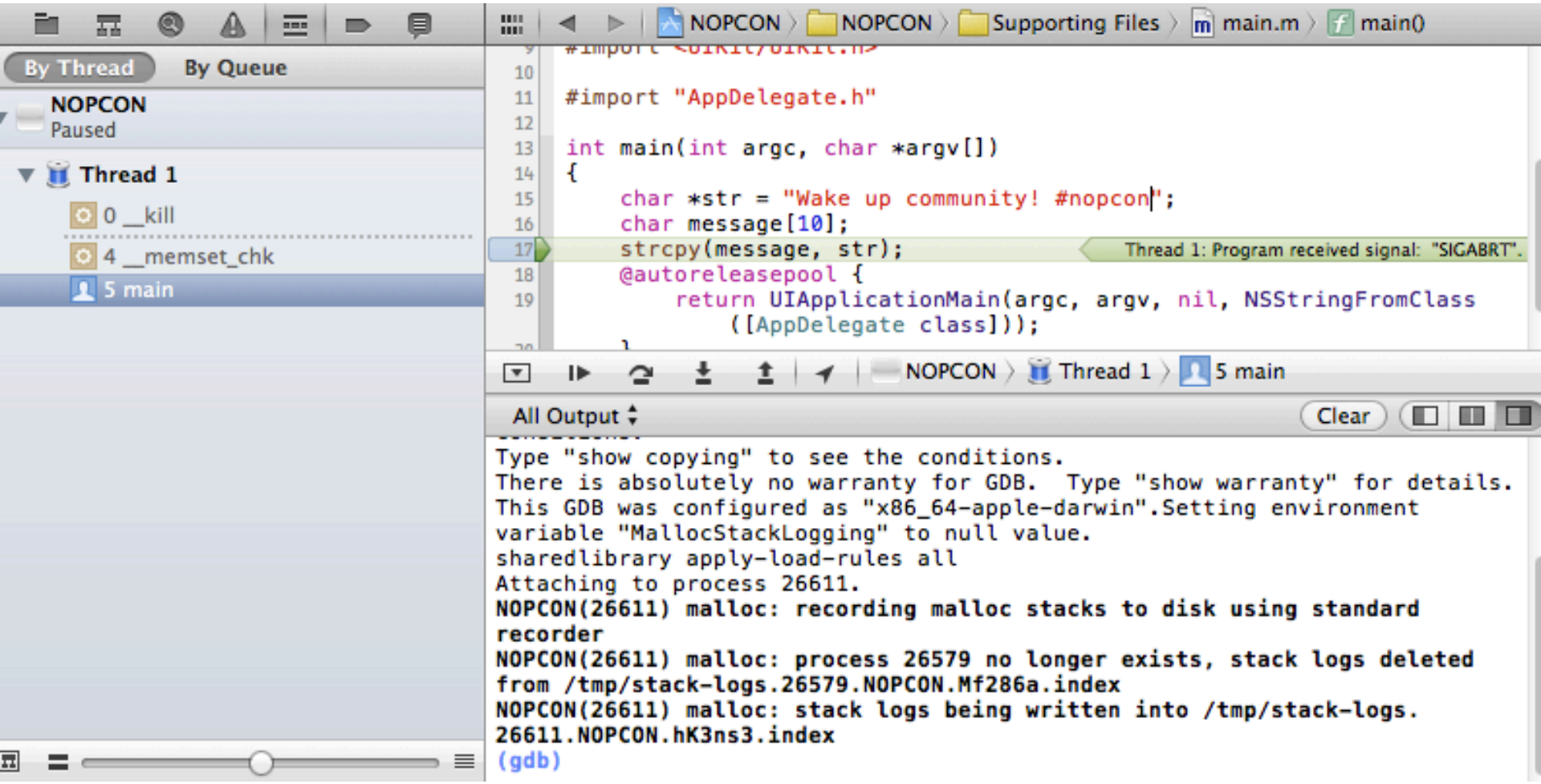
- Statik analiz yazılımlarının iOS uygulama desteği henüz yok
- Kaynak kodunun birebir incelenmesi (manuel)
- Xcode IDE içerisinde bulunan static analyzer kullanılabilir (Clang Analyzer)
  http://bit.ly/xcode-static



Kaynak Kodu Analizi



Kaynak Kodu Analizi



Teşekkürler!

İletişim
Sertan Kolat
sertan@gmail.com
sertankolat.com
twitter: @warex