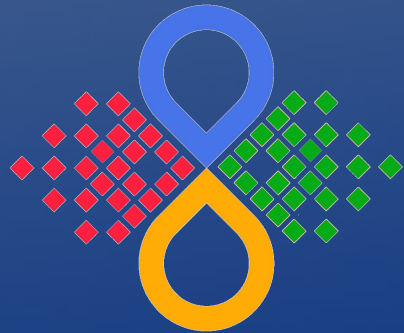


# Mobil Uygulamalarda Gvenlik Denetimi

Nebi Őenol YILMAZ  
DanıŐman / Ynetici Ortak  
senol.yilmaz@secrove.com



Secrove Information Security Consulting

# Ajanda

- Hakkımızda
- Mobil Dünya
- Güvenlik İhtiyacı
- Uygulama Denetimi
- Örnek Uygulama



# Hakkımızda

- Nebi Şenol YILMAZ, CISA, C|EH, ISO 27001 LA
- Secrove Information Security Consulting
  - Bilgi Güvenliği Danışmanlığı
  - Zafiyet Araştırmaları
  - Bilgi Güvenliği Eğitimleri
  - Siber İstihbarat Çalışmaları



# Mobil Dünya

- Gözümüz
- Kulağımız
- Dilimiz

haline geldi...



# Mobil Dünya



İşimiz artık parmaklarımızın ucunda, ya da ....



# Mobil Dünya



Avucumuzun içinde ....



# Mobil Dünya

:)



ve bütün hizmetler önümüze geliyor ....



# Güvenlik İhtiyacı





# Güvenlik İhtiyacı



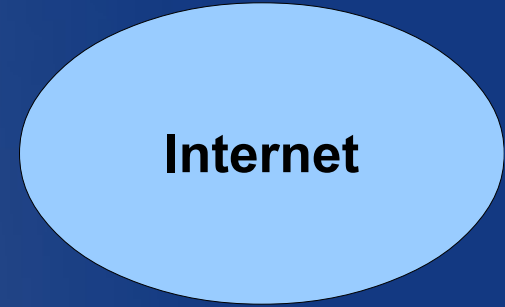
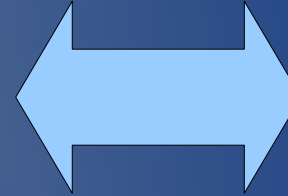
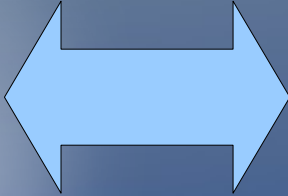
# Uygulama Denetimi

- Ağ Üzerinde Denetim
- Statik Kod Analizi
- Dinamik Analiz



# Uygulama Denetimi

- Ağ Üzerinde Denetim



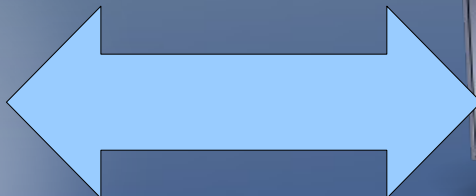
# Uygulama Denetimi

- Ağ Üzerinde Denetim
  - Veriler açık olarak mı iletiliyor?
  - Gizli veri sızdırma mevcut mu?
  - Veriler manipüle edilebiliyor mu?
  - Manipülasyon sunucu tarafında zafiyet oluşturuyor mu?



# Uygulama Denetimi

- Statik Kod Analizi



# Uygulama Denetimi

- Statik Kod Analizi
  - Otomatik aralar ile kod analizi
  - Uzman insan kaynađı ile kod analizi



# Uygulama Denetimi

- Dinamik Analiz



# Uygulama Denetimi

- Dinamik Analiz
  - Uygulamanın çalışması sırasında manipülasyon yapmamızı sağlar.
- Client-side kontrollerin hepsi by-pass edilebilir.
- Gizlenmiş fonksiyonların çağrılması sağlanabilir.
- Gizlenmiş veriler dump olarak alınabilir.





# Uygulama Denetimi

- Dinamik Analiz
  - Debugger (gdb)
  - Otool
  - Class-dump-z
  - Snoop-it
  - Cycrypt



# Uygulama Denetimi

- Dinamik Analiz
  - Debugger (gdb)

```
(gdb) attach <PID>
Attaching to program: `'/private/var/mobile/Applications/...'`, process PID.
Reading symbols for shared libraries . done
Reading symbols for shared libraries ..... done
Reading symbols for shared libraries + done
0x364d7004 in mach_msg_trap ()
```



# Uygulama Denetimi

- Dinamik Analiz
  - otool

```
SecrovePhone:~ root# otool -o /Applications/Terminal.app/Terminal
/Applications/Terminal.app/Terminal:
Contents of (__DATA,__objc_classlist) section
0001edec 0x19818
    isa 0x19804
  superclass 0x0
    cache 0x0
  vtable 0x0
    data 0x1a6dc (struct class_ro_t *)
      flags 0x0
    instanceStart 4
    instanceSize 21
      ivarLayout 0x0
        name 0x132ac MobileTerminalAppDelegate
      baseMethods 0x1a5f4 (struct method_list_t *)
    entsize 12
```



# Uygulama Denetimi

- Dinamik Analiz
- class-dump-z

```
SecrovePhone:~/iphone_armv6 root# ./class-dump-z /System/Library/CoreServices/SpringBoard.app/SpringBoard

/**
 * This header is generated by class-dump-z 0.2-0.
 * class-dump-z is Copyright (C) 2009 by KennyTM~, licensed under GPLv3.
 *
 * Source: (null)
 */

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

typedef struct CGSize {
    float width;
    float height;
} CGSize;

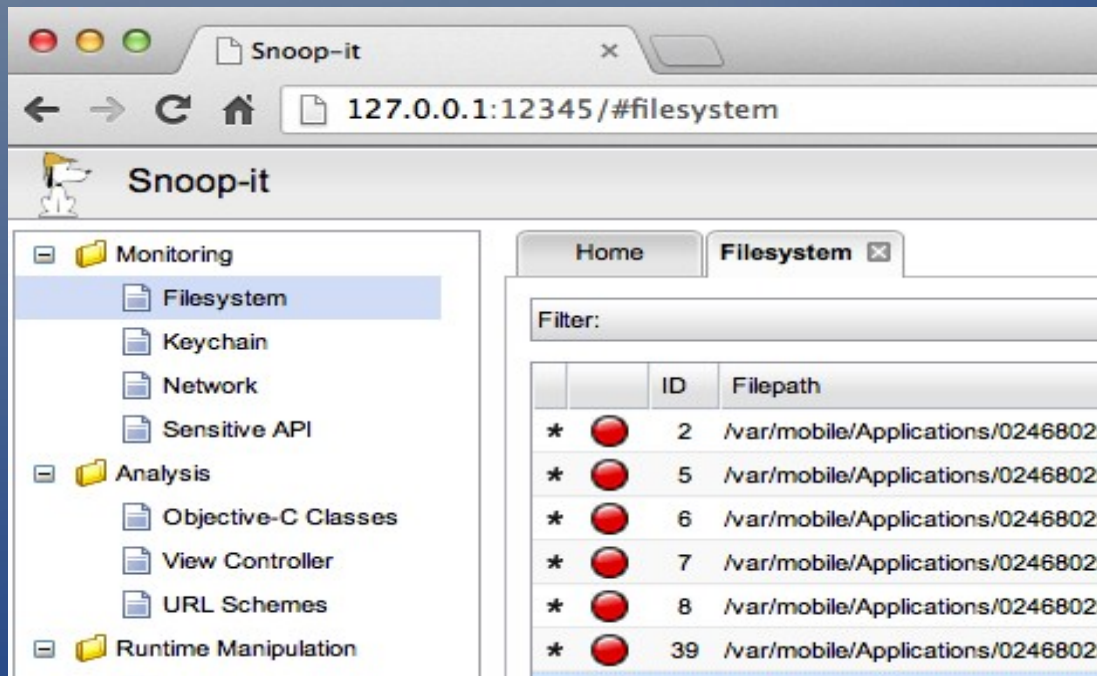
typedef struct CGRect {
    CGPoint origin;
    CGSize size;
} CGRect;

typedef struct _NSZone NSZone;
```



# Uygulama Denetimi

- Dinamik Analiz
  - Snoop-it



# Uygulama Denetimi

- Dinamik Analiz
- cycript

```
SecrovePhone:~/iphone_armv6 root# cycript -p 8599
cy# UI
Display all 714 possibilities? (y or n)
cy# UIApp
@"<UIApplication: 0x2899b0>"
cy# ?expand
expand == true
cy# UIApp.windows[0].recursiveDescription
@"<TTNavigatorWindow: 0x297cc0; baseClass = UIWindow; frame = (0 0; 320 480); layer = <UIWindowLayer:
| <UILayoutContainerView: 0x6622d0; frame = (0 0; 320 480); autoresize = W+H; layer = <CALayer: 0x6
| | <UINavigationController: 0x662640; frame = (0 0; 320 480); clipsToBounds = YES; autoresize
| | | <UIViewControllerWrapperView: 0x658860; frame = (0 84; 320 396); autoresize = W+H; laye
| | | | <UIView: 0x665b10; frame = (0 0; 320 396); autoresize = W+H; layer = <CALayer: 0x6
| | | | | <UITextField: 0x663880; frame = (10 130; 100 20); text = ''; clipsToBounds =
| | | | | | <UITextField: 0x12f8800; frame = (0 0; 100 20); text = ''; opaque = NO
| | | | | | | <TileHostLayer: 0x66b370> (layer)
| | | | | | | | <TileLayer: 0x685db0> (layer)
| | | | | | | <UITextSelectionView: 0x2a56d0; frame = (0 0; 0 0); userInteractionEnabled
| | | | | | | | <UIView: 0x2a77c0; frame = (0 0; 3 20); userInteractionEnabled = NO
| | | | | | | <UILabel: 0x665fd0; frame = (-300 33; 320 20); transform = [1, 0, 0, 1, -300,
onEnabled = NO; layer = <CALayer: 0x666070>>
| | | | | | | <UILabel: 0x666500; frame = (0 33; 320 20); text = 'Enter your passcode'; cl
x6664b0>>
| | | | | | | <UILabel: 0x664120; frame = (0 151; 320 20); text = 'Wrong Passcode. Try aga
CALayer: 0x663ed0>>
```



# Uygulama Denetimi

- Örnek Uygulama
  - Cycrypt
- Görsel özelliklerde işlem yapabiliriz
  - SpringBoard üzerinde işlemler gerçekleştirmek
- Fonksiyon özelliklerinde işlem yapabiliriz
  - PhotoVault uygulamasında authentication by-pass gerçekleştirmek



# Örnek Uygulama - cyscript

- İlk olarak jailbreak yapılmış telefonumuza:
    - Cyscript
    - Class-dump-z
- kurmalıyız.





# Örnek Uygulama - cyscript

- SSH ile telefona erişip, üzerinde işlem yapacağımız uygulamayı seçeceğiz:

```
SecrovePhone:~ root# ps -ef
UID      PID  PPID  C   STIME TTY          TIME CMD
0         1    0    0   0:00.00 ??        0:42.06 /sbin/launchd
0        19    1    0   0:00.00 ??        8:08.99 /usr/libexec/UserEventAgent -l System
0        21    1    0   0:00.00 ??        0:26.11 /usr/sbin/notifyd
0        23    1    0   0:00.00 ??        0:25.54 /usr/sbin/syslogd
0        25    1    0   0:00.00 ??        1:15.81 /usr/libexec/configd
501      27    1    0   0:00.00 ??        55:39.87 /System/Library/CoreServices/SpringBoard.app/SpringBoard
25       29    1    0   0:00.00 ??        10:46.54 /System/Library/Frameworks/CoreTelephony.framework/Support/CommCenter
0        39    1    0   0:00.00 ??        0:14.92 /usr/libexec/lockdown
0        45    1    0   0:00.00 ??        1:05.22 /System/Library/CoreServices/powerd.bundle/powerd
0        51    1    0   0:00.00 ??        13:37.22 /usr/libexec/locationd
0        55    1    0   0:00.00 ??        1:10.11 /usr/sbin/wifid
501      70    1    0   0:00.00 ??        5:58.69 /usr/sbin/mediaserverd
501      71    1    0   0:00.00 ??        0:02.24 /System/Library/PrivateFrameworks/MediaRemote.framework/Support/mediaremoted
65       72    1    0   0:00.00 ??        0:26.71 /usr/sbin/mDNSResponder -launchd
501      74    1    0   0:00.00 ??        1:17.99 /System/Library/PrivateFrameworks/IMCore.framework/imagent.app/imagent
501      75    1    0   0:00.00 ??        0:22.15 /System/Library/PrivateFrameworks/IAP.framework/Support/iapd
0        77    1    0   0:00.00 ??        0:07.73 /usr/libexec/fseventsd
501      78    1    0   0:00.00 ??        0:04.80 /usr/sbin/fairplayd.N94
501      79    1    0   0:00.00 ??        0:11.07 /System/Library/PrivateFrameworks/DataAccess.framework/Support/dataaccessd
501      86    1    0   0:00.00 ??        0:26.34 /System/Library/PrivateFrameworks/ApplePushService.framework/apsd
501      87    1    0   0:00.00 ??        0:53.24 /System/Library/PrivateFrameworks/AggregateDictionary.framework/Support/aggregated
501      92    1    0   0:00.00 ??        0:11.11 /usr/sbin/BTServer
0       147    1    0   0:00.00 ??        0:04.86 /usr/libexec/networkd
501     1625    1    0   0:00.00 ??        0:24.88 /Applications/MobileMail.app/MobileMail
501     2009    1    0   0:00.00 ??        0:11.86 /var/mobile/Applications/11881D39-991C-4B49-BE10-CCBE91230982/LinkedIn.app/LinkedIn
501     2112    1    0   0:00.00 ??        0:33.06 /var/mobile/Applications/E140986E-33F3-491A-80D9-DCD5B81D0A4D/Foursquare.app/Foursquare
501     4000    1    0   0:00.00 ??        3:51.65 /Applications/MobileSafari.app/MobileSafari
501     4308    1    0   0:00.00 ??        0:11.88 /var/mobile/Applications/A4F3ED51-C752-4491-BBF4-3A4B2ACA069F/Twitter.app/Twitter
501     4543    1    0   0:00.00 ??        0:03.69 /usr/libexec/ptpd -t usb
0       4556    1    0   0:00.00 ??        0:00.43 sshd: nsyilmaz@ttys000
501     4577    1    0   0:00.00 ??        0:00.66 /Applications/MobilePhone.app/MobilePhone
0       4557  4556    0   0:00.00 ttys000  0:00.10 -sh
0       4591  4557    0   0:00.00 ttys000  0:00.01 ps -ef
SecrovePhone:~ root#
```



# Örnek Uygulama - cyscript

- Cyscript ile, işlem yapacağımız process'e attach olacağız:
- Ağaç yapısında uygulama window görsellerine erişeceğiz:

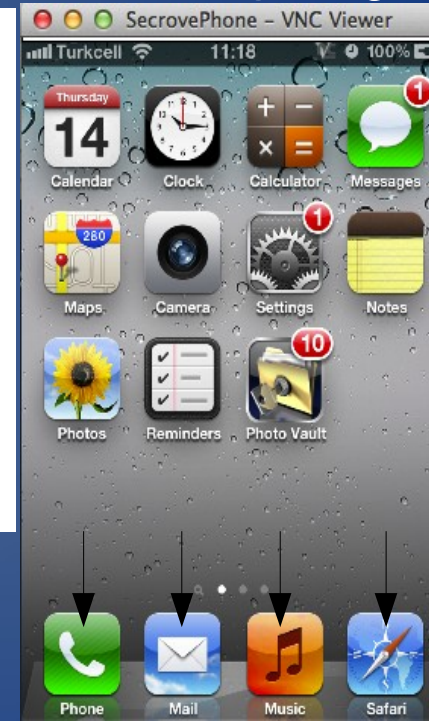
```
SecrovePhone:~ root# cyscript -p SpringBoard
cy# UIApp
@"<SpringBoard: 0xc6519e0>"
cy#
cy# ?expand
expand == true
cy#
cy#
cy# UIApp.windows [0] .recursiveDescription
@"<SBAppWindow: 0x4a0b60; baseClass = UIWindow; frame = (0 0; 320 480); layer = <UIWindowLayer: 0x49f410>>
  |<SBUIRootView: 0x4ac2d0; frame = (0 0; 320 480); alpha = 0; layer = <CALayer: 0x4ac370>>
  | |<UIView: 0x4ac4e0; frame = (0 0; 320 480); autoresize = W+H; layer = <CALayer: 0x4ac560>>
  | | |<SBWallpaperView: 0x4ad0f0; baseClass = UIImageView; frame = (0 0; 320 480); userInteractionEnabled = NO; layer = <CALayer: 0x4ad1a0>>
  | | | |<UIImageView: 0x4ac5e0; frame = (0 0; 320 62); opaque = NO; userInteractionEnabled = NO; layer = <CALayer: 0x4a0b30>>
  | | | |<UIImageView: 0x49f4e0; frame = (0 243; 320 237); opaque = NO; userInteractionEnabled = NO; layer = <CALayer: 0x4777b0>>
  | | | |<SBIconContentView: 0x493e70; frame = (0 0; 320 480); clipsToBounds = YES; autoresize = W+H; layer = <CALayer: 0x49f480>>
  | | | | |<UIView: 0x4aceb0; frame = (0 371; 320 109); opaque = NO; autoresize = W+TM; layer = <CALayer: 0x4757b0>>
  | | | | | |<SBDockIconListView: 0x495a60; frame = (0 20; 320 89); autoresize = TM; layer = <CALayer: 0x495b10>>
  | | | | | | |<SBIconView: 0xc6cfe0; frame = (16 11; 59 74); opaque = NO; layer = <CALayer: 0xc6cfcf0>>
  | | | | | | | |<SBIconImageContainerView: 0xc6cfef0; frame = (0 0; 59 74); autoresize = W+H; layer = <CALayer: 0xc6cff70>>
  | | | | | | | | |<UIImageView: 0xc6ed710; frame = (0 54; 59 62); transform = [1, 0, 0, -1, 0, 54]; opaque = NO; userInteractionEnabled = NO
0xc6ee170>>
  | | | | | | | | | |<UIImageView: 0xc6cd580; frame = (0 -1; 59 60); opaque = NO; userInteractionEnabled = NO; layer = <CALayer: 0xc6cd500>>
  | | | | | | | | | |<SBIconImageView: 0xc6dabc0; baseClass = UIImageView; frame = (0 -2; 59 62); opaque = NO; userInteractionEnabled = NO; lay
d1590>>
  | | | | | | | | | | |<SBIconLabel: 0xc6e9cc0; baseClass = UIControl; frame = (-13 60; 86 16); opaque = NO; userInteractionEnabled = NO; layer = <CAL
ext: Phone
  | | | | | | | | | | | |<SBIconView: 0xc6ee2b0; frame = (92 11; 59 74); opaque = NO; layer = <CALayer: 0xc6ee370>>
  | | | | | | | | | | | | |<SBIconImageContainerView: 0xc6ee3a0; frame = (0 0; 59 74); autoresize = W+H; layer = <CALayer: 0xc6ee3d0>>
  | | | | | | | | | | | | | |<UIImageView: 0xc6ee4b0; frame = (0 54; 59 62); transform = [1, 0, 0, -1, 0, 54]; opaque = NO; userInteractionEnabled = NO
0xc6ee660>>
  | | | | | | | | | | | | | | |<UIImageView: 0xc6ee420; frame = (0 -1; 59 60); opaque = NO; userInteractionEnabled = NO; layer = <CALayer: 0xc6ee460>>
  | | | | | | | | | | | | | | |<SBIconImageView: 0xc6ee5c0; baseClass = UIImageView; frame = (0 -2; 59 62); opaque = NO; userInteractionEnabled = NO; lay
ee600>>
  | | | | | | | | | | | | | | | |<SBIconLabel: 0x4d6ef0; baseClass = UIControl; frame = (-13 60; 86 16); opaque = NO; userInteractionEnabled = NO; layer = <CALa
t: Mail
  | | | | | | | | | | | | | | | |<SBIconView: 0xc6ee7e0; frame = (169 11; 59 74); opaque = NO; layer = <CALayer: 0xc6ee8a0>>
  | | | | | | | | | | | | | | | | |<SBIconImageContainerView: 0xc6ee8d0; frame = (0 0; 59 74); autoresize = W+H; layer = <CALayer: 0xc6ee900>>
  | | | | | | | | | | | | | | | | | |<UIImageView: 0xc6eeb90; frame = (0 54; 59 62); transform = [1, 0, 0, -1, 0, 54]; opaque = NO; userInteractionEnabled = NO
0xc6eed40>>
  | | | | | | | | | | | | | | | | | |<UIImageView: 0xc6ee950; frame = (0 -1; 59 60); opaque = NO; userInteractionEnabled = NO; layer = <CALayer: 0xc6eeb40>>
  | | | | | | | | | | | | | | | | | |<SBIconImageView: 0xc6eecc0; baseClass = UIImageView; frame = (0 -2; 59 62); opaque = NO; userInteractionEnabled = NO; lay
eece0>>
```



# Örnek Uygulama - cyscript

- Hedefimizde uygulamaların “icon”ları var.
- Görsel “subview” özelliklerini kullanarak “SBIconView”a erişeceğiz.

```
cy#  
cy# UIApp.windows[0].subviews [0].subviews [0].subviews [1].subviews [0].subviews [0].subviews [0].icon  
@"<SBApplicationIcon: 0x4a9e60> com.apple.mobilephone"  
cy#  
cy#  
cy#  
cy# UIApp.windows[0].subviews [0].subviews [0].subviews [1].subviews [0].subviews [0].subviews [1].icon  
@"<SBApplicationIcon: 0x4ac8b0> com.apple.mobilemail"  
cy#  
cy#  
cy#  
cy# UIApp.windows[0].subviews [0].subviews [0].subviews [1].subviews [0].subviews [0].subviews [2].icon  
@"<SBApplicationIcon: 0x4a9b80> com.apple.mobileipod"  
cy#  
cy#  
cy#  
cy# UIApp.windows[0].subviews [0].subviews [0].subviews [1].subviews [0].subviews [0].subviews [3].icon  
@"<SBApplicationIcon: 0x4ab4a0> com.apple.mobilesafari"  
cy#  
cy#  
cy#  
cy#
```



# Örnek Uygulama - cyscript

- Uygulama “icon”larına eriştiğimize göre, işlem yapabiliriz.
- Bir uygulama'yi görünmez yapalım.

```
cy#  
cy# [UIApp.windows[0].subviews [0].subviews [0].subviews [1].subviews [0].subviews [0].subviews [2] setHidden: YES]  
cy#  
cy#  
cy#  
cy#
```

- İlgili object'in “setHidden” metodunu çağırıyoruz.
- Metod çağırırken komutları [.....] içerisinde kullanıyoruz.



# Örnek Uygulama - cyscript

- Object'ler hiyerarşik olduğu için bir üst subview üzerinde işlem yapalım.

```
cy#  
cy# [UIApp.windows[0].subviews [0].subviews [0].subviews [1].subviews [0].subviews [0].subviews [2] setHidden: YES]  
cy#  
cy#  
cy# [UIApp.windows[0].subviews [0].subviews [0].subviews [1].subviews [0].subviews [0] setHidden: YES] ←  
cy#  
cy#
```

- Eriştığımız “subview” icon container olduğu için container içindeki bütün “icon”lar kayboldu.



# Örnek Uygulama - cyscript

- Object'lerde daha üste çıktığımızda...

```
cy#  
cy# [UIApp.windows[0].subviews [0].subviews [0].subviews [1].subviews [0].subviews [0].subviews [2] setHidden: YES]  
cy#  
cy# [UIApp.windows[0].subviews [0].subviews [0].subviews [1].subviews [0].subviews [0] setHidden: YES]  
cy#  
cy#  
cy# [UIApp.windows[0].subviews [0].subviews [0].subviews [1] setHidden: YES] ←  
cy#  
cy#
```

- Artık masaüstünü tamamen gizlemiş olduk.



# Örnek Uygulama - cyscript

- ... ve herşeyi geri getirelim...

```
cy#
cy# [UIApp.windows[0].subviews [0].subviews [0].subviews [1] setHidden: NO]
cy#
cy#
cy# [UIApp.windows[0].subviews [0].subviews [0].subviews [1].subviews [0].subviews [0] setHidden: NO]
cy#
cy#
cy# [UIApp.windows[0].subviews [0].subviews [0].subviews [1].subviews [0].subviews [0].subviews [2] setHidden: NO]
cy#
cy#
```

- setHidden: NO



# Örnek Uygulama - crypted

- Şimdi de PhotoVault uygulamasına bir bakalım.

- Uygulama giriş için parola istiyor...
- Bu ekranı by-pass edebilir miyiz?





# Örnek Uygulama - cyscript

- Cyscript ile uygulamaya attach olup, bu ekranı geçmeye ilişkin fonksiyon çağırısı yapabilirsek, by-pass etmiş olacağız.
- Bunun için “Application Delegate” içerisindeki fonksiyonlara göz atmamız gerekiyor.
- Bu noktada “class-dump-z” kullanacağız.



# Örnek Uygulama - cycript

- Uygulamaya attach olup, adım adım ilerleyelim...

```
SecrovePhone:~ root# ps -ef | grep PhotoVault
501 4791 1 0 0:00.00 ?? 0:03.61 /Applications/PhotoVault.app/PhotoVault
0 4802 4557 0 0:00.00 ttys000 0:00.00 grep PhotoVault
SecrovePhone:~ root#
SecrovePhone:~ root#
SecrovePhone:~ root# cycript -p 4791
cy#
cy# UIApplication.delegate
@"<AppDelegate: 0x647ae0>"
cy#
cy#
```

- Process ID: 4791
- Application Delegate: “AppDelegate”
- Class-dump-z ile uygulamanın class-dump'ını alıp işimize yarayacak fonksiyonlara bakabiliriz.



# Örnek Uygulama - crypted

- Uygulamayı dump edip, “AppDelegate” içindeki fonksiyonları inceleyelim.

```
nsyilmaz — ssh — 181x48
SecrovePhone:~/iphone_armv6 root# ps -ef | grep PhotoVault
 501 4791  1  0  0:00.00 ??          0:06.51 /Applications/PhotoVault.app/PhotoVault
  0 4825 4817  0  0:00.00 ttys001  0:00.00 grep PhotoVault
SecrovePhone:~/iphone_armv6 root#
SecrovePhone:~/iphone_armv6 root#
SecrovePhone:~/iphone_armv6 root#
SecrovePhone:~/iphone_armv6 root# ./class-dump-z      /Applications/PhotoVault.app/PhotoVault  > PhotoVault.dump
SecrovePhone:~/iphone_armv6 root#
```

```
nsyilmaz — ssh — 181x48
@interface AppDelegate : NSObject <UIApplicationDelegate, MFMailComposeViewControllerDelegate, UIAlertViewDelegate> {
    UIViewController* viewController;
    UITabBarController* aTabBarController;
    NSMutableArray* openedAlbums;
}
@property(assign, nonatomic) UITabBarController* aTabBarController;
-(void)applicationDidFinishLaunching:(id)application;
-(void)applicationWillEnterForeground:(id)application;
-(void)applicationWillResignActive:(id)application;
-(BOOL)navigator:(id)navigator shouldOpenURL:(id)url;
-(BOOL)application:(id)application handleOpenURL:(id)url;
-(void)dealloc;
-(id)documentsDirectory;
-(void)runOnce;
-(void)pinManagement;
-(void)pinLockController:(id)controller didFinishSelectingNewPin:(id)pin;
-(void)pinLockControllerDidFinishRemovingPin;
-(void)pinLockControllerDidCancel;
-(void)pinLockControllerDidFinishUnlocking;
-(void)lockController:(id)controller didFinish:(id)finish;
-(void)lockControllerDidCancel:(id)lockController;
-(void)promptForEmail;
-(void)emailPin;
-(void)mailComposeController:(id)controller didFinishWithResult:(int)result error:(id)error;
-(void>alertView:(id)view clickedButtonAtIndex:(int)index;
-(BOOL)checkInstaLockForAlbum:(id)album;
-(void)addAlbumToOpenedAlbums:(id)openedAlbums;
@end
```



# Örnek Uygulama - cycrypt

- Bu fonksiyonlar içinde “pinLockControllerDidFinishUnlocking” isminde bir fonksiyon mevcut. Denemeye değer...

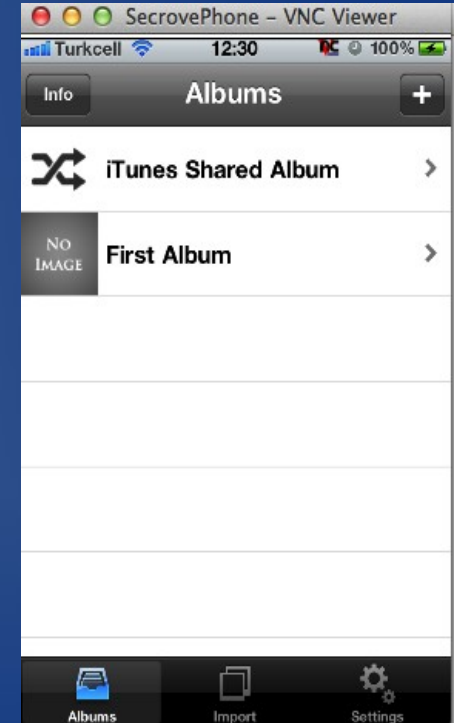
```
nsyilmaz — ssh — 181x48
@interface AppDelegate : NSObject <UIApplicationDelegate, MFMailComposeViewControllerDelegate, UIAlertViewDelegate> {
    UIViewController* viewController;
    UITabBarController* aTabBarController;
    NSMutableArray* openedAlbums;
}
@property(assign, nonatomic) UITabBarController* aTabBarController;
-(void)applicationDidFinishLaunching:(id)application;
-(void)applicationWillEnterForeground:(id)application;
-(void)applicationWillResignActive:(id)application;
-(BOOL)navigator:(id)navigator shouldOpenURL:(id)url;
-(BOOL)application:(id)application handleOpenURL:(id)url;
-(void)dealloc;
-(id)documentsDirectory;
-(void)runOnce;
-(void)pinManagement;
-(void)pinLockController:(id)controller didFinishSelectingNewPin:(id)pin;
-(void)pinLockControllerDidFinishRemovingPin;
-(void)pinLockControllerDidCancel;
-(void)pinLockControllerDidFinishUnlocking;
-(void)lockController:(id)controller didFinish:(id)finish;
-(void)lockControllerDidCancel:(id)lockController;
-(void)promptForEmail;
-(void)emailPin;
-(void)mailComposeController:(id)controller didFinishWithResult:(int)result error:(id)error;
-(void>alertView:(id)view clickedButtonAtIndex:(int)index;
-(BOOL)checkInstaLockForAlbum:(id)album;
-(void)addAlbumToOpenedAlbums:(id)openedAlbums;
@end
```



# Örnek Uygulama - cycrypt

- Cycrypt içinden “pinLockControllerDidFinishUnlocking” fonksiyonunu call ediyoruz.

```
cy#  
cy# [UIApp.delegate pinLockControllerDidFinishUnlocking]  
cy#  
cy#  
cy#  
cy#
```



# Örnek Uygulama - cyscript

- Fonksiyon çağrımız işe yarıyor ve authentication ekranını by-pass etmiş oluyoruz
- Peki başka neler yapabiliriz?
- PhotoVault Uygulamasının “iconBadge”ini değiştirelim.



```
cy#  
cy#  
cy# [UIApp setApplicationIconBadgeNumber: 999]  
cy#  
cy#  
cy# █
```



# Örnek Uygulama - cyscript

- Uygulamanın belleğinde işlem yapmamıza iman sağlayan “cyscript” ile
  - Uygulama arayüzüne ilişkin manipülasyonlar
  - Uygulama içindeki değişkenlere ilişkin manipülasyonlar
  - Uygulam içindeki fonksiyon çağrılarına ilişkin manipülasyonlar

gerçekleştirilerek, uygulama içerisindeki kontroller by-pass edilebilmektedir.



# Teşekkürler !

