Secure Data Storage on iOS with SQLCipher

Dr. Markus Maria Miedaner
Syracom Consulting AG
Dr. Yiannis Pavlosoglou
USB AG

markus.miedaner@syracom.de
yiannis@owasp.org

OWASP
15.11.2012

The OWASP Foundation
http://www.owasp.org

Top 10 Mobile Risks, Release Candidate v1.0

- Insecure Data Storage
- Weak Server Side Controls
- Insufficient Transport Layer Protection
- Client Side Injection
- Poor Authorization and Authentication
- Improper Session Handling
- Security Decisions Via Untrusted Inputs
- Side Channel Data Leakage
- Broken Cryptography
- Sensitive Information Disclosure

Previous work on this topic

- „Most apps are less secure than the security provided by the operating system."
  - http://www.elcomsoft.com/WP/BH-EU-2012-WP.pdf
- 2012 Elcomsoft analyzed 14 iOS password managing apps.
- Only one employed an encrypted database.

© smarterplanet.tumblr.com

Introduction to iOS Security

What does iOS offer to protect your data?

- A sandbox for each app
- Encrypted Filesystem
  - Two Keys:
    - DeviceKey (derived from UID-Key)
    - PasscodeKey (derived from user pass code)
- Policies and Mobile Device Management Systems
- Code signing and ASLR

© macworld.com.au

File protection on iOS

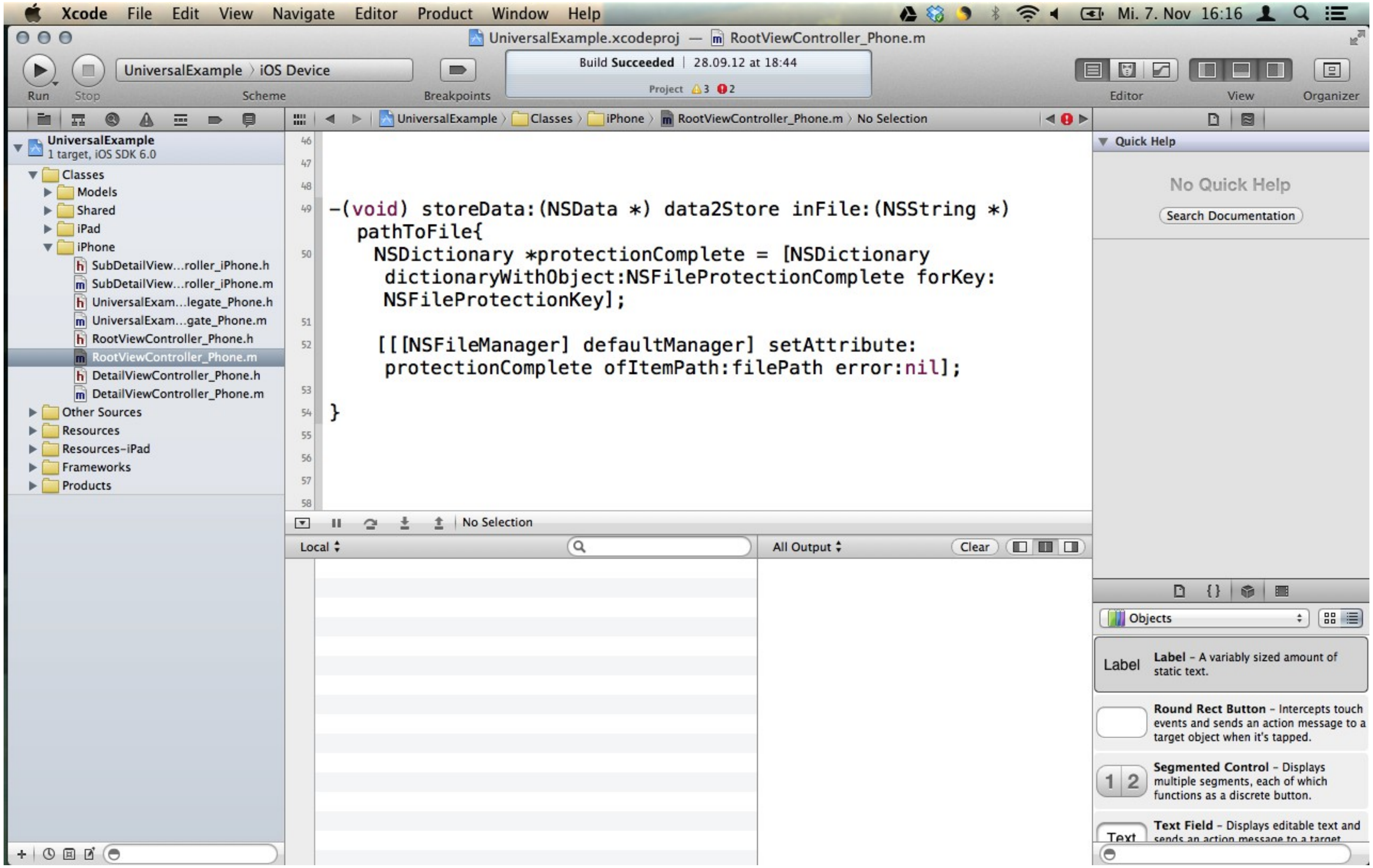
© midwestdocumentshredding.com

- ProtectionClasses:
  - NSFileProtectionNone
  - NSFileProtectionCompleteUnlessOpen
  - NSFileProtectionCompleteUntilFirstUserAuthentication
  - NSProtectionComplete

© archivepeterborough.co.uk

OWASP

Code Example for storing data in a file



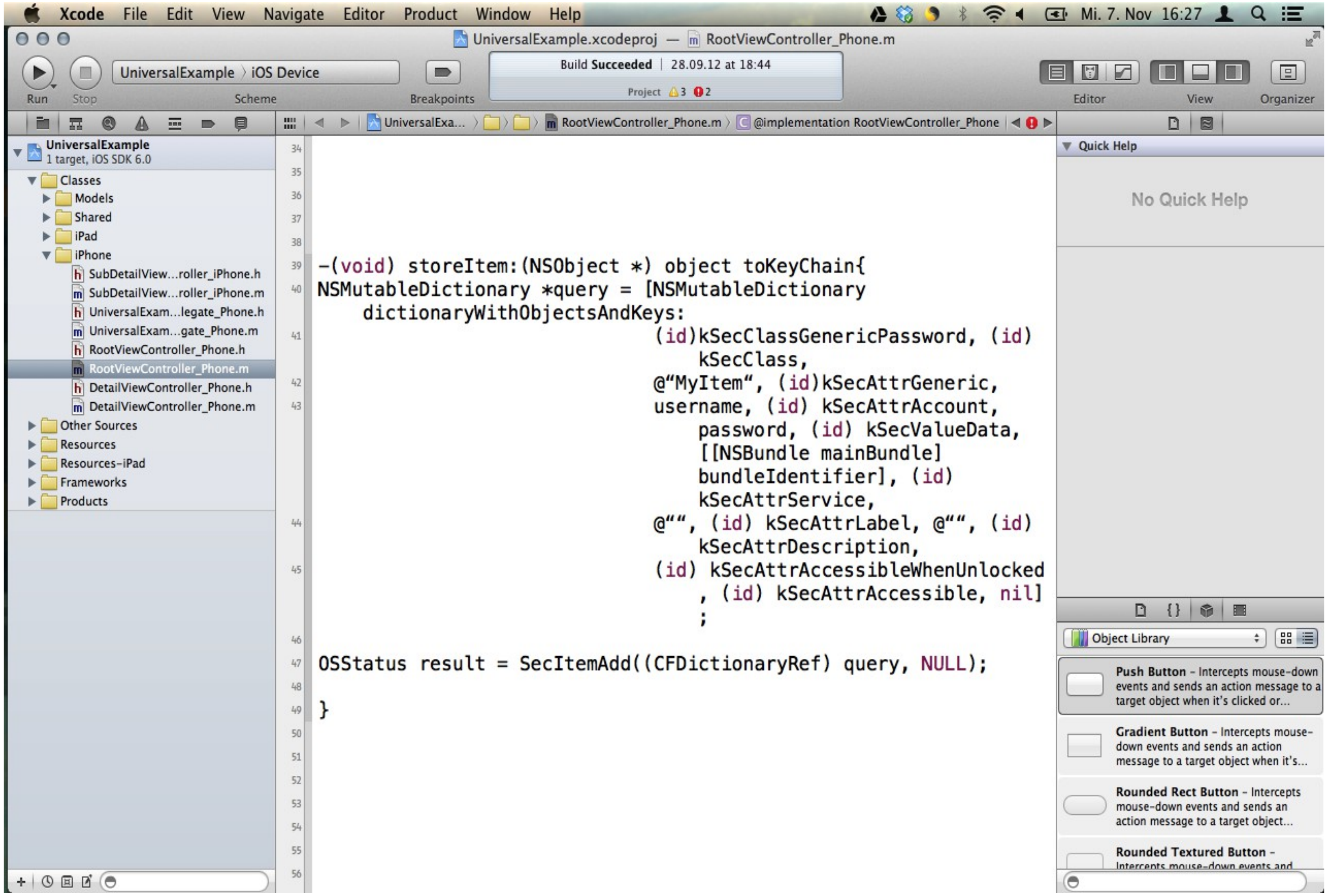
```
-(void) storeData:(NSData *) data2Store inFile:(NSString *)
  pathToFile{
    NSDictionary *protectionComplete = [NSDictionary
     dictionaryWithObject:NSFileProtectionComplete forKey:
     NSFileProtectionKey];

    [[[NSFileManager] defaultManager] setAttribute:
     protectionComplete ofItemPath:filePath error:nil];

}
```

Xcode File Edit View Navigate Editor Product Window Help
Mi. 7. Nov 16:16
UniversalExample.xcodeproj — RootViewController_Phone.m
Run
Stop
UniversalExample › iOS Device
Scheme
Breakpoints
Build Succeeded | 28.09.12 at 18:44
Project ⚠3 ❗2
Editor
View
Organizer
UniversalExample › Classes › iPhone › RootViewController_Phone.m › No Selection
UniversalExample
1 target, iOS SDK 6.0
Classes
Models
Shared
iPad
iPhone
SubDetailView...roller_iPhone.h
SubDetailView...roller_iPhone.m
UniversalExam...legate_Phone.h
UniversalExam...gate_Phone.m
RootViewController_Phone.h
RootViewController_Phone.m
DetailViewController_Phone.h
DetailViewController_Phone.m
Other Sources
Resources
Resources-iPad
Frameworks
Products
Quick Help
No Quick Help
Search Documentation
No Selection
Local
All Output
Clear
Objects
Label – A variably sized amount of static text.
Round Rect Button – Intercepts touch events and sends an action message to a target object when it's tapped.
Segmented Control – Displays multiple segments, each of which functions as a discrete button.
Text Field – Displays editable text and sends an action message to a target

KeyChainItems – ProtectionClasses

- KsecAttrAccessibleWhenUnlocked
- kSecAttrAccessibleAfterFirstUnlock
- kSecAttrAccessibleAlways
- kSecAttrAccessibleWhenUnlockThisDeviceOnly
- kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly
- kSecAttrAccessibleThisDeviceOnly

Example Code for storing in KeyChain


Xcode File Edit View Navigate Editor Product Window Help
Mi. 7. Nov 16:27
UniversalExample.xcodeproj — RootViewController_Phone.m
Run Stop Scheme Breakpoints Editor View Organizer
UniversalExample iOS Device
Build Succeeded | 28.09.12 at 18:44
Project 3 2
UniversalExample
1 target, iOS SDK 6.0
Classes
Models
Shared
iPad
iPhone
SubDetailView...roller_iPhone.h
SubDetailView...roller_iPhone.m
UniversalExam...legate_Phone.h
UniversalExam...gate_Phone.m
RootViewController_Phone.h
RootViewController_Phone.m
DetailViewController_Phone.h
DetailViewController_Phone.m
Other Sources
Resources
Resources-iPad
Frameworks
Products
UniversalExa... RootViewController_Phone.m @implementation RootViewController_Phone
Quick Help
No Quick Help
Object Library
Push Button - Intercepts mouse-down events and sends an action message to a target object when it's clicked or...
Gradient Button - Intercepts mouse-down events and sends an action message to a target object when it's...
Rounded Rect Button - Intercepts mouse-down events and sends an action message to a target object...
Rounded Textured Button -

```
-(void) storeItem:(NSObject *) object toKeyChain{
NSMutableDictionary *query = [NSMutableDictionary
    dictionaryWithObjectsAndKeys:
                              (id)kSecClassGenericPassword, (id)
                                  kSecClass,
                              @"MyItem", (id)kSecAttrGeneric,
                              username, (id) kSecAttrAccount,
                                  password, (id) kSecValueData,
                                  [[NSBundle mainBundle]
                                  bundleIdentifier], (id)
                                  kSecAttrService,
                              @"", (id) kSecAttrLabel, @"", (id)
                                  kSecAttrDescription,
                              (id) kSecAttrAccessibleWhenUnlocked
                                  , (id) kSecAttrAccessible, nil]
                                  ;

OSStatus result = SecItemAdd((CFDictionaryRef) query, NULL);

}
```

BruteForce against PassCodes on iPhone4

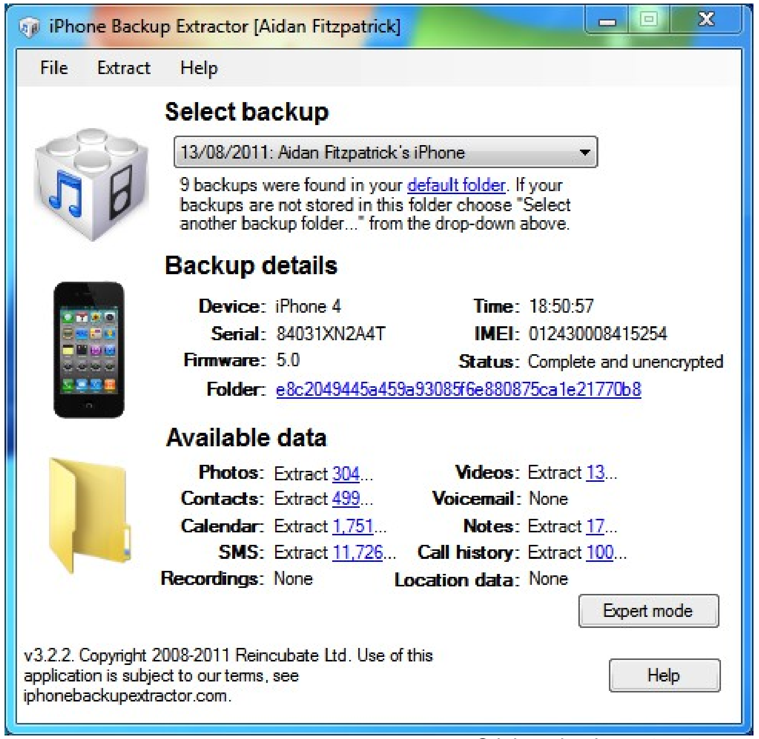
© seul-le-cinema.blogspot.com

Length of Passcode	Complexity	Time
4	Numeric	18 Minutes
4	Alphanumeric	19 Days
6	Alphanumeric	196 Years
8	Alphanumeric	755.000 Years
8	Alphanumeric (Complex)	27 Mil. Years

© iOS-Hacker Handbook, 2012, Charly Miller et al.

How to get the file/data off the device

- iTunes Backup
- iPhoneBackupExtractor
- Jailbroken iPhone
  - Untethered jailbreak
  - Tethered jailbreak
- Attacks against the app



Select backup

13/08/2011: Aidan Fitzpatrick's iPhone

9 backups were found in your default folder. If your backups are not stored in this folder choose "Select another backup folder..." from the drop-down above.

Backup details

Device:	iPhone 4	Time:	18:50:57
Serial:	84031XN2A4T	IMEI:	012430008415254
Firmware:	5.0	Status:	Complete and unencrypted
Folder:	e8c2049445a459a93085f6e880875ca1e21770b8		

Available data

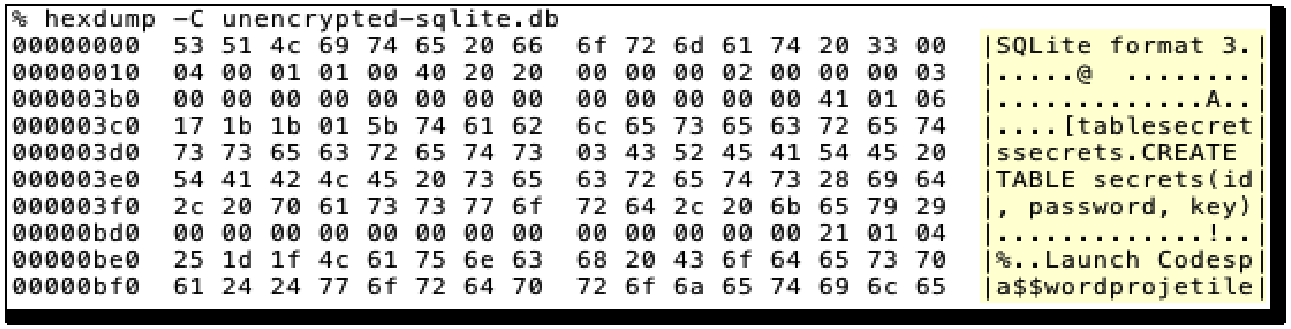
Photos:	Extract 304...	Videos:	Extract 13...
Contacts:	Extract 499...	Voicemail:	None
Calendar:	Extract 1,751...	Notes:	Extract 17...
SMS:	Extract 11,726...	Call history:	Extract 100...
Recordings:	None	Location data:	None

v3.2.2. Copyright 2008-2011 Reincubate Ltd. Use of this application is subject to our terms, see iphonebackupextractor.com.

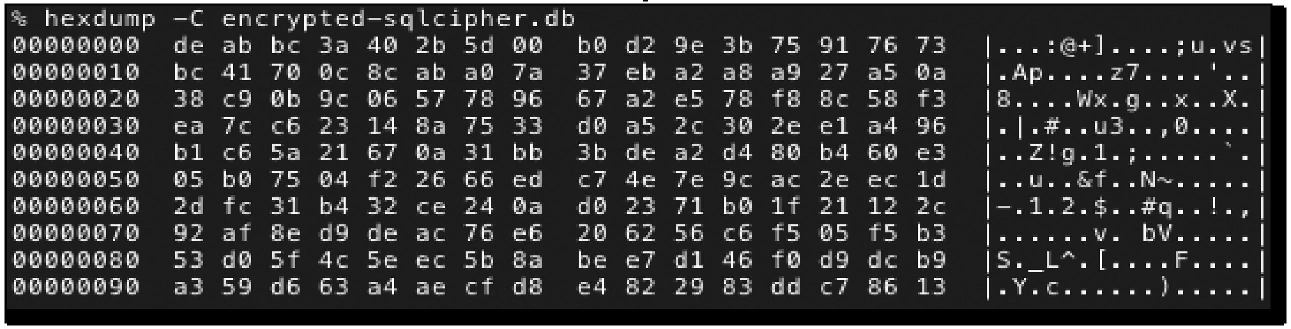
© iphonebackupextractor.com

SQLCipher – Database Security

What are we actually talking about?



```
% hexdump -C unencrypted-sqlite.db
00000000  53 51 4c 69 74 65 20 66  6f 72 6d 61 74 20 33 00  |SQLite format 3.|
00000010  04 00 01 01 00 40 20 20  00 00 00 02 00 00 00 03  |.....@  ........|
000003b0  00 00 00 00 00 00 00 00  00 00 00 00 00 41 01 06  |.............A..|
000003c0  17 1b 1b 01 5b 74 61 62  6c 65 73 65 63 72 65 74  |....[tablesecret|
000003d0  73 73 65 63 72 65 74 73  03 43 52 45 41 54 45 20  |ssecrets.CREATE |
000003e0  54 41 42 4c 45 20 73 65  63 72 65 74 73 28 69 64  |TABLE secrets(id|
000003f0  2c 20 70 61 73 73 77 6f  72 64 2c 20 6b 65 79 29  |, password, key)|
00000bd0  00 00 00 00 00 00 00 00  00 00 00 00 00 21 01 04  |.............!..|
00000be0  25 1d 1f 4c 61 75 6e 63  68 20 43 6f 64 65 73 70  |%..Launch Codesp|
00000bf0  61 24 24 77 6f 72 64 70  72 6f 6a 65 74 69 6c 65  |a$$wordprojetile|
```

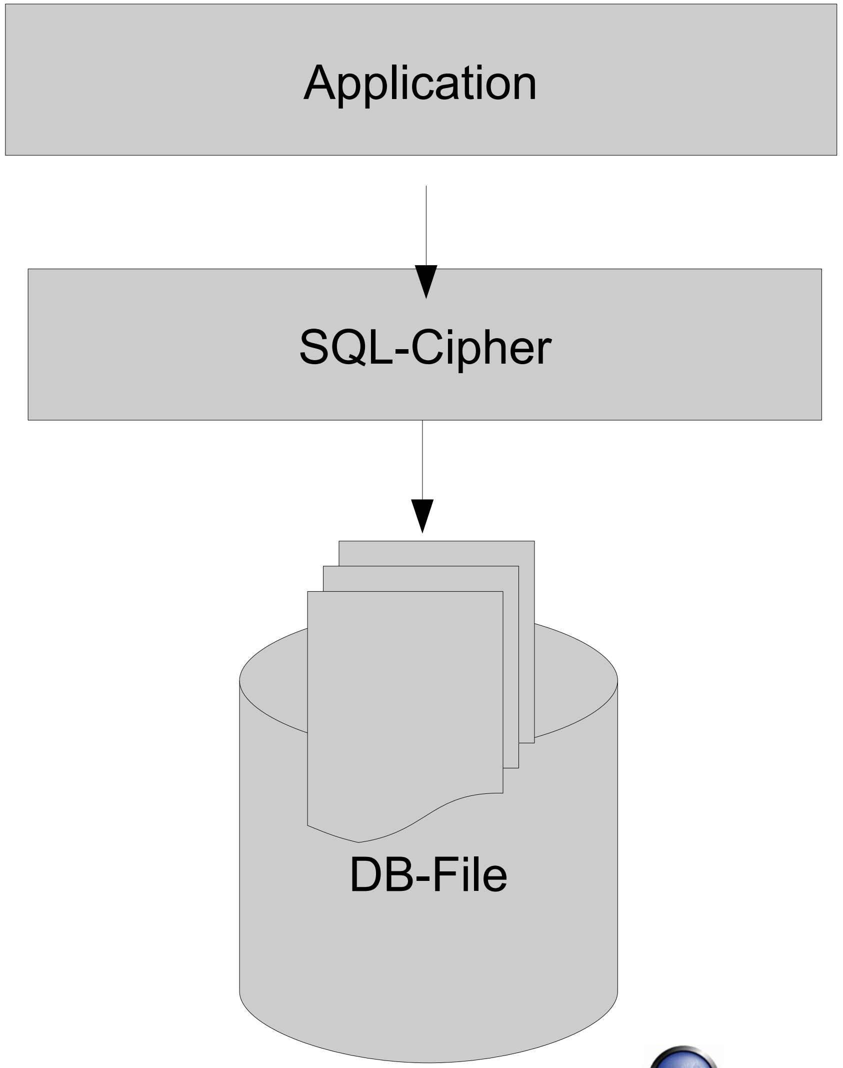


```
% hexdump -C encrypted-sqlcipher.db
00000000  de ab bc 3a 40 2b 5d 00  b0 d2 9e 3b 75 91 76 73  |...:@+]....;u.vs|
00000010  bc 41 70 0c 8c ab a0 7a  37 eb a2 a8 a9 27 a5 0a  |.Ap....z7....'..|
00000020  38 c9 0b 9c 06 57 78 96  67 a2 e5 78 f8 8c 58 f3  |8....Wx.g..x..X.|
00000030  ea 7c c6 23 14 8a 75 33  d0 a5 2c 30 2e e1 a4 96  |.|.#..u3..,0....|
00000040  b1 c6 5a 21 67 0a 31 bb  3b de a2 d4 80 b4 60 e3  |..Z!g.1.;.....`.|
00000050  05 b0 75 04 f2 26 66 ed  c7 4e 7e 9c ac 2e ec 1d  |..u..&f..N~.....|
00000060  2d fc 31 b4 32 ce 24 0a  d0 23 71 b0 1f 21 12 2c  |-.1.2.$..#q..!.,|
00000070  92 af 8e d9 de ac 76 e6  20 62 56 c6 f5 05 f5 b3  |......v. bV.....|
00000080  53 d0 5f 4c 5e ec 5b 8a  be e7 d1 46 f0 d9 dc b9  |S._L^.[....F....|
00000090  a3 59 d6 63 a4 ae cf d8  e4 82 29 83 dd c7 86 13  |.Y.c......).....|
```

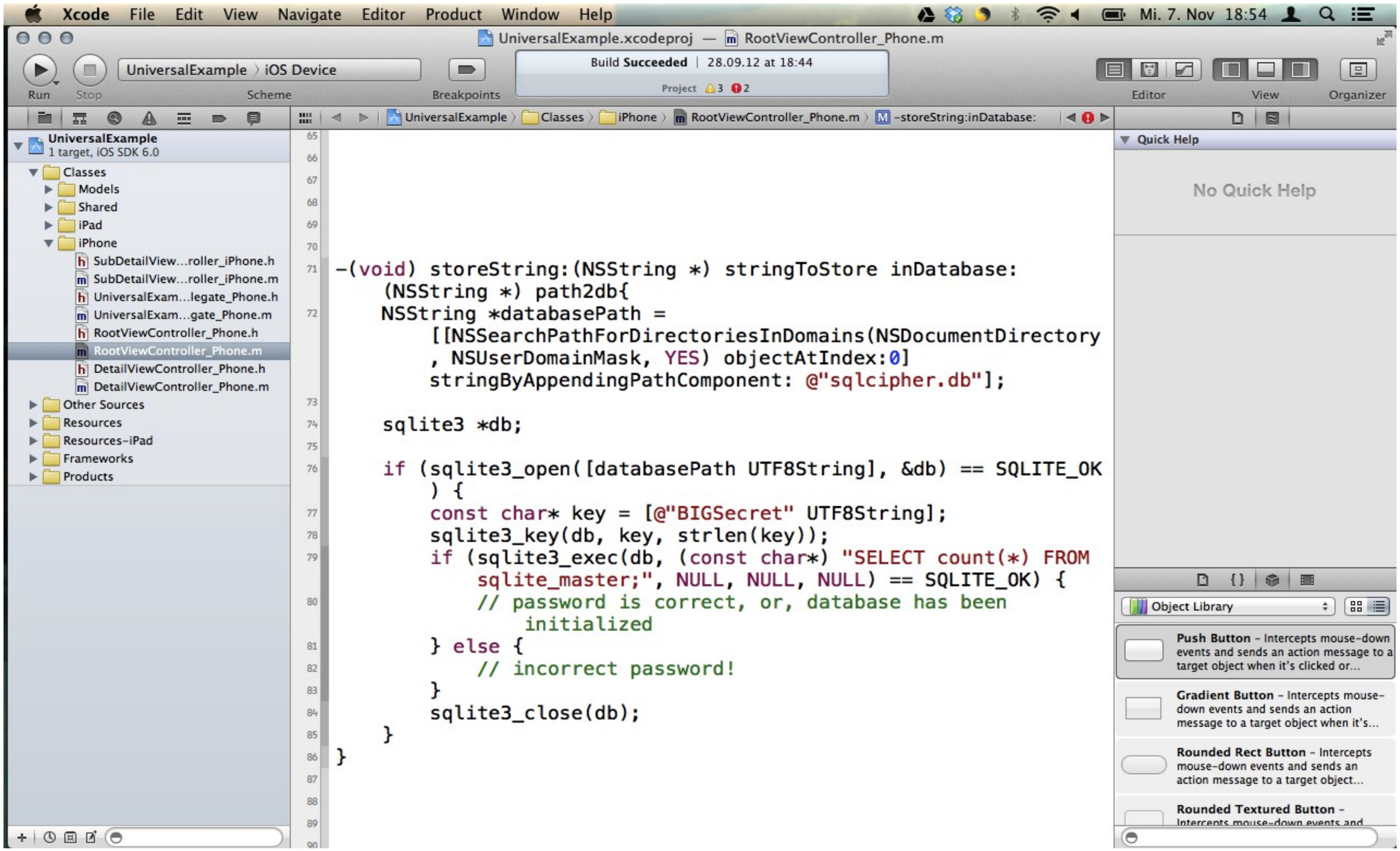
© sqlcipher.net

SQLCipher - Architecture

- Each DB has a 16 byte salt
- Works on „pages“ of 1024 bytes
- Each page has its own IV
- Each page has an HMAC_SHA1 signature
- Pages are AES-256 encrypted
- Transparent for the application layer



SQLCipher – Code Example



```
-(void) storeString:(NSString *) stringToStore inDatabase:
    (NSString *) path2db{
    NSString *databasePath =
        [[NSSearchPathForDirectoriesInDomains(NSDocumentDirectory
        , NSUserDomainMask, YES) objectAtIndex:0]
        stringByAppendingPathComponent: @"sqlcipher.db"];

    sqlite3 *db;

    if (sqlite3_open([databasePath UTF8String], &db) == SQLITE_OK
        ) {
        const char* key = [@"BIGSecret" UTF8String];
        sqlite3_key(db, key, strlen(key));
        if (sqlite3_exec(db, (const char*) "SELECT count(*) FROM
            sqlite_master;", NULL, NULL, NULL) == SQLITE_OK) {
            // password is correct, or, database has been
               initialized
        } else {
            // incorrect password!
        }
        sqlite3_close(db);
    }
}
```

Xcode File Edit View Navigate Editor Product Window Help
Mi. 7. Nov 18:54
UniversalExample.xcodeproj — RootViewController_Phone.m
Run Stop Scheme Breakpoints Editor View Organizer
UniversalExample › iOS Device
Build Succeeded | 28.09.12 at 18:44
Project 3 2
UniversalExample › Classes › iPhone › RootViewController_Phone.m › -storeString:inDatabase:
UniversalExample
1 target, iOS SDK 6.0
Classes
Models
Shared
iPad
iPhone
SubDetailView...roller_iPhone.h
SubDetailView...roller_iPhone.m
UniversalExam...legate_Phone.h
UniversalExam...gate_Phone.m
RootViewController_Phone.h
RootViewController_Phone.m
DetailViewController_Phone.h
DetailViewController_Phone.m
Other Sources
Resources
Resources-iPad
Frameworks
Products
Quick Help
No Quick Help
Object Library
Push Button – Intercepts mouse-down events and sends an action message to a target object when it's clicked or...
Gradient Button – Intercepts mouse-down events and sends an action message to a target object when it's...
Rounded Rect Button – Intercepts mouse-down events and sends an action message to a target object...
Rounded Textured Button – Intercepts mouse-down events and

Setting the scene – ready to attack

© smbnow.com

Attacking an encrypted database file

- File generator based on sqlite -init init.txt

- Decrypting the file
  - Directly and checking for magic number
    - hard to do :)

  - Using sqlCipher-cli
    - works – hurray!

© feelpositive.wordpress.com

© jaybot7.com

Brute forcing an encrypted DB

4 Characters

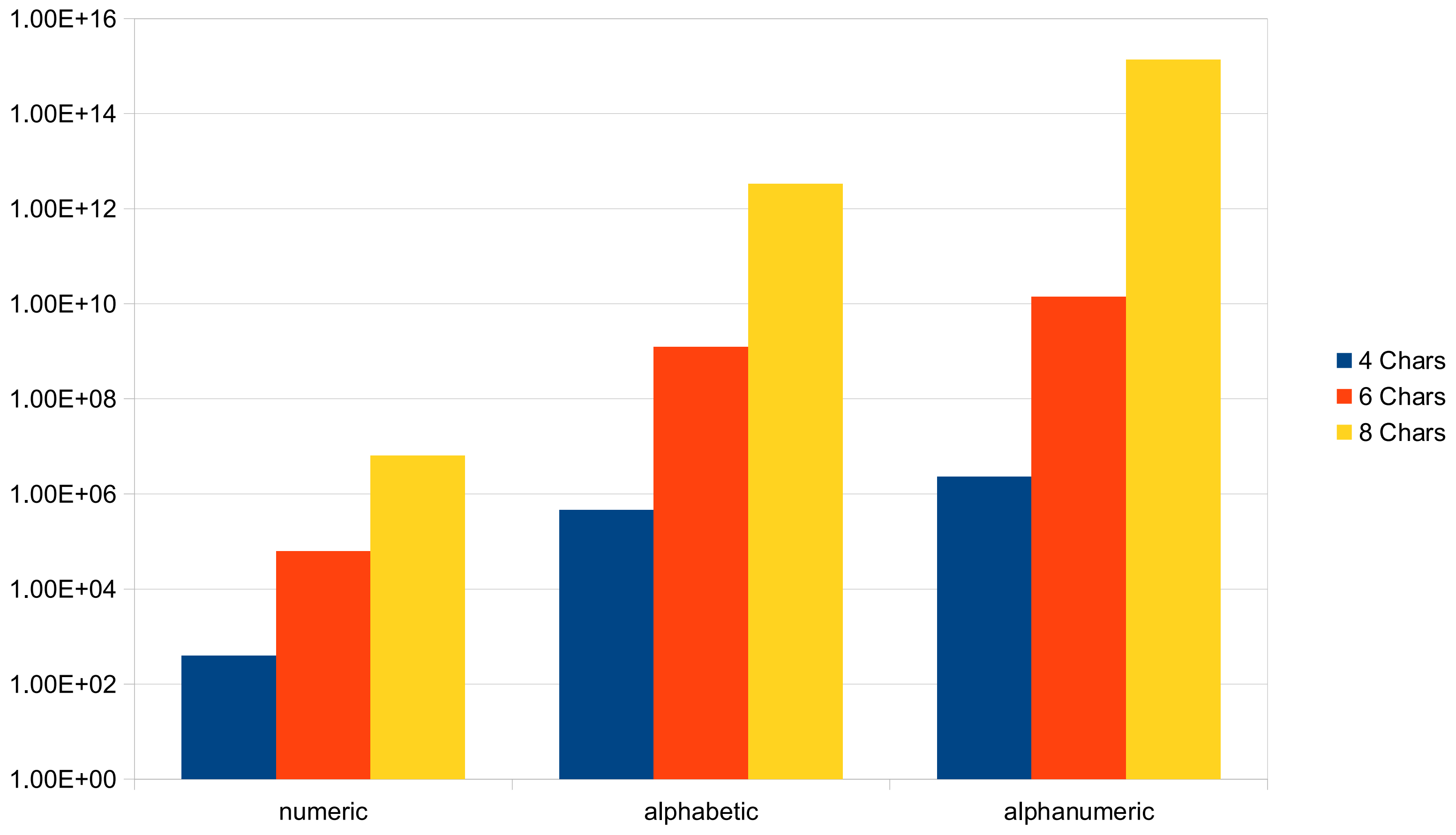
Numeric (0-9)	6.8	minutes
Alphabetic (a-zA-Z)	128	hours
Alphanumeric (a-zA-Z0-9+*$%&/()[]-_.:,;)	27	days

8 Characters

Numeric (0-9)	73	days
Alphabetic (a-zA-Z)	107,462	years
Alphanumeric (a-zA-Z0-9+*$%&/()[]-_.:,;)	2,754,150	years

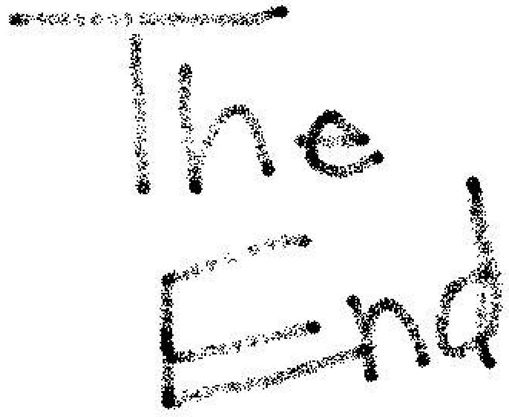
- Hardware
  - MacBook: 2 Ghz Intel, 2GB RAM

Brute forcing an encrypted database (seconds)



Summary

- Mobile OS-Security often harder
- Don't rely solely on OS-Security features
- Use strong cryptography whenever possible



© http://jholverstott.files.wordpress.com/

© allthingsd.com