Angriffe auf iPhone und iPad in der Praxis

- Mythos und Wirklichkeit -

Klaus Rodewig
Senior IT Security Analyst - TÜV Trust IT GmbH

Ihr Referent

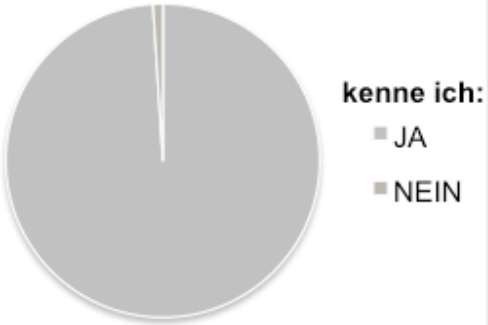
- Senior IT Security Analyst
- Certified Professional for Secure Software Engineering
- ISO 27001 Auditor
- über 12 Jahre Berufserfahrung bei führenden Unternehmen der Branchen Engineering, Telekommunikation, Medien, Logistik, Geheimschutz, Banken und Versicherungen sowie bei Behörden
- Autor bei Galileo Press

*Auflage 2 erscheint im Sommer

TÜV Austria

Der DACH-TÜV: TÜV TRUST IT (TA) GmbH

Die Marke TÜV ®



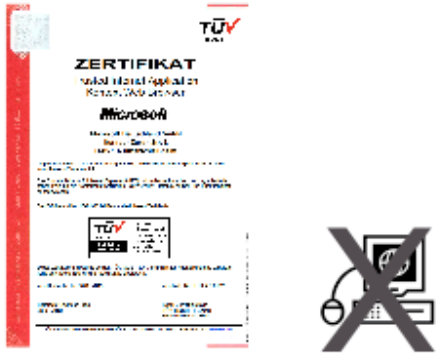
DACH – TÜV

TÜV - Tätigkeiten

Seit 1872

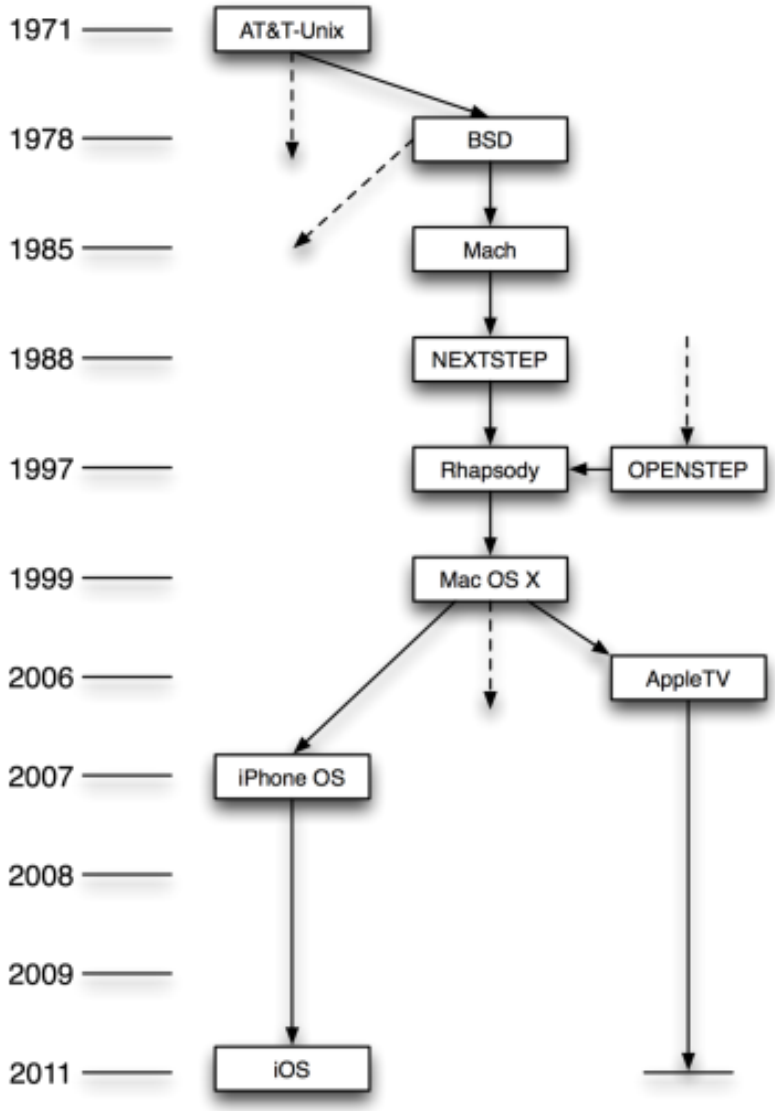
TÜV AUSTRIA

Neutralität und Unabhängigkeit



Unser Team

iOS


1971
1978
1985
1988
1997
1999
2006
2007
2008
2009
2011
AT&T-Unix
BSD
Mach
NEXTSTEP
Rhapsody
OPENSTEP
Mac OS X
AppleTV
iPhone OS
iOS

Sicherheitsmechanismen iOS

- Sandboxing
- Mandatory Code Signing
  - Verwendung von Zertifikaten in allen sicherheitskritischen Bereichen
- App Store / Enterprise App Store
- zentrale Keychain
  - Datenbank für Passwörter, private Schlüssel und Zertifikate
- ab iPhone 3GS: Hardware-basierte Verschlüsselung (AES256)
  - Remote Wipe, physischer Zugriffsschutz
- MDM-API

iDevices

- iPhone
  - iPhone 2G
  - iPhone 3G
  - iPhone 3GS
  - iPhone 4
  - iPhone 4S
- iPad
  - iPad 1
  - iPad 2
  - *iPad 3 (7.3.2012 ?)*
- iPod Touch
  - iPod Touch 1G
  - iPod Touch 2G
  - iPod Touch 3G
  - iPod Touch 4G

- Hardware:
  - bis zu 1 GHz Dualcore-Prozessor
  - bis zu 1 GB RAM
  - A-GPS
  - Kompass
  - Gyroskop
  - Mikrofon
  - Kamera
  - Sprachsteuerung
  - WLAN
  - Bluetooth
  - GSM
  - UMTS
  - HSDPA
  - USB

Infrastruktur

- dezentraler Zugriff auf vorhandene Infrastruktur
  - Exchange
  - Lotus Notes
  - IMAP, POP, SMTP
  - LDAP
  - ...
- Management optional
  - Kommunikation über Apple Push-Dienst
- konträres Paradigma zu Blackberry
  - Blackberry Enterprise Server
  - Kommunikation über RIM-NOC

Funktionsumfang iDevice

- System-Apps für die "Grundversorgung"
  - Email
  - Kalender
  - Adressbuch
- App Store für spezielle Anwendungsfälle
  - Apple App Store
  - Enterprise App Store
- kein direkter Zugriff auf Systemressourcen durch Apps
  - Verwendung von API-Klassen und -Methoden
  - alle Apps laufen im selben Benutzerkontext

iDevice aus Sicht des Angreifers

- Unix-Betriebssystem
  - im Detail noch optimierungsfähig
- 24x7 - high availability
- (dauerhafte) Verbindung zum Internet
- Geo-Lokalisierung
- Private und dienstliche Daten
- Datenübermittlung über Mobilfunk
- viele Schnittstellen und Komponenten
  - viele Angriffsvektoren
  - viele noch unbekannte Angriffsklassen

Werte im iDevice

Adressbuch

Keychain

Email

Exchange

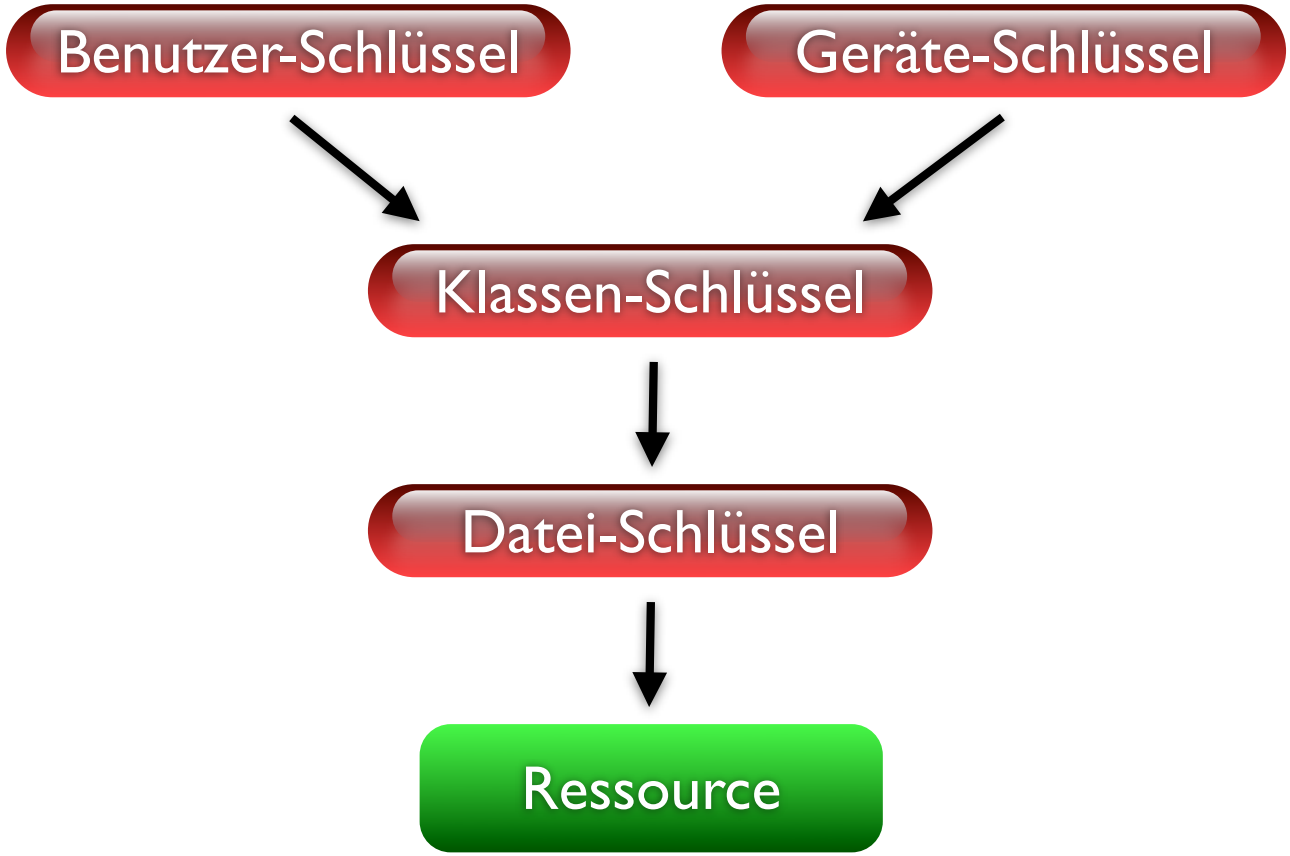
Safari

WLAN

Kalender

Position

Verschlüsselung



Schutzklassen für das Dateisystem

Entschlüsselt	Schutzklasse
Immer	**`NSFileProtectionNone`**
Nach erster Eingabe des Passcodes	`NSFileProtectionCompleteUntilFirstUserAuthentication`
Nach Boot oder Eingabe des Passcodes	`NSFileProtectionComplete`
Zugriff im entsperrten Zustand, danach weiter entschlüsselt	`NSFileProtectionCompleteUnlessOpen`

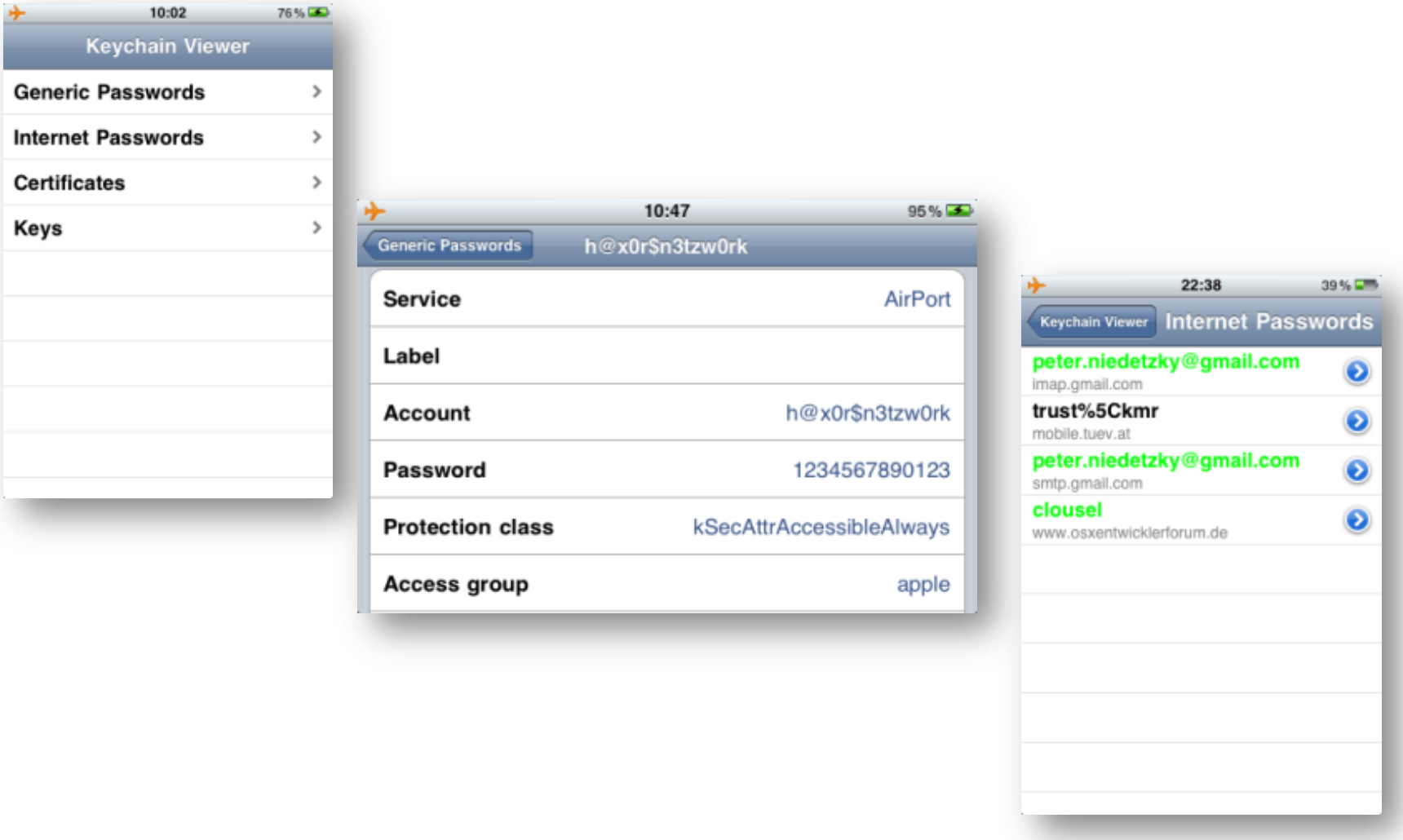
Schutzklassen für die Keychain

Entschlüsselt	Schutzklasse
Immer	`kSecAttrAccessibleAlways`
Immer, nur aktuelles Gerät	`kSecAttrAccessibleAlwaysThisDeviceOnly`
Nach erster Eingabe des Passcodes	**`kSecAttrAccessibleAfterFirstUnlock`**
Nach erster Eingabe des Passcodes, nur aktuelles Gerät	`kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly`
Nach Eingabe des Passcodes	`kSecAttrAccessibleWhenUnlocked`
Nach Eingabe des Passcodes, nur aktuelles Gerät	`kSecAttrAccessibleWhenUnlockedThisDeviceOnly`

System-Standards

Item	Protection class
WLAN-Kennwörter	`kSecAttrAccessibleAlways`
Exchange-Zugangsdaten	`kSecAttrAccessibleAlways`
VPN-Zugangsdaten	`kSecAttrAccessibleAlways`
Email-Zugangsdaten	`kSecAttrAccessibleAfterFirstUnlock`
LDAP-, CalDAV-, CardDAV-Zugangsdaten	`kSecAttrAccessibleWhenUnlocked`
iTunes-Backup-Passwort	`kSecAttrAccessibleWhenUnlockedThisDeviceOnly`

KeychainViewer



Fehler im iOS

Arbitrary code execution

- iOS 4.0 (2010): u.a. 19 arbitrary code execution
- iOS 4.1 (2010): u.a. 27 arbitrary code execution
- iOS 4.2 (2010): u.a. 42 arbitrary code execution
- iOS 4.3 (2011): u.a. 53 arbitrary code execution
- iOS 5.0 (2011): u.a. 12 arbitrary code execution
- alle iOS-Versionen bis 4.3.5: SSL-Bug bei Prüfung des CA-Bits

Jailbreak

- Kompromittierung auf Kernel-Ebene
- Schreibzugriff auf /
- kein Code Signing
- kein Sandboxing
- Deaktivierung aller Sicherheitsmechanismen
  - z.B. Zugriff auf Emails, Keychain, Zertifikate, etc.
- Firmware & Tools unbekannter Herkunft
- jailbreakme.com

Spyware

- Analyse von 1407 kostenlosen Apps für iPhone und iPad
  - 825 aus dem Apple-Store
  - 582 aus dem freien Cydia-Store (Jailbreak notwendig)

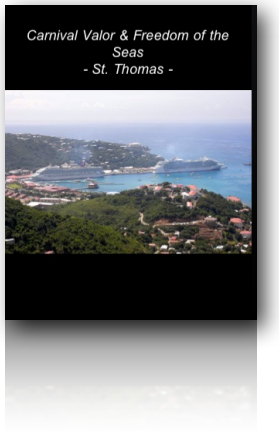
- 55% der untersuchten Apps übermitteln heimlich Daten an Entwickler und/oder Werbefirmen
  - UDID (seit iOS 5 nicht mehr relevant)
  - Lokalisation
  - Adressbuch
  - Kalender

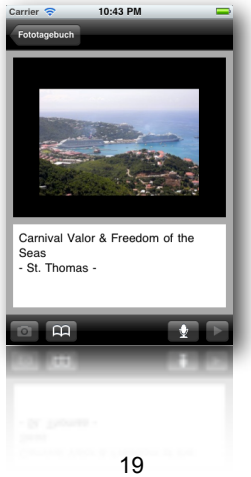
- Apple Review Guidelines
  - nicht transparent
  - fokussiert auf das Geschäftsmodell von Apple
  - keine explizite Überprüfung auf Sicherheitslücken

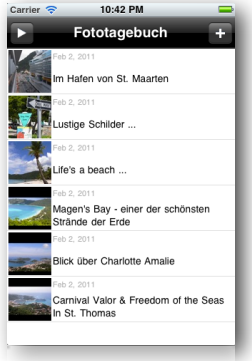
- Reaktion von Apple: *$DEVELOPER

Fototagebuch

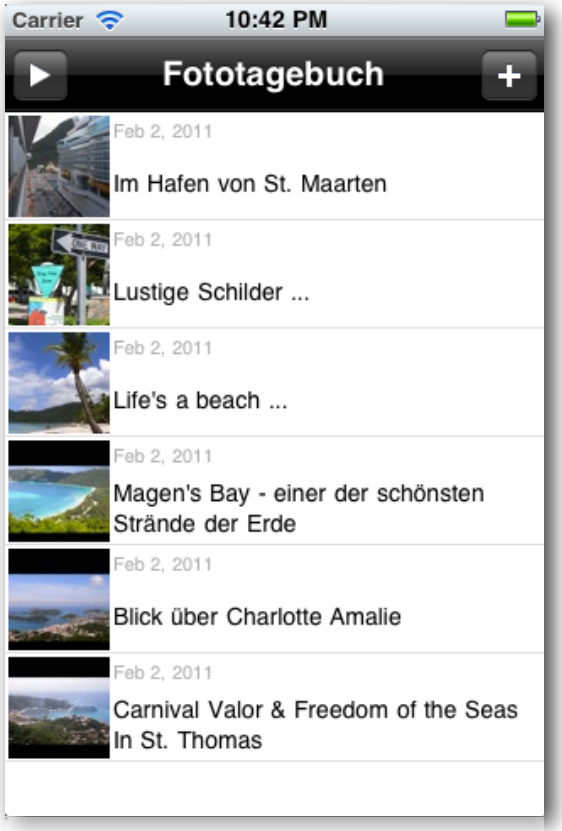
- Tagebuchfunktion mit Bild und Ton
- Fotos mit GPS-Koordinaten
- Facebook-Integration
  - Tagebuch-Einträge
  - Convenience-Funktion: Adressbuch hochladen
- Twitter-Integration

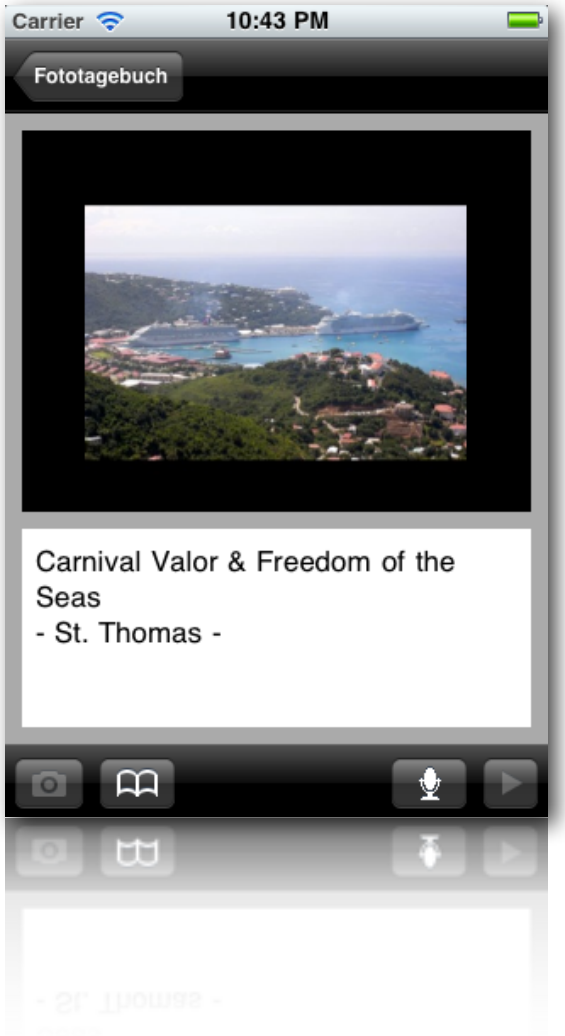


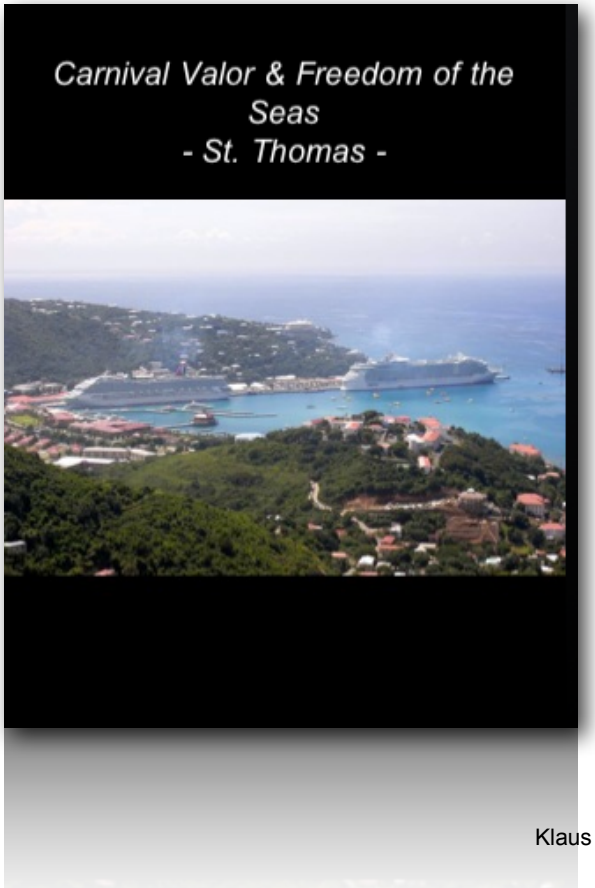




Nice, glossy, awesome







Besondere Funktionen

- Auslesen der UDID (iOS < 5)
- Auslesen des gesamten Adressbuchs
  - Facebook: Identifikation des Benutzers möglich
- kontinuierliches Ermitteln und Übertragen des Standorts
  - Umgehung: Geotagging der Tagebuch-Einträge, Facebook/Twitter
  - Alternative: Bilder mit GPS-Tag (keine Warnung)
- Übertragen der Daten an unseren Server
- Umfang: knapp 100 Zeilen Code
- Nicht im App Store erhältlich ;-)
- *analog SpyPhone von Nicolas Seriot*

Unsichere Apps

Anonymer Entwickler

Frage: Verschlüsselte Datei-Ablage

"I will admit that I'm still slightly nervous of making security a selling point - by doing so, I may expose myself to a certain level of liability should I make a mistake - I'd rather forgot a few sales than get hauled up on some security breach legal action thing..."

Fallstricke

Apple-Dokumentation zu CommonCryptor.h

„Another option for block ciphers is Cipher Block Chaining, known as CBC mode. When using CBC mode, an Initialization Vector (IV) is provided along with the key when starting an encrypt or decrypt operation. If CBC mode is selected and no IV is provided, an IV of all zeroes will be used. „

Bootloader-Bug

iPhone <= 4 & iPad 1

- Bootloader im Geräte-ROM gespeichert
  - manipulationssicher
- Bootloader lädt über drei Stufen das im Flash-Speicher liegende Betriebssystem
  - Betriebssystem ist signiert
  - Bootloader prüft die Signatur
- Notfallprozedur, um korrupte Installationen reparieren zu können
  - DFU-Modus
  - Booten über USB
  - Aktivierung auch im gesperrten oder ausgeschalteten Zustand
- Buffer Overflow im Bootloader
  - Booten eines unsignierten (manipulierten) Betriebssystems

Angriff gegen Bootloader-Bug

- Starten einer Firmware mit SSH-Server
- Verbindung vom Rechner per SSH zum iDevice
- Mounten der Systempartitionen
- Brute-Force-Angriff auf den Keybag
  - Passcode
  - Schutzmechanismen nur über GUI
- Dauer:
  - 4 Zeichen numerisch: 30 Minuten
  - 4 Zeichen alphanumerisch: 33 Tage
  - 5 Zeichen alphanumerisch: 5,5 Jahre

MDM-API

- Inventarisierung und Überwachung
- Verteilen von Richtlinien
  - Passwort-Richtlinie
  - Jugendschutz
  - JavaScript im Browser
  - iCloud
  - …
- Verteilen von Konfigurationen
  - Konto-Einstellungen
  - VPN
  - Zertifikate
  - …
- **nicht**: selektive App-Installation ($$$)

Zusammenfassung I

Exemplarische Auswahl von Bedrohungen

- Blindfllug (Patchlevel, installierte Apps, Konfiguration, Profile, …)
  - *Mobile Device Management*
- unsichere Verbindung zur Infrastruktur
  - *Mail-Gateway mit Authentisierung*
- Jailbreak
  - *MDM mit guter Jailbreak-Erkennung*
- Datenabfluss durch böse Apps
  - *Risiko-Management, Whitelist, Mobile Device Policy*
- Sicherheitslücken durch unsichere Apps
  - *Whitelist, Awareness, SDL für Enterprise Apps, SDL für Dokumentenverarbeitung*

Zusammenfassung II

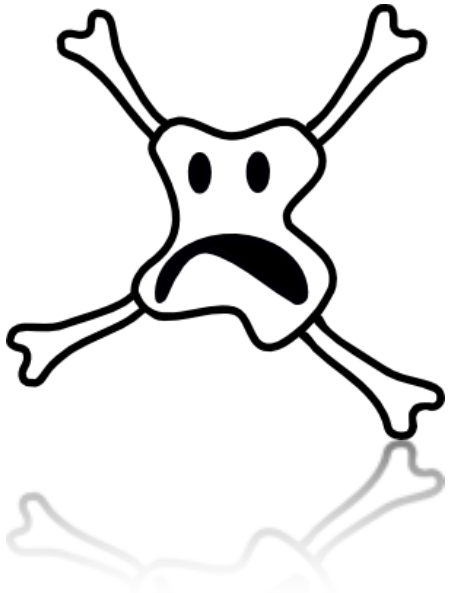
Exemplarische Auswahl von Bedrohungen

- unsichere Hardware (Remote Wipe, Bootloader-Bug)
  - *Passwort-Richtlinie (technisch und organisatorisch), Whitelist von erlaubten Endgeräten*
- BYOD
  - *MDM mit selective Wipe, Mobile Device Policy*
- gutes Konzept
  - *fundiert & angemessen*

Live-Hacking

Quot erat expectandum …

- X.509-basierte Email-Verschlüsselung mit S/MIME
  - "Industriestandard"
  - eingeführt mit iOS 5
- ermöglicht Ende-zu-Ende-Verschlüsselung
  - Outlook, Lotus Notes, …
- "kleines" Problem beim Versenden von Anhängen …



Vielen Dank für Ihre Aufmerksamkeit!