Privacy Support in iOS and OS X

Session 710

Erik Neuenschwander
Apple Product Security

Agenda

- UDID
- Data isolation
- New privacy UI
- Privacy practices

UDID

UDID

- API introduced in iPhone OS 2.0
- Deprecated in iOS 5
  - “Do not use the uniqueIdentifier property. To create a unique identifier specific to your app, you can call the CFUUIDCreate function to create a UUID, and write it to the defaults database using the NSUserDefaults class.”
- “But wait!!”

UDID → ?

- Three APIs

UDID → Application Identifier

- New API

```
[NSUUID UUID]
```

- Unique 128-bit value with no hardware details
- Different each time you call it
- Usable to uniquely identify something
- If saved in the app's defaults/preferences
  - Lifetime is app-install dependent
  - Backed up
  - Restored across devices

UDID → Vendor Identifier

- New API

```
[[UIDevice currentDevice] identifierForVendor]
```

- Provides a device-unique Identifier per Team ID
- Mapping stored and managed by iOS
- Erased with removal of the last app for that Team ID

UDID → Vendor Identifier

	Installed app count	Identifier
com.exampleSomeDev	3	53BDBF59-43E3-4B6E-A5C8-52F2102931BA
com.exampleOtherDev	1	BAC1966B-77DE-4F7B-9513-168BCF628058
com.exampleThirdDev	2	CBE2C854-D369-4B96-AF6A-AFF5F2756250

UDID → Vendor Identifier

	Installed app count	Identifier
com.exampleSomeDev	2	53BDBF59-43E3-4B6E-A5C8-52F2102931BA
com.exampleOtherDev	1	BAC1966B-77DE-4F7B-9513-168BCF628058
com.exampleThirdDev	2	CBE2C854-D369-4B96-AF6A-AFF5F2756250

UDID → Vendor Identifier

	Installed app count	Identifier
com.exampleSomeDev	1	53BDBF59-43E3-4B6E-A5C8-52F2102931BA
com.exampleOtherDev	1	BAC1966B-77DE-4F7B-9513-168BCF628058
com.exampleThirdDev	2	CBE2C854-D369-4B96-AF6A-AFF5F2756250

UDID → Vendor Identifier

	Installed app count	Identifier
com.exampleSomeDev	0	53BDBF59-43E3-4B6E-A5C8-52F2102931BA
com.exampleOtherDev	1	BAC1966B-77DE-4F7B-9513-168BCF628058
com.exampleThirdDev	2	CBE2C854-D369-4B96-AF6A-AFF5F2756250

UDID → Vendor Identifier

	Installed app count	Identifier
com.exampleOtherDev	1	BAC1966B-77DE-4F7B-9513-168BCF628058
com.exampleThirdDev	2	CBE2C854-D369-4B96-AF6A-AFF5F2756250

UDID → Vendor Identifier

	Installed app count	Identifier
com.exampleSomeDev	1	
com.exampleOtherDev	1	BAC1966B-77DE-4F7B-9513-168BCF628058
com.exampleThirdDev	2	CBE2C854-D369-4B96-AF6A-AFF5F2756250

UDID → Vendor Identifier

	Installed app count	Identifier
com.exampleSomeDev	1	02C3EBF3-2951-4D4E-8048-03A5C1FF6C79
com.exampleOtherDev	1	BAC1966B-77DE-4F7B-9513-168BCF628058
com.exampleThirdDev	2	CBE2C854-D369-4B96-AF6A-AFF5F2756250

UDID → Vendor Identifier

- New API

```
[[UIDevice currentDevice] identifierForVendor]
```

- Backed up
- Will not be restored onto a different device (like UDID)

UDID → Advertising Identifier

- New API

```
[[UIDevice currentDevice] identifierForAdvertising]
```

- Unique to the device
- Available to all applications
- Used for advertising
  - iAd has converted from UDID for iOS 6 and later
- Forgotten with Erase All Content & Settings
- Backed up
- Will not be restored onto a different device (like UDID)

UDID → New APIs

- Application Identifier

```
[NSUUID UUID]
```

- Vendor Identifier

```
[[UIDevice currentDevice] identifierForVendor]
```

- Advertising Identifier

```
[[UIDevice currentDevice] identifierForAdvertising]
```

UDID → New API

	Scope	Lifetime	Backed up	Restores across devices
Application ID	App	Uninstall app	Yes	Yes
Vendor ID	Developer	Uninstall developer's apps	Yes	No
Advertising ID	Device	Erase all Content and Settings	Yes	No

UDID → ~~UDID~~

- Replacement APIs available in iOS 6
- Begin your transition now
  - Build new apps on the new APIs
  - Transition existing apps when you submit updates
- UDID and similar identifiers will be disallowed in the future
  - Legacy behavior does not change
  - Existing installed applications will not be affected

Data Isolation

Data Isolation

- OS mediates between application and data
- Transparent to application
- Existing API trigger user consent

Data Isolation

Consent alerts

Data Isolation

- Application receives no data if denied
- User can manage permissions in iOS Settings/OS X System Preferences

Data Isolation

iOS 6 implementation

- Builds on top of the sandbox
- User permission gathered by iOS
- Access to data is disallowed without user permission
- If permissions changes, app is quit
  - Background task expiration handler is called, if registered
  - iOS then kills the application

Data Isolation

Mountain Lion implementation

- For purpose-specific API, user permission gathered by OS X
- Aid to developers
- If permission changes, user can choose to quit the app
- Sandboxed apps must also pass sandbox check

Data Isolation

Current support

- Location services

Data Isolation

New support

- Contacts (both iOS 6 and OS X Mountain Lion)
- Calendars
- Reminders
- Photos

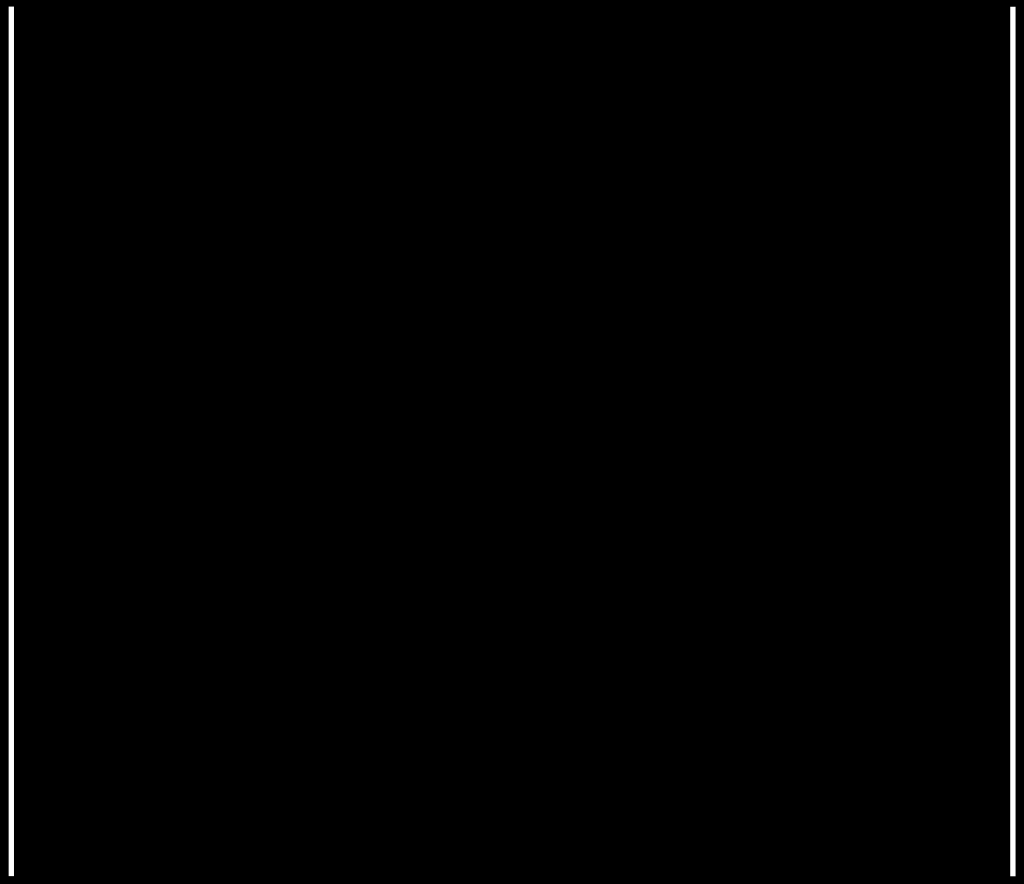
Data Isolation

New support

- Applies to existing applications
  - No resubmission, recompilation
- Changes can improve user experience

(No) Data Isolation

How it works today



(No) Data Isolation

How it works today

(No) Data Isolation

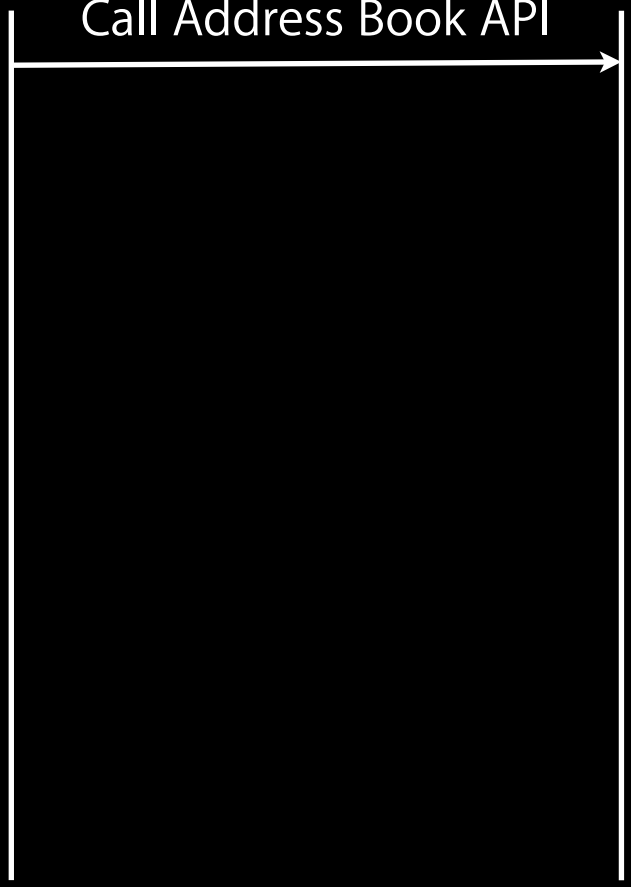
How it works today

Data Isolation

Contacts on Mountain Lion

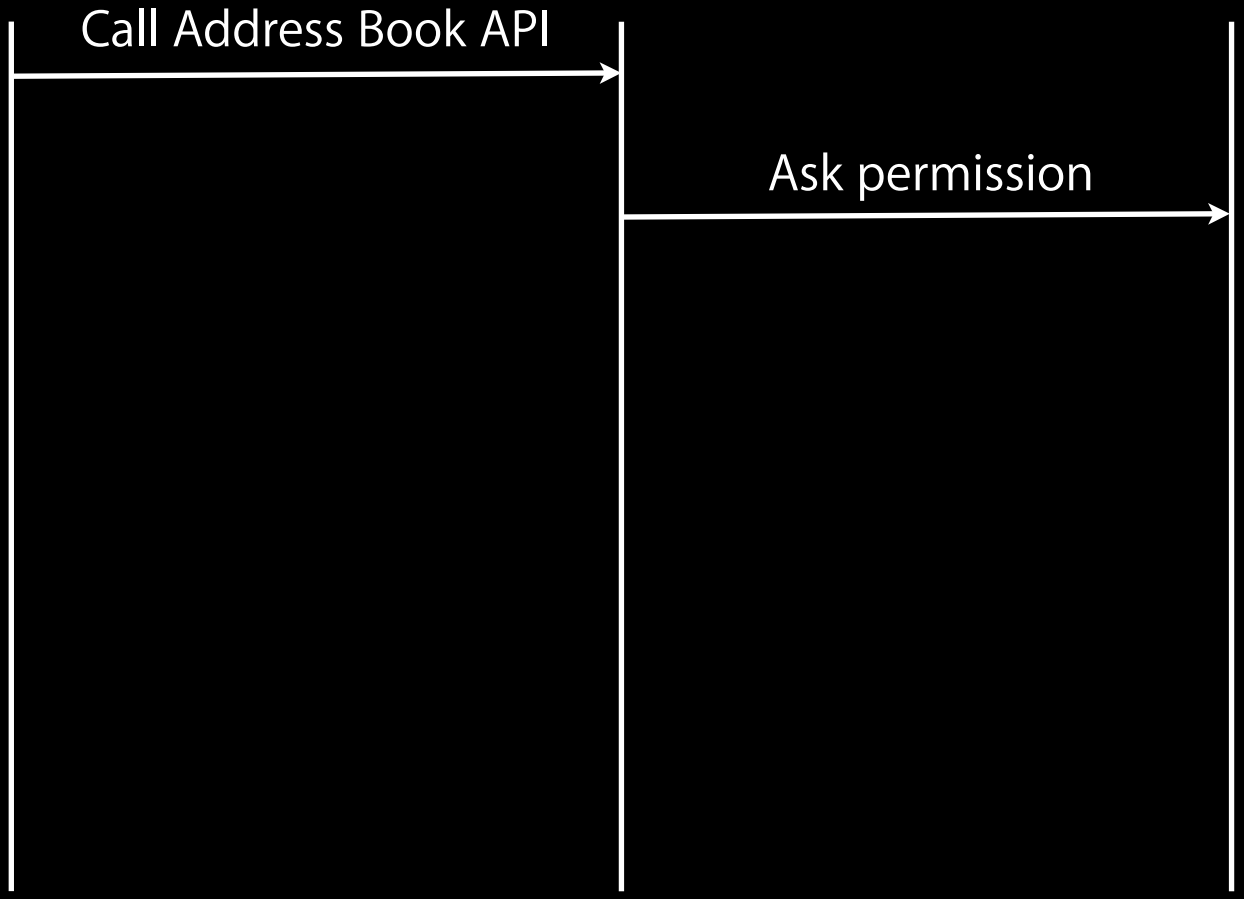
Data Isolation

Contacts on Mountain Lion



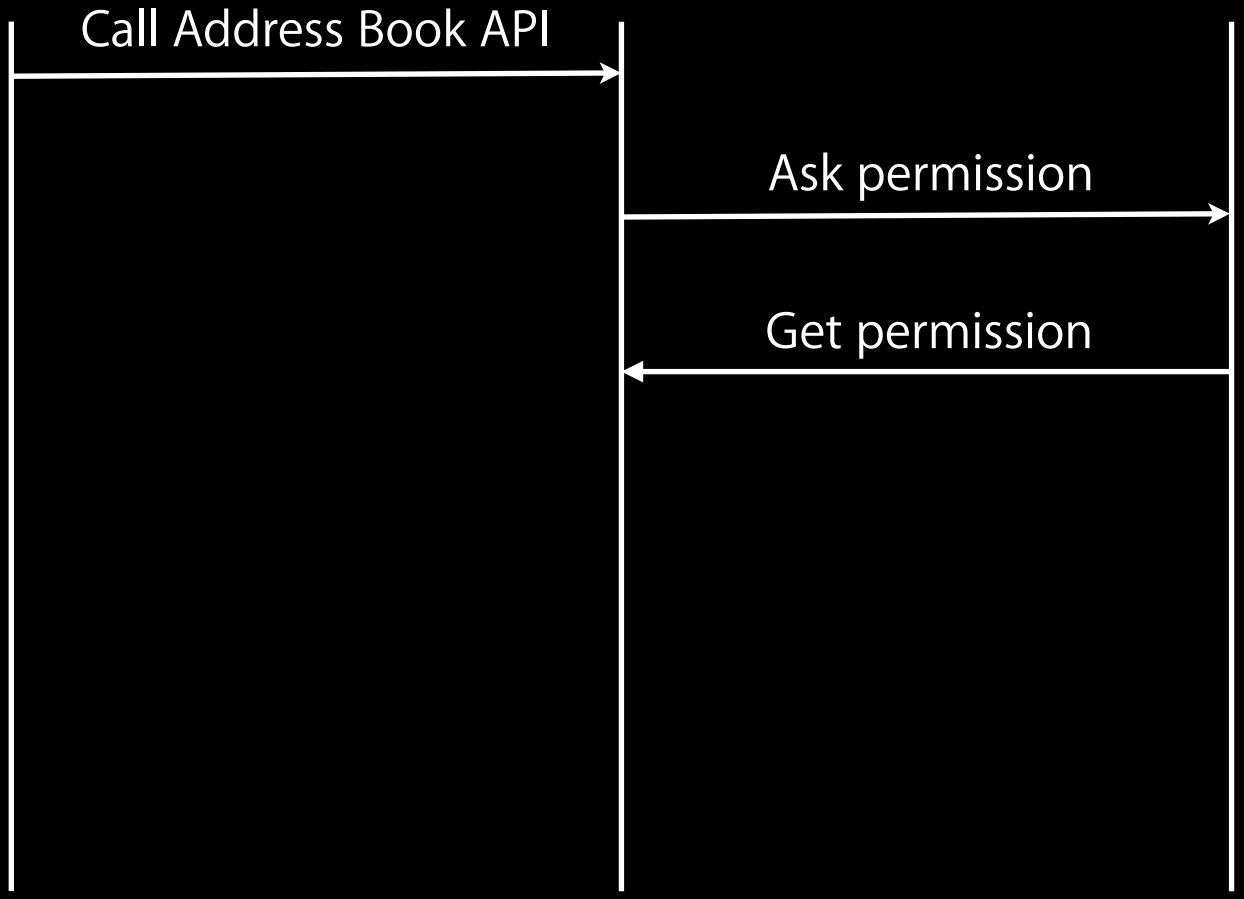
Data Isolation

Contacts on Mountain Lion



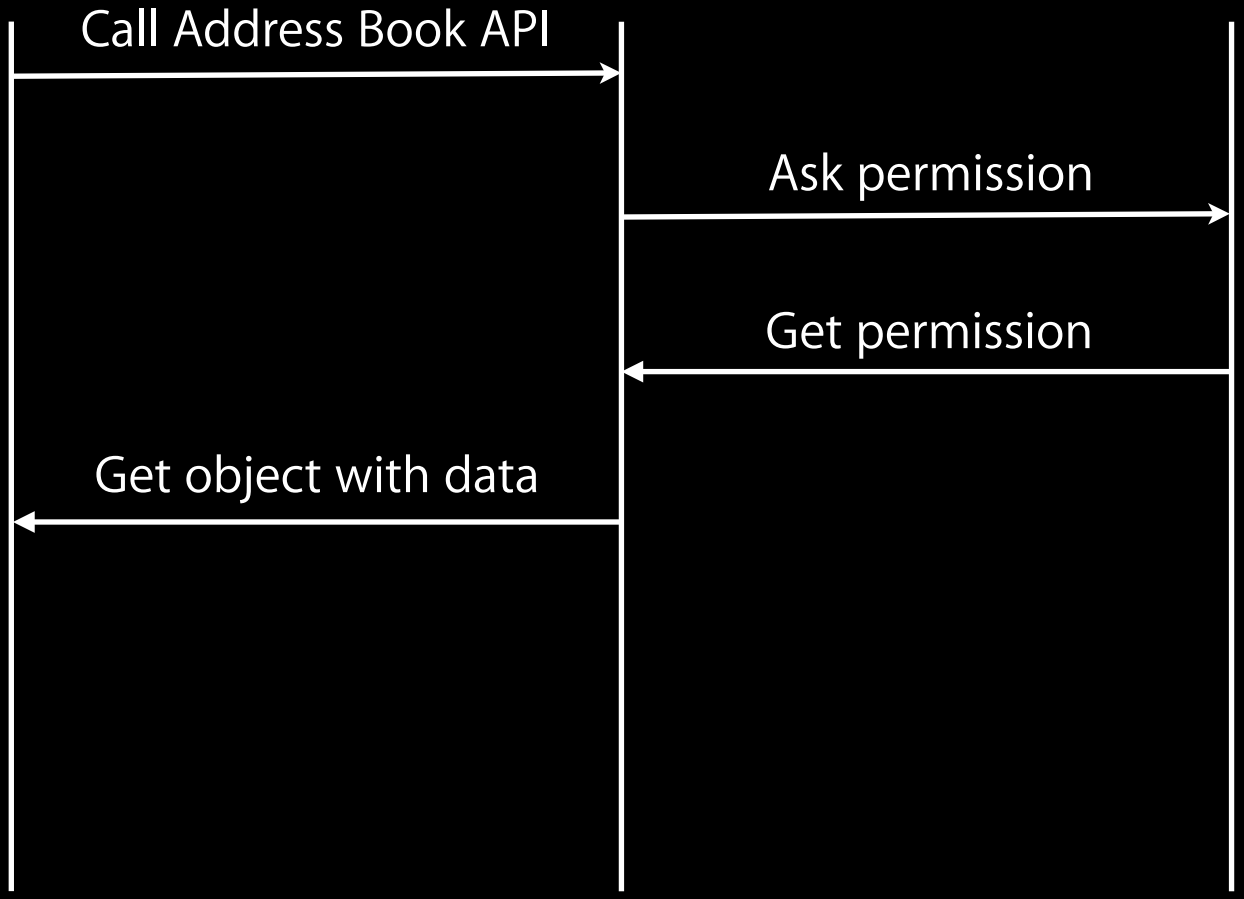
Data Isolation

Contacts on Mountain Lion



Data Isolation

Contacts on Mountain Lion



Data Isolation

Contacts on Mountain Lion

- For purpose-specific API, user permission gathered by OS X
  - Address Book framework

```
[ABAddressBook sharedAddressBook]
[[ABPerson alloc] init]
...
```

- Call blocks while permission is requested from the user
  - Wrap in a dispatch block

Data Isolation

Contacts on Mountain Lion

- Granted access: populated object
- Denied access: nil return value
- For explicit data access, user permission gathered by OS X
  - Sync Services
  - Spotlight
  - Apple Script

Data Isolation

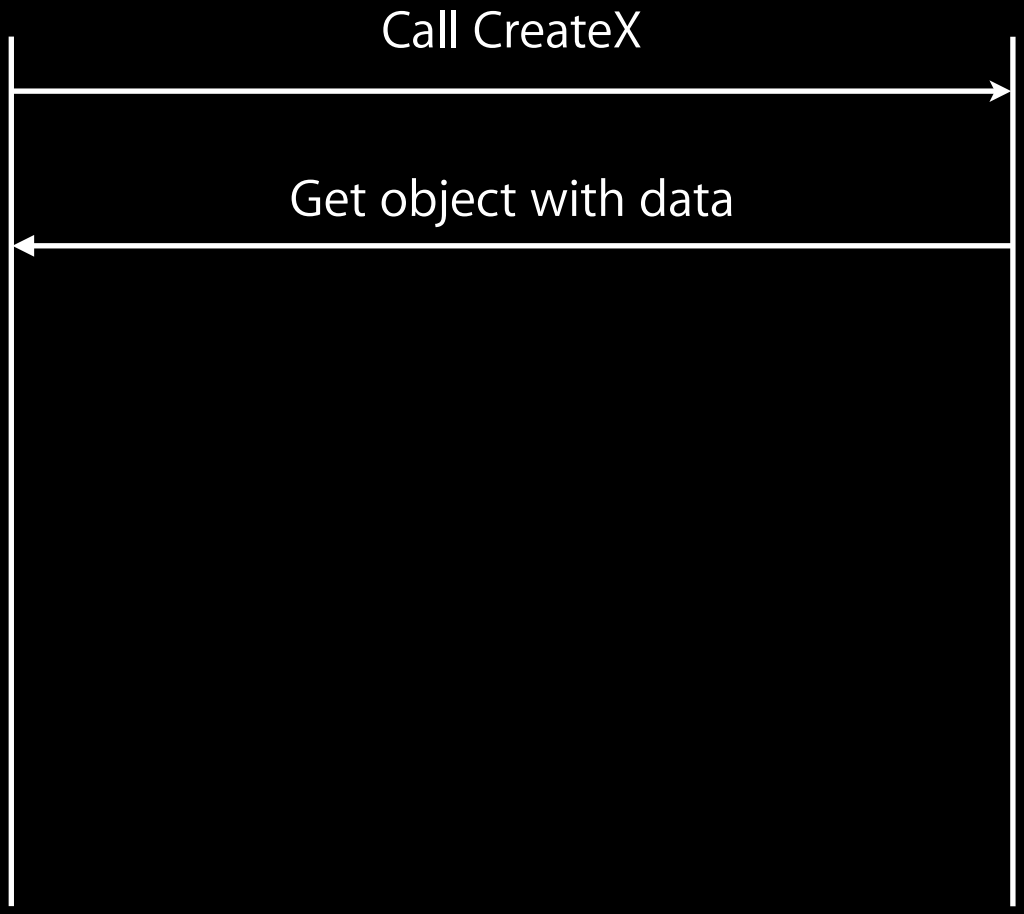
Contacts on Mountain Lion

- Sandboxed apps have additional checks
  - Address Book is outside the sandbox
- Access is disallowed without proper entitlement
  - Build with just the entitlements you need

    `com.apple.security.personal-information.addressbook`
  - “Allow Address Book Data Access” in Xcode UI
- Sandbox check occurs before permission check

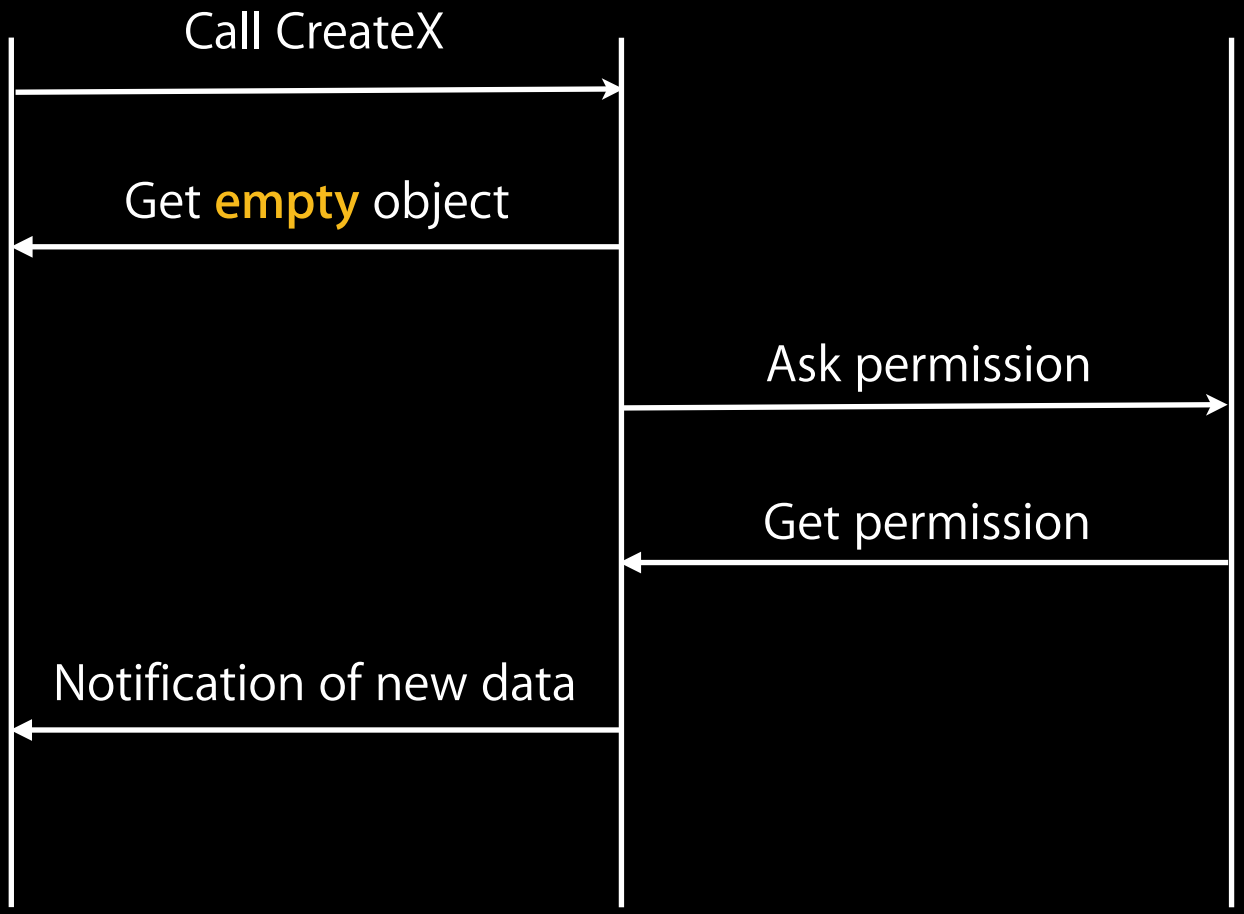
(No) Data Isolation

How it works today



Data Isolation

iOS



Data Isolation

iOS

- Initial access will synchronously return
- Access permission will come later
- Need to handle change notifications
  - Was always a good idea anyway

Data Isolation

Access checks

- Query your app's status for any supported data class
  - Can be done before you attempt access
- New API in iOS 6
  - Not present in the seed you have
- Will return four possible states
  - not determined
  - granted
  - denied (explicitly by the user)
  - restricted (may be due to Restrictions being enabled)

Data Isolation

iOS

- Contacts
- Calendars
- Reminders
- Photos

Data Isolation

Contacts

- Access to ABAddressBookRef is managed

```
ABAddressBookCreate()
```

Data Isolation

Contacts

- Access to ABAddressBookRef is managed

```
~~ABAddressBookCreate()~~
ABAddressBookCreateWithOptions(options, &error)
```

  - options parameter reserved for future use
  - error indicates if access was previously denied
  - deprecated API still gathers user permission

Data Isolation

Contacts

- Initially access is not determined
  - ABAddressBookCreateWithOptions returns empty read-only object
- Register it with ABAddressBookRegisterExternalChangeCallback
- In your callback, update it by calling ABAddressBookRevert

Data Isolation

Contacts

- Returned Address Book may be a nil object
  - True if permission was previously denied
  - Adding entries to a nil object will not be useful
- Returned Address Book may have no entries
  - True if permission is still pending
  - Two-way sync against this “empty” list may be undesirable
- Test all the possibilities

Data Isolation

Calendars

- Access to EKEventStore is managed

```
[EKEventStore init]
```

Data Isolation

Calendars

- Access to EKEventStore is managed

```
~~[EKEventStore init]~~
[EKEventStore initWithAccessToEntityTypes:EKEntityMaskEvent]
```

Data Isolation

Calendars

- Access to EKEventStore is managed

```
~~[EKEventStore init]~~
[EKEventStore initWithAccessToEntityTypes:EKEntityMaskEvent]
```

Data Isolation

Reminders

- Very similar to Calendar events
- Also part of EventKit
- use `EKEntityMaskReminder` instead of `EKEntityMaskEvent`

```
[EKEventStore initWithAccessToEntityTypes:EKEntityMaskReminder]
```

Data Isolation

Photos

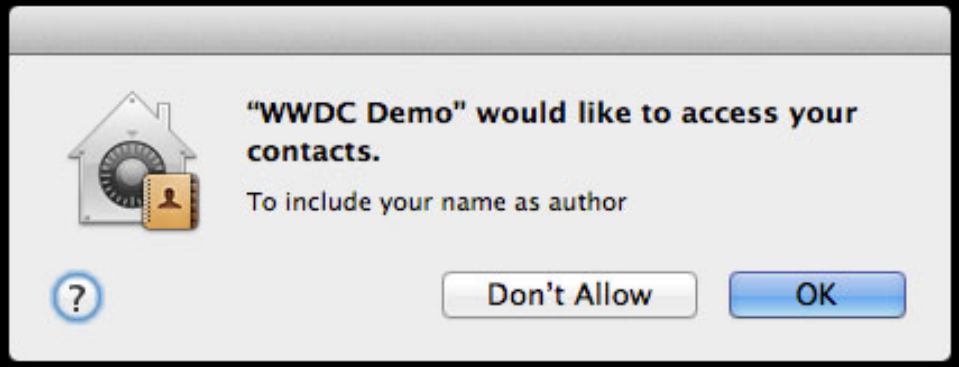
- Access to ALAssetsLibrary is not managed
- Calling one of the get or set methods is managed
- Example

```
-[ALAssetsLibrary enumerateGroupsWithTypes:usingBlock:failureBlock:]
```

  - failureBlock will be called if denied access
- Photos include all metadata

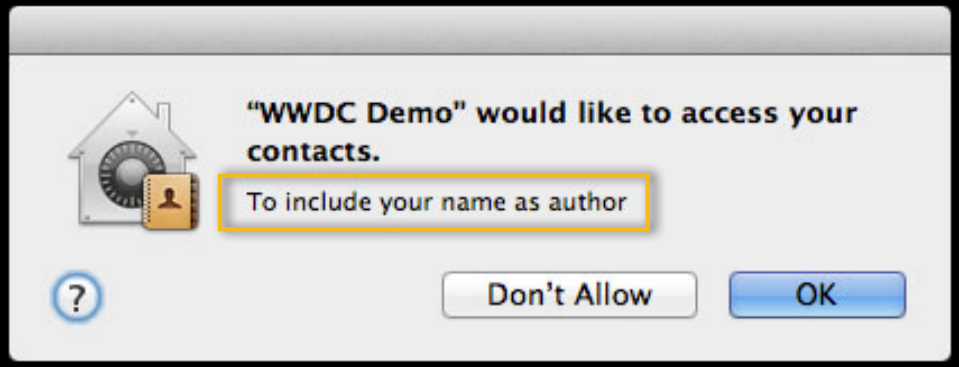
Data Isolation

Consent Alerts



Data Isolation

Purpose String



Data Isolation

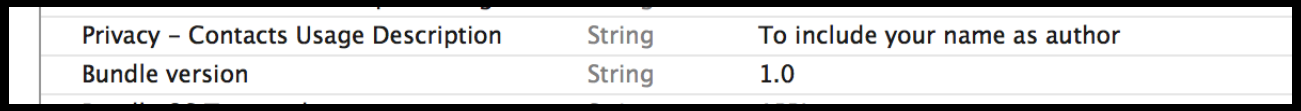
Conveying purpose

- Each permissions dialog supports a developer-specified purpose
- Optional, highly encouraged
- One purpose per kind of data
- Set in your app's Info.plist
  - Use Info tab of in Xcode's Project editor
- Look for "Privacy - " keys and provide a value
  - e.g. "Privacy - Photo Library Usage Description"
  - One provided for each kind of data

Data Isolation

Conveying purpose

- Look for "Privacy - " keys and provide a value
  - e.g. "Privacy - Contacts Usage Description"
  - One provided for each kind of data



Data Isolation

Testing on OS X

- Just run your app
- Apps can only trigger the prompt once
  - tccutil reset AddressBook (man tccutil for more info)
- Test all cases
  - Permission previously denied
  - Permission being sought and granted
  - Permission being sought and denied
- Fail gracefully

Data Isolation

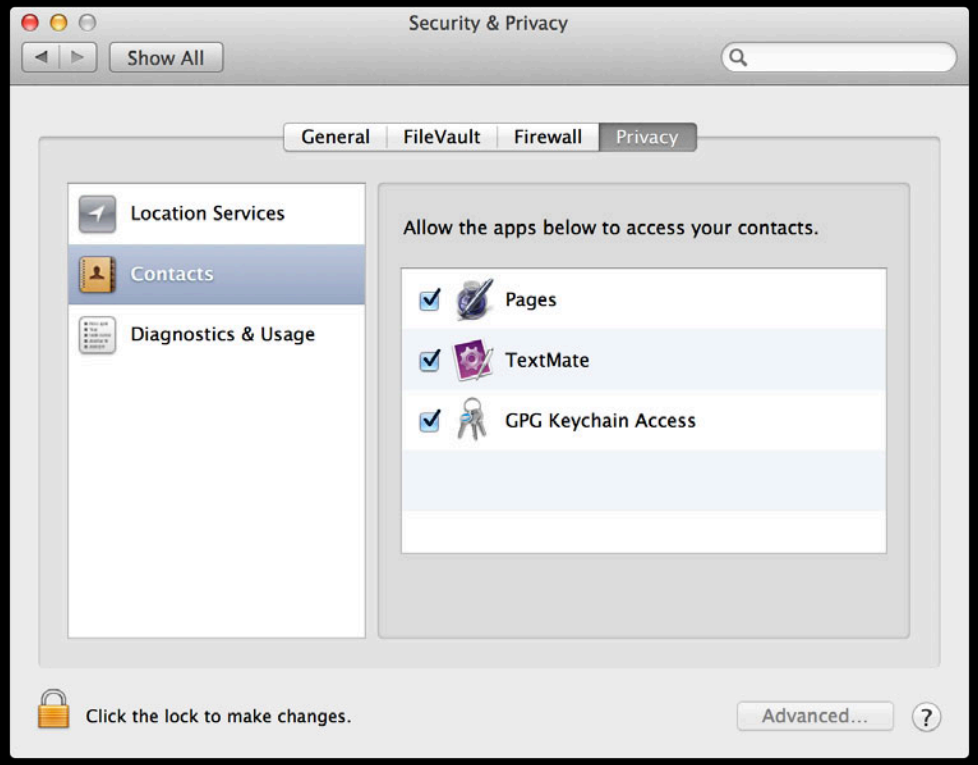
Testing on iOS

- Isolation is not supported in the iOS Simulator
  - Test on the device
- Apps can only trigger the prompt once
  - Settings > General > Reset > Reset Location & Privacy
- Test all cases
  - Permission previously denied
  - Permission being sought and granted
  - Permission being sought and denied
  - Permission restricted
- Fail gracefully

New Privacy UI

New Privacy UI

User control



New Privacy UI

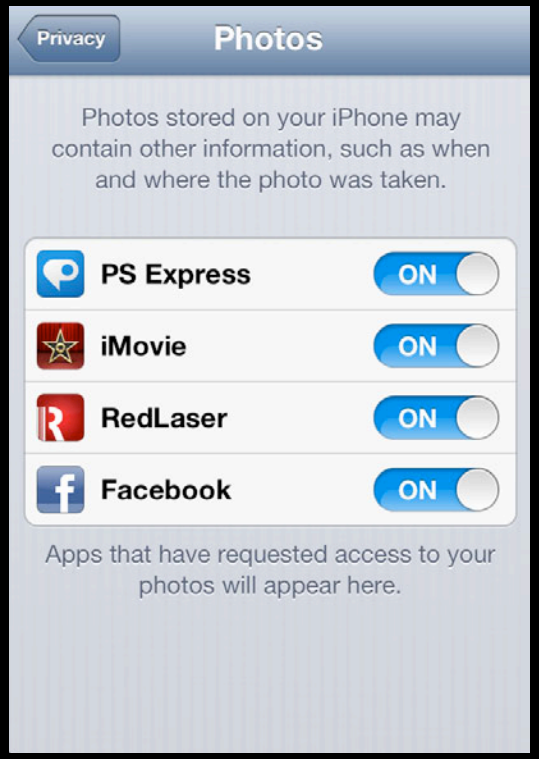
User control

New Privacy UI

User control

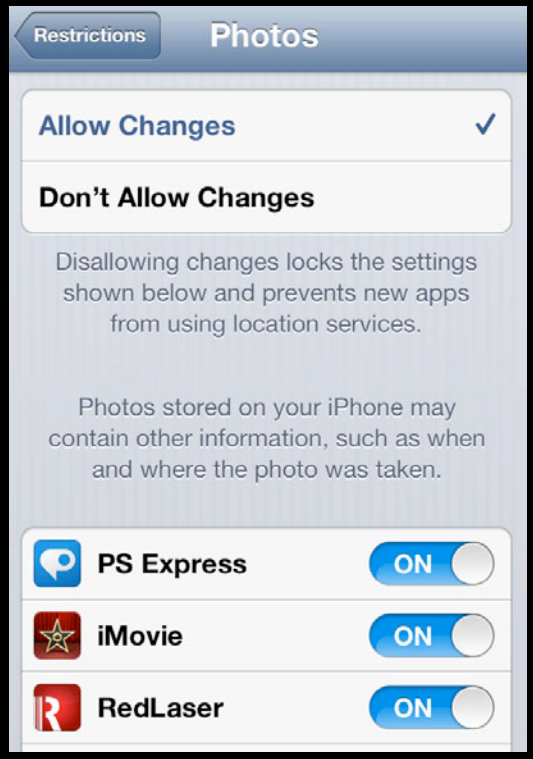
New Privacy UI

User control



New Privacy UI

User control



Best Practices

Best Practices

- Transparency
- Control
- Data collection techniques

Best Practices

Transparency

- Privacy policy or statement
  - Important to have one
  - Can submit a link to Apple in iTunes Connect
  - Link visible on the App Store in a future release
- Give user opportunities to inspect data

Best Practices

Control

- Ask for permission with context
- Explain your purpose
- Ask at the time you need it
  - Just-in-time notice provides additional context
  - Bad idea: Everything right at launch time
- Allow post hoc changes
- Fail gracefully

Best Practices

Data collection techniques

- All collection efforts reduce privacy
  - Does not entail any collection is bad/evil/wrong/misguided
- Within the positive of your collection, minimize the negative
- True both for apps and servers
- Holding on to rich data has risks

Best Practices

Collection techniques

- Anonymize
- Aggregate
- Sample
- De-resolve
- Decay
- Minimize

Best Practices

Anonymize

Best Practices

Anonymize

- Initial log: `<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"`

Best Practices

Anonymize

- Initial log: `<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"`
- Better: `<Error>: Illegal token in “FY2013.keynote”`

Best Practices

Anonymize

- Initial log: `<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"`
- Better: `<Error>: Illegal token in “FY2013.keynote”`
- Even Better: `<Error>: Illegal token in com.apple.keynote file`

Best Practices

Aggregate

Best Practices

Aggregate

- Initial log: `<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"`

Best Practices

Aggregate

- Initial log: `<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"`
- Better: `<Error>: Illegal tokens {com.apple.keynote: 21; com.foo.doc: 3}`

Best Practices

Sample

Best Practices

Sample

- Initial log: `<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"`

Best Practices

Sample

- Initial log: `<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"`
- Better: Collect data from only 1 computer in 10 (or 100, or more)

Best Practices

Sample

- Initial log: `<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"`
- Better: Collect data from only 1 computer in 10 (or 100, or more)
- Even Better: Collect data from only 1 operation in 10 (or 100...)

Best Practices

De-resolve

Best Practices

De-resolve

- Initial log: `<Info>: May  4 15:03:19: Action succeeded, processed 22341 bytes`

Best Practices

De-resolve

- Initial log: `<Info>: May  4 15:03:19: Action succeeded, processed 22341 bytes`
- Better: `<Info>: May  4 15:00: Action succeeded, processed 22 kB`

Best Practices

De-resolve

- Initial log: `<Info>: May  4 15:03:19: Action succeeded, processed 22341 bytes`
- Better: `<Info>: May  4 15:00: Action succeeded, processed 22 kB`
- Better: `<Info>: Friday 15:00: Action succeeded, processed 20 kB`

Best Practices

Decay

Best Practices

Decay

- Initial log: `<Info>: May  4 15:03:19: Action succeeded, processed 22341 bytes`

Best Practices

Decay

- Initial log: `<Info>: May  4 15:03:19: Action succeeded, processed 22341 bytes`
- After 7 days: `<Info>: May  4: Action succeeded, processed 22341 bytes`

Best Practices

Decay

- Initial log: `<Info>: May  4 15:03:19: Action succeeded, processed 22341 bytes`
- After 7 days: `<Info>: May  4: Action succeeded, processed 22341 bytes`
- After 30 days: `<Info>: [Redacted]: Action succeeded, processed 22 kB`

Best Practices

Minimize

Best Practices

Minimize

- Initial log: `<Info>: May  4 15:03:19: Action succeeded, processed 22341 bytes`

Best Practices

Minimize

- Initial log: `<Info>: May  4 15:03:19: Action succeeded, processed 22341 bytes`
- Better:

Best Practices

Techniques

- Anonymize
- Aggregate
- Sample
- De-resolve
- Decay
- Minimize

Takeaway Points

Takeaway Points

- Discontinue use of UDID API
  - Adopt the replacements
- Test all cases of Data Isolation access
  - Fail gracefully
- Add Purpose Strings to your app's Info
- Submit a privacy statement link to the App Store
- Make sure users know what you're collecting and can control it
- Collect only what data you need


WWDC2012