iOS DEVICE AND APP TRUST EVALUATION

Lecture 17b

COMPSCI 702

Security for Smart-Devices

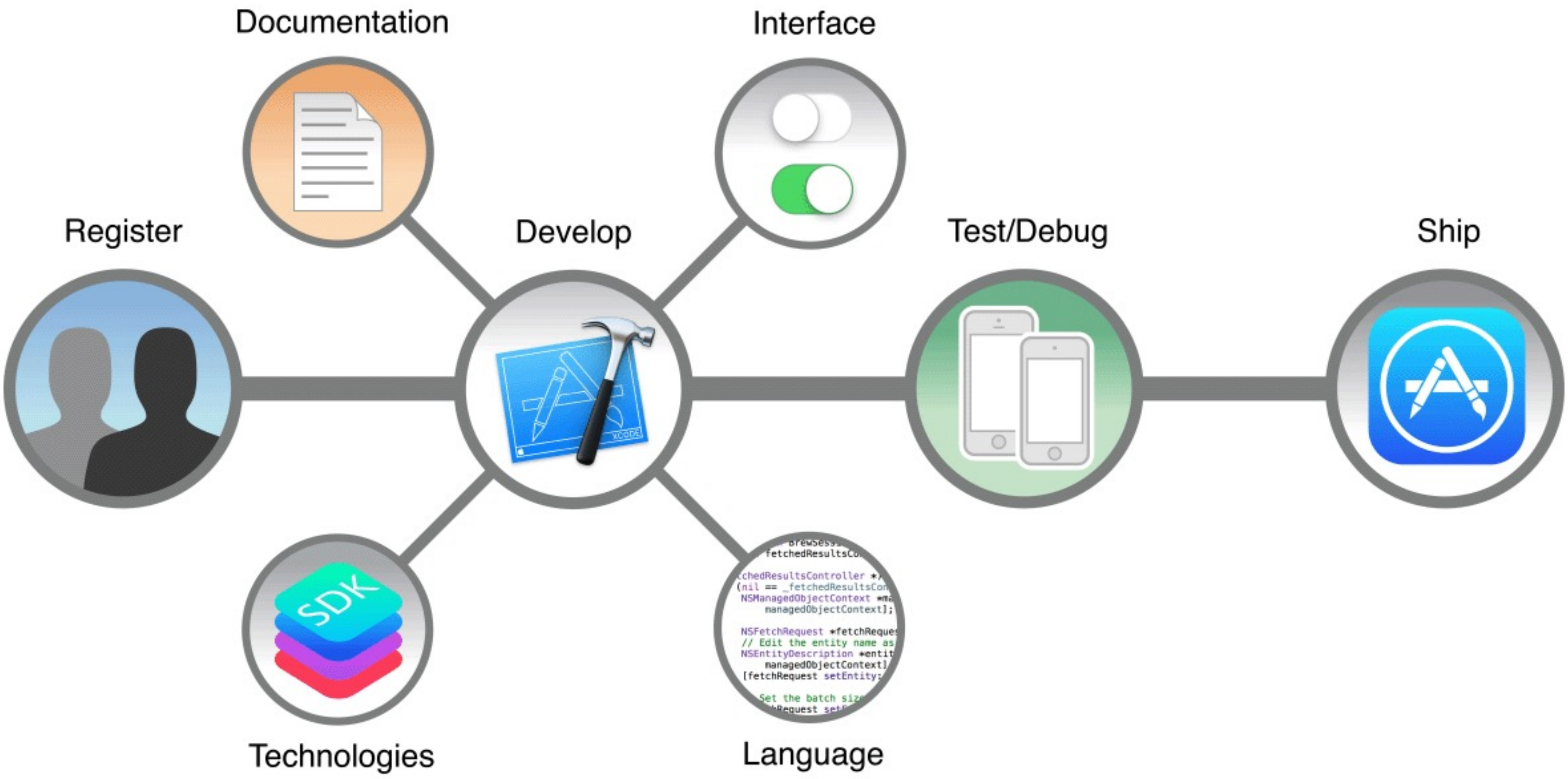
Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

April 21, 2021

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

iOS APP DEVELOPMENT LIFECYCLE



Documentation

Interface

Register

Develop

Test/Debug

Ship

Technologies

Language

```
    BrewSess
    fetchedResultsCo

tchedResultsController *
(nil == _fetchedResultsCon
 NSManagedObjectContext *ma
      managedObjectContext];

 NSFetchRequest *fetchReques
 // Edit the entity name as
 NSEntityDescription *entit
      managedObjectContext]
 [fetchRequest setEntity:

   Set the batch size
   hRequest set
```

HOW DOES iOS VERIFY THAT IT CAN RUN AN APP?

- The app submission to app store
  - Accepted apps are signed by Apple
  - Only signed apps are installed
- The device checks certificate and signature before running the app
- App code and memory continually checked as it runs

iOS APP TESTING

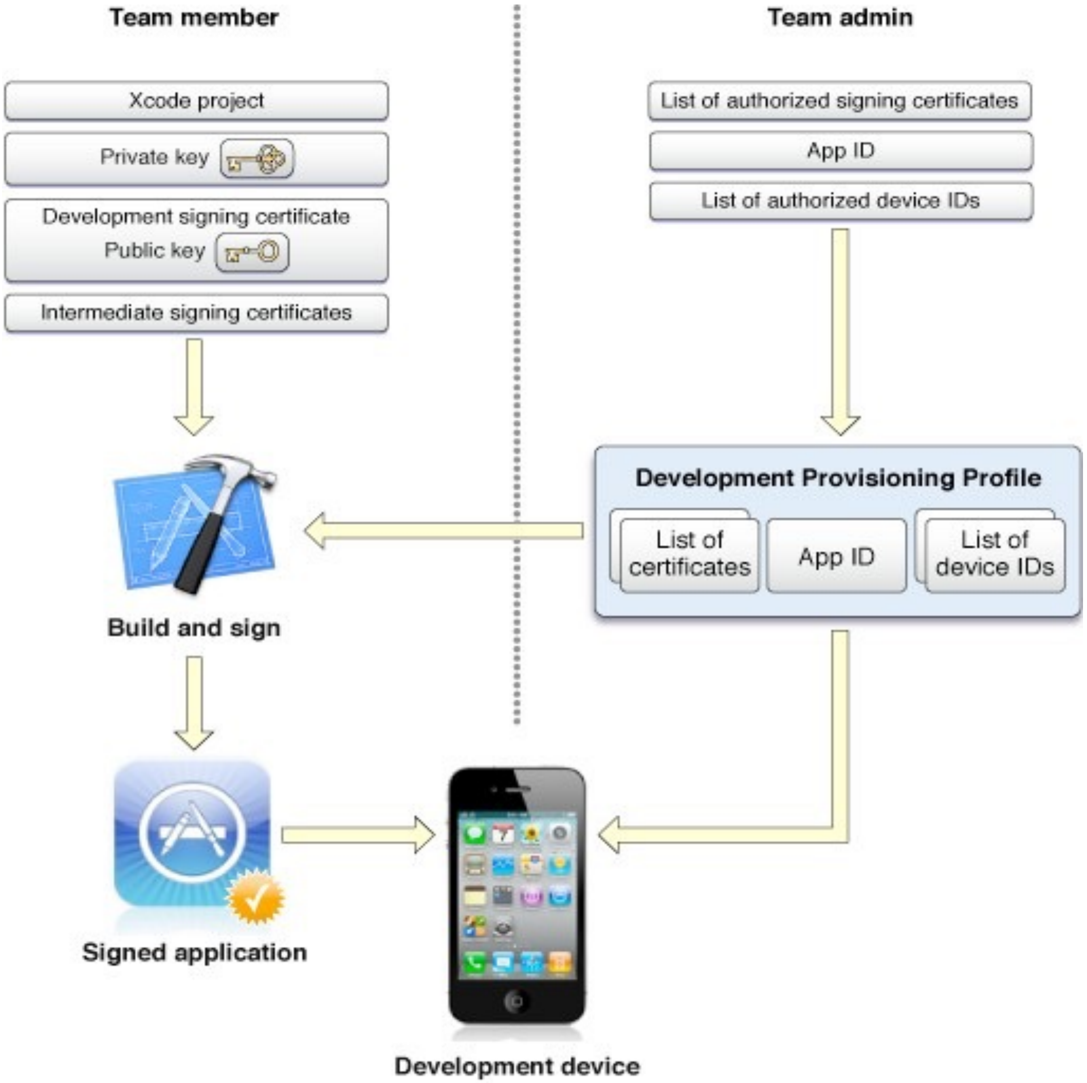
- If signing is always required, how can an app developer test or debug a newly developed app?

iOS APP DEVELOPMENT: XCODE

- Developers can develop apps using Xcode
  - An IDE provided by Apple
  - Current version 8.3, released in March 2017
  - To have the app signed by Apple
  - Or to run it on a device requires a provisioning profile to be installed on the device for that app

- The developer must get a certificate from Apple

iOS APP DEVELOPMENT


Team member
Team admin
Xcode project
Private key
Development signing certificate
Public key
Intermediate signing certificates
List of authorized signing certificates
App ID
List of authorized device IDs
Development Provisioning Profile
List of certificates
App ID
List of device IDs
Build and sign
Signed application
Development device

WHAT IS A PROVISIONING PROFILE?

- An XML property list (plist)
  - Which **app**
    - App ID – some random characters followed by the company ID and app name
  - Which **devices**
    - Each device has a Unique Device ID (UDID)
      - Usually a 40-char HEX string
  - For development, trust is based on the developer’s certificate, which is in the profile
- It configures a device to allow the execution of signed code
  - Installed on a device only if the device ID is in the profile

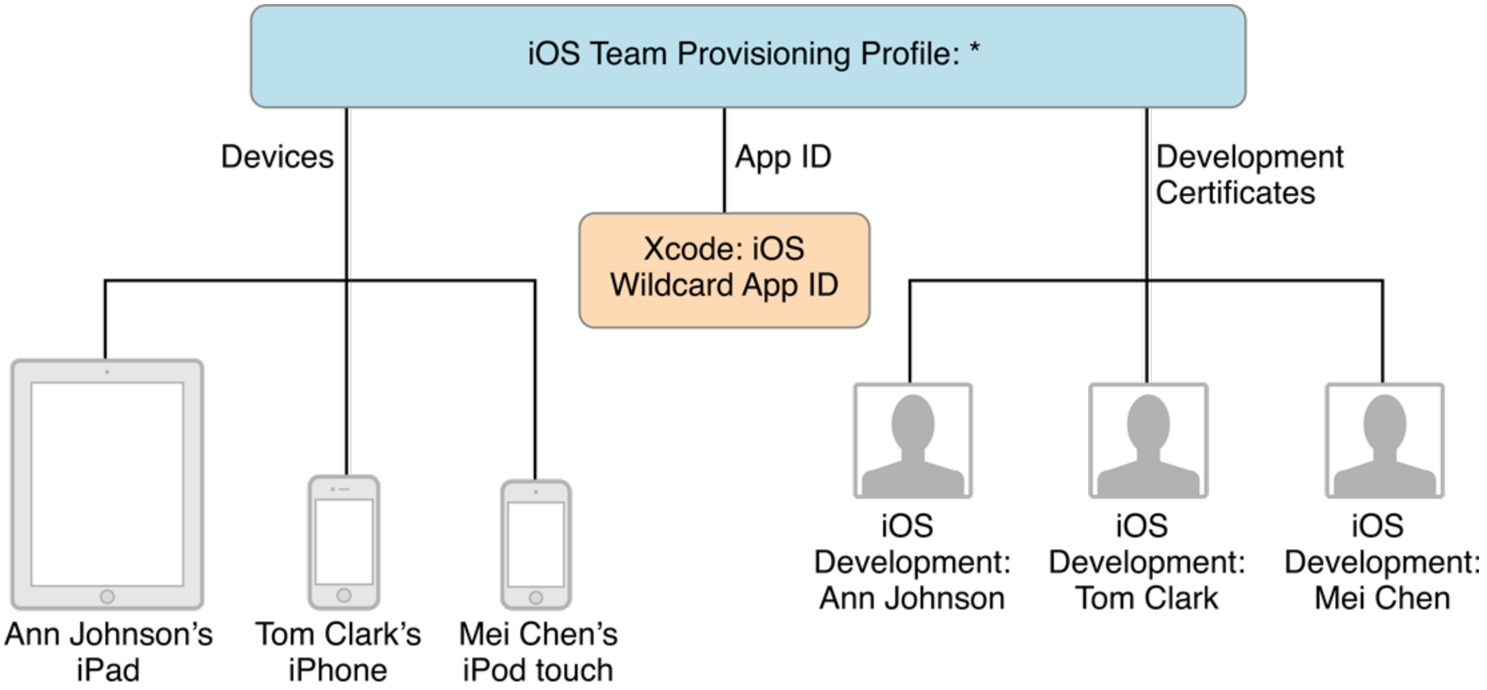
ENTITLEMENTS

- Profiles also include entitlements
  - Adding policies regarding what an app can do
  - Or allow debugging

- Apple can add entitlements to limit functionality

- Stored in a property list

TEAM PROVISIONING PROFILES


iOS Team Provisioning Profile: *
Devices
App ID
Development Certificates
Xcode: iOS Wildcard App ID
Ann Johnson's iPad
Tom Clark's iPhone
Mei Chen's iPod touch
iOS Development: Ann Johnson
iOS Development: Tom Clark
iOS Development: Mei Chen

Source: developer.apple.com

APPLE DEVELOPER PROGRAM: TEAM ROLES

- Team agent
- Team admin
- Team member

TEAM AGENT

- Legally responsible for the team
- Acts as the initial primary contact with Apple
- Can invite team members and change the access level of any other team member
- There is only one team agent

TEAM ADMIN

- Can set the privilege levels of other team members
  - Except the team agent

- Manages all assets used to sign your apps
  - Either during development or when your team is ready to distribute an app

TEAM MEMBER

- Can create her development certificate
- Register a device connected to her Mac
- Create a team provisioning profile using Xcode
- Cannot register devices

APPLE DEVELOPER PROGRAM: ROLES AND PRIVILEGES

Privilege	Team agent	Team admin	Team member
Accept legal agreements	✓	×	×
Renew membership	✓	×	×
Create Developer ID certificates	✓	×	×
Invite members and assign roles	✓	✓	×
Create distribution certificates	✓	✓	×
Create development provisioning profiles	✓	✓	✓

Source: developer.apple.com

MEMBERSHIP TYPES

- Individuals
  - Apple Developer Program
    - 99 USD per membership year
- Organisations
  - Apple Developer Program
    - 99 USD per membership year
  - Apple Developer Enterprise Program
    - 299 USD per membership year
- Educational Institutions
  - iOS Developer University Program
    - Free

MEMBERSHIP BENEFITS

Resources	Sign in with Apple ID	Individual	Organisation	Enterprise Program
Xcode Developer Tools	✓	✓	✓	✓
Test on Device	✓	✓	✓	✓
App Store Distribution		✓	✓	
In-house App Distribution				✓
Team Management			✓	✓
App Analytics		✓	✓	
Cost	Free	99 USD	99 USD	299 USD

Source: developer.apple.com

APP STORE DEPLOYMENT

- Apple certifies and signs the app bundle (executable, resources, etc.)
  - App ID
  - No device information
  - Trust is based on Apple's certificate
    - iOS ships with root anchors for certificate chains

- Because Apple checks the app before distribution, it acts like an antivirus program
  - That is why, there is no need for anti-virus apps in iOS

CERTIFICATE REVOCATION

- Apple supports revocation through
  - Certificate Revocation List (CRL)
    - Go to server and get a list of revoked certificates
  - Or Online Certificate Status Protocol (OCSP)
    - A server tells if a certificate is still valid

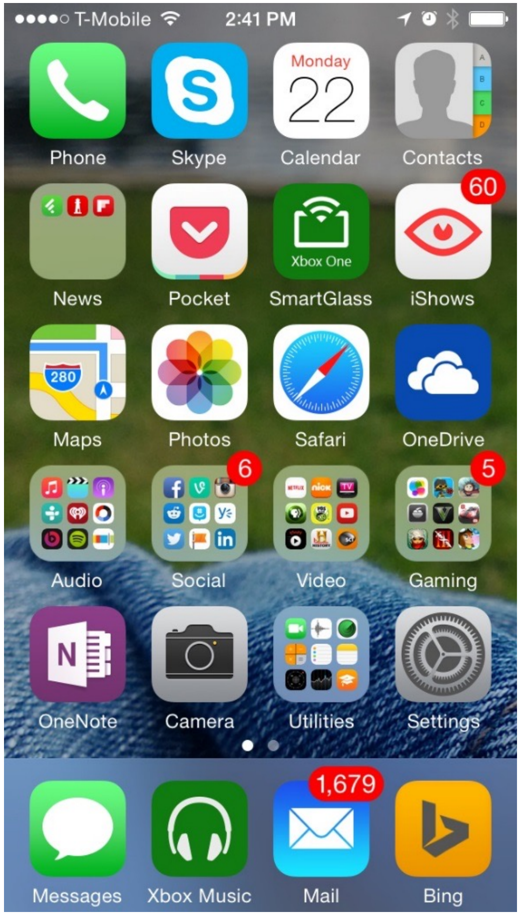
VALIDATING A PROVISIONING PROFILE

- The signing certificate is signed by Apple
  - It is called “Apple iPhone OS Provisioning Profile Signing”

- The certificate signing chain is no longer than three links
  - Development
    - Developer – Apple Worldwide Developer Relations CA – Apple Root CA
  - Deployment on app store
    - Apple iPhone OS Application Signing – Apple iPhone CA – Apple Root CA

APPS WITH THE DEVICE

- Actually with the OS
- Do not have to have a signature
  - The binary's hash is stored in the iOS kernel in the static trust cache



AT INSTALLATION

- Apps have a signature and certificate
  - Certificate must originate from Apple
  - The installer generates a message digest from the app (hash value)
  - The public key in the certificate is used to check that the digest and signature match

CODE SIGNING

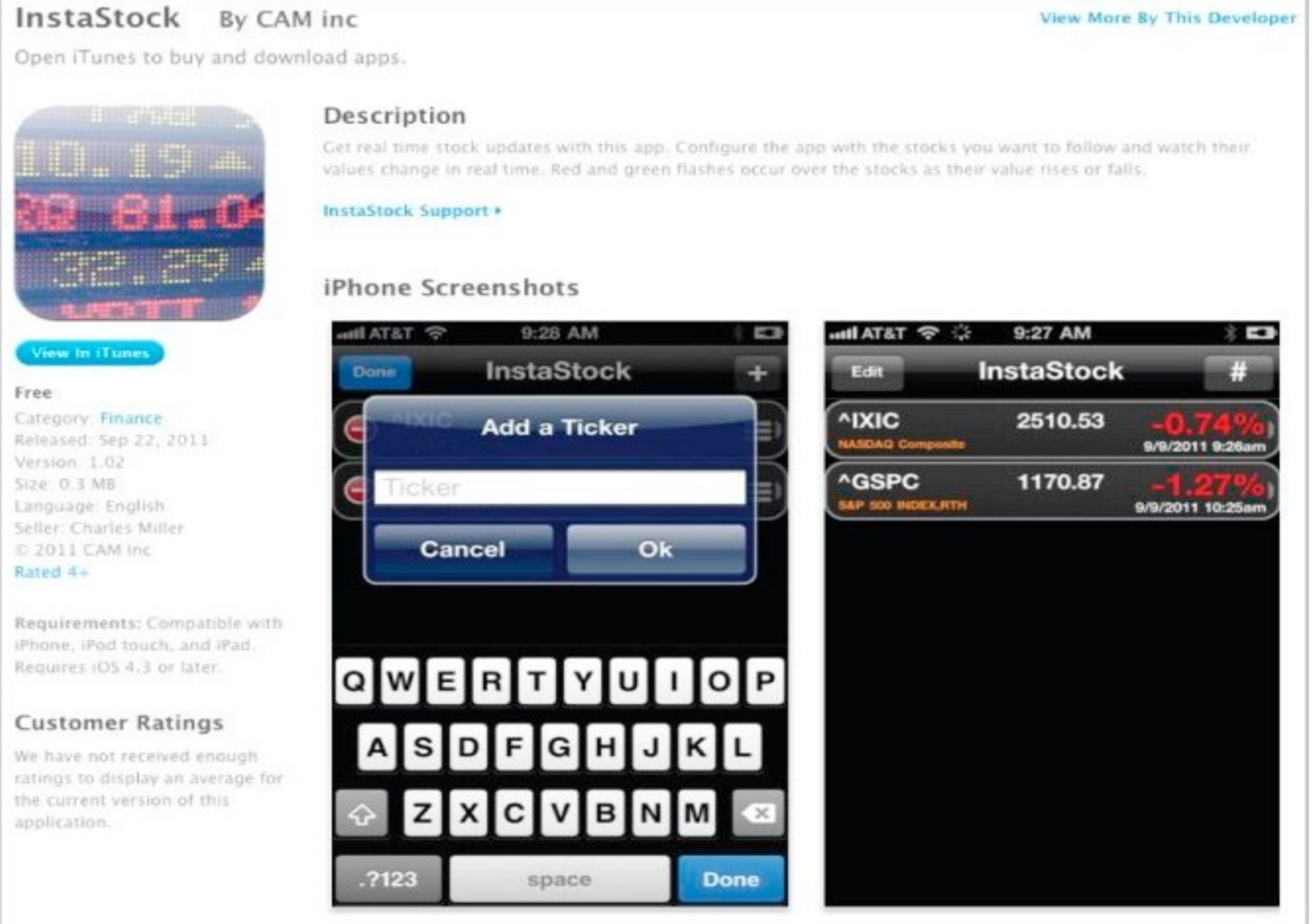
- Code signing is mandatory
  - Cannot install an app without it being correctly signed
- Code Signing Enforcement (CSE)
  - Ensures that the code has not been modified when running
  - Only valid code can be executed
  - Cannot be turned off (unless jailbroken)
  - Better than Data Execution Prevention (DEP)

VERIFYING SIGNING ON THE RUN

- Done in the virtual memory system
  - “dirty bit” – means page has been modified
- When an executable is loaded
  - The signature is loaded and checked
    - Is it in the static trust cache?
      - No – calls a function to check the signature

DATA EXECUTION PREVENTION (DEP)

- Executable pages are not writeable
  - W ^ X
- Prevents code modification
  - Uses the ARM NX bit on pages (never execute)
- Prevents dynamic production of code
  - Except the Mobile Safari JIT code
- All page requests and permission changes are checked



InstaStock By CAM inc

View More By This Developer

Open iTunes to buy and download apps.

Description

Get real time stock updates with this app. Configure the app with the stocks you want to follow and watch their values change in real time. Red and green flashes occur over the stocks as their value rises or falls.

InstaStock Support ▸

iPhone Screenshots

View In iTunes

Free

Category: Finance
Released: Sep 22, 2011
Version: 1.02
Size: 0.3 MB
Language: English
Seller: Charles Miller
© 2011 CAM Inc
Rated 4+

Requirements: Compatible with iPhone, iPod touch, and iPad. Requires iOS 4.3 or later.

Customer Ratings

We have not received enough ratings to display an average for the current version of this application.

This is the app by **Charles Miller** who created a writable executable area of memory then patched a copy of the dynamic linker to allow unsigned libraries to be run. It then connected to his website and could install any libraries he wanted. He did it to test the App Store review process. He **was kicked out of the Apple developers' program.**

TO BE CONTINUED

- See the next lecture

Questions?

Thanks for your attention!