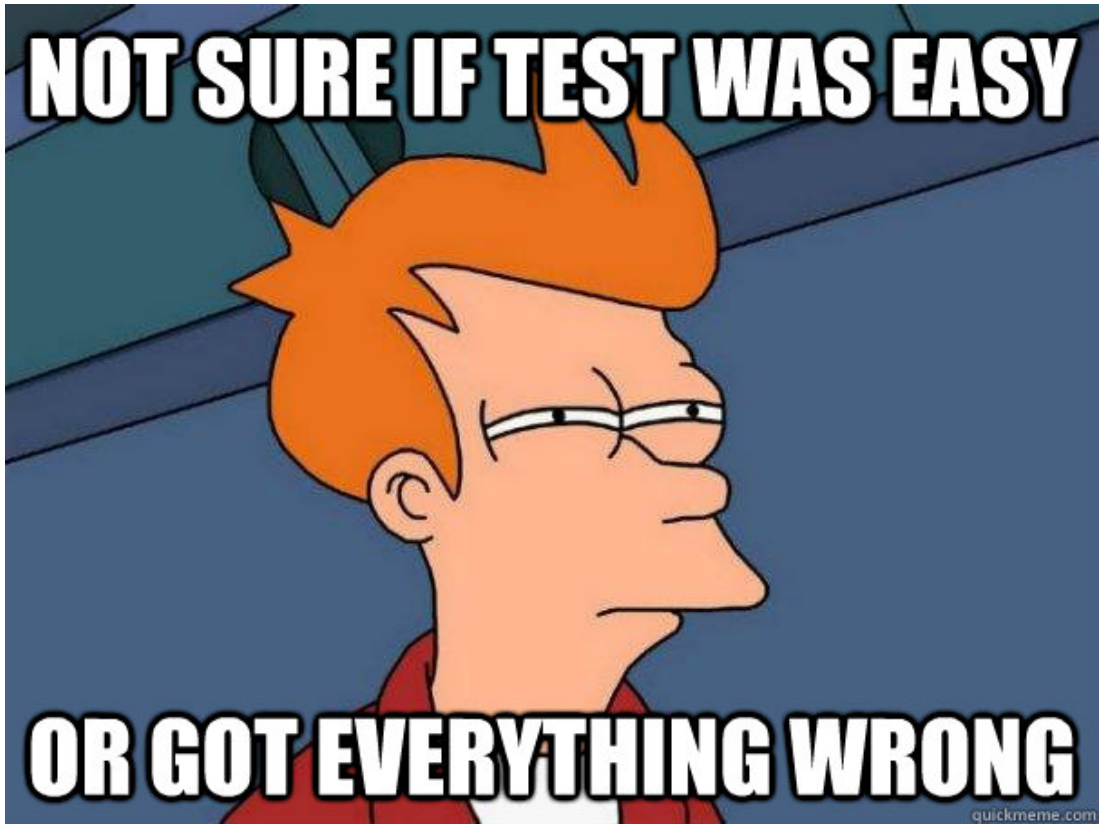
Mobile Security
Fall 2015

Patrick Tague

#14 – Mobile Dev Best Practices

Questions about the Exam?



Email them to all 3 of us.

Class #14

- Best practices

- Managing data, dealing with policy, understanding laws, etc.

Best practices for security and privacy in mobile app development

Understand Your App

- Before touching an IDE or even sketching your app functionality on paper, think about what services it uses and the potential risks
  - Do you create or collect data?
  - Do you rely on external communications?
  - Do you access location?
  - Do you share content to servers or other users?

Understand the Ecosystem

- App developers need to consider:
  - What IDE/SDK/API/platform tools are involved in development, what these tools do, how they work, what they provide, etc.
  - What type of users are targeted
  - What libraries / third-party toolkits are used
  - What external services are relied on

Understand the Browser

- Developers using the mobile browser should know the differences from typical PC browsers
  - Understand the strengths and weaknesses
  - Understand the limitations
    - Cookies
    - Caching pages
    - Remembering passwords
    - Caching credentials
  - Understand the security gaps

Have a Security Expert

- Make sure your development team has at least one person dedicated to checking security requirements / concerns at every step
  - If your team is just you, you're that person.
  - Whenever something is changed, evaluate its impact on security & privacy

Data

Data Collection & Retention

- Don't access or collect data that isn't needed
  - If you have a legit purpose, fine; otherwise, no
  - Some platforms / app stores have rules you're required to follow, or you can get in trouble
- Limit linking sensitive data to user identity
  - Only store sensitive data with IDs when needed to provide a service
- Delete data when you no longer need it, or when a user closes their account
  - At minimum, unlink the ID from the data

Data Protection

- Encryption:
  - Encrypt any data in transit when authenticating users, transferring personal info, etc
    - SSL/TLS is an easy option, supported by all of the platforms, that can protect against unsecured or poorly secured networks
  - Encrypt stored data, especially sensitive information, passwords, etc.
    - Most platforms have built-in support tools, that you can use if their protections match your security/privacy goals

Data Protection

- De-Identification:
  - Make an effort to de-identify user data before sharing
  - Sanitizing data identities can be done if you need to keep the linking private; hashing IDs can help

User Authentication

- Make sure that users can correctly log out of a mobile session
- If a user changes their password in the back-end, the mobile session should end and re-authenticate
- If your app collects/accesses sensitive data, consider two-factor authentication

Policy

Privacy Policy

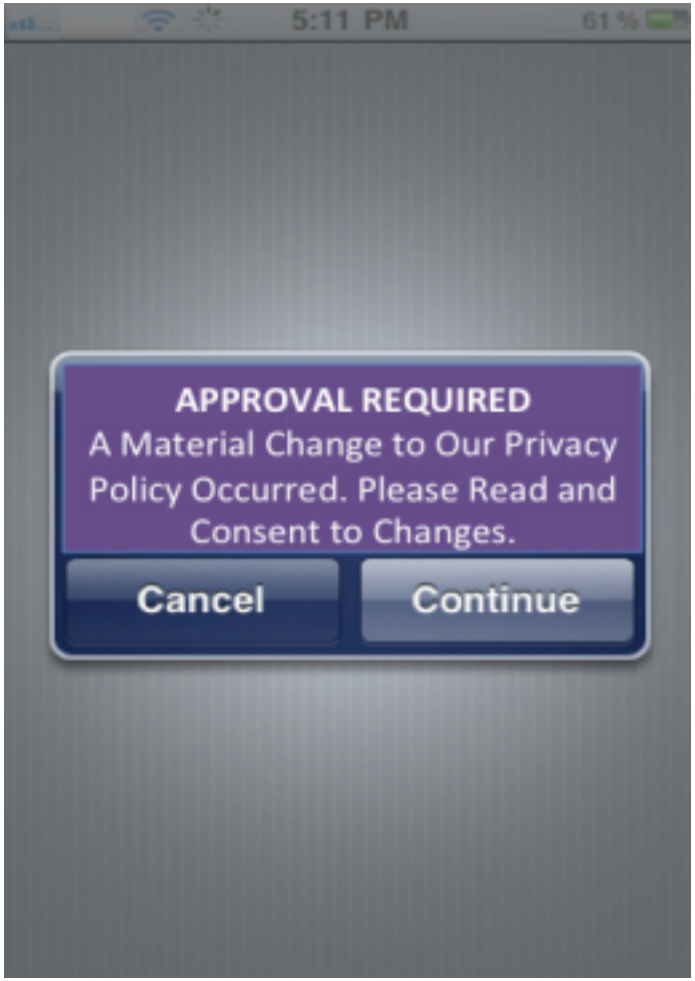
- Your app should include or refer to a detailed privacy policy that describes what data you collect, what you use it for, and who you share it with (and why)
  - Don't be lazy and copy some standard text
  - Be complete and accurate or you can get in some serious trouble
- Once you have a policy, follow it
  - Undisclosed practices can get you in trouble

ID / Linking Disclosure

- Tell your users if you are storing their IDs along with their data
  - Even if you don't store IDs, let them know if you use the data in a way that can be linked to their device, account, etc.

Ack Policy Changes

- Whenever you change your privacy policy, take the effort to alert users of the changes
  - Especially when the data collection / storage / sharing properties of your app change
  - Don't tell your users that you have the right to change the policy at any time without notification, or you can get in trouble



“Sensitive” Data

- There's no official definition of what makes data sensitive, so use good judgment
  - It's probably better to strongly protect something that someone doesn't think is sensitive than to not protect something that someone thinks is sensitive
  - “Sensitive” usually includes data related to health, finances, race, religion, political affiliation / party membership, sexuality, etc.

Notice

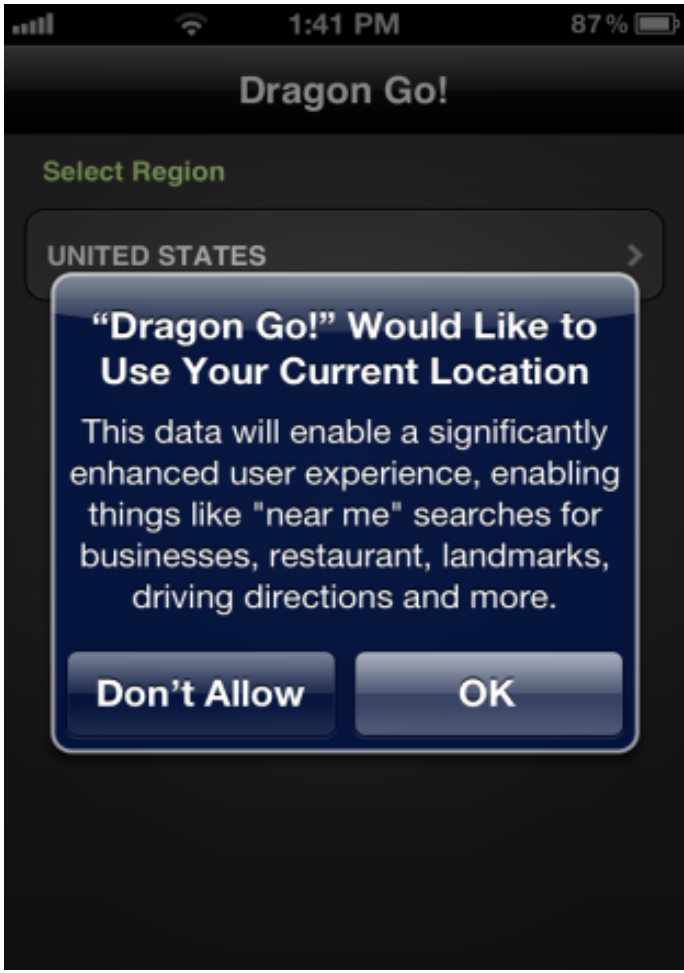
- Give your users notice that your app shares data with 3rd-parties, why it's being shared, and what they're using it for (of course, make sure you know these things first)

- If your policy is all-or-none, tell your users about the trade-offs, so they are educated about their choice

- Let users know when you share their location

Location

- Get permission from users before accessing their location (most OSs force this)
- Get additional permission before sharing their location (almost nobody does this) or using it in "unexpected ways"
- Include the collection method, granularity, linkability, storage time, etc. in your privacy policy



Choice

Individual Choice

- Whenever possible (and if allowed by the OS), you should give users the ability to opt out
  - Esp. of collection, storage, and transfer of personal information
  - If possible, let them also get access to the data for their own purposes (this is required in some places)
  - Also, try to make sure whatever you collect is correct, up-to-date, and needed

- Make sure to ask in a timely manner
  - Namely, before taking action, while in context

Responsibility

Privacy Responsibility

- Your development team is responsible for:
  - Reviewing / updating your privacy policy whenever changes are made
  - Archive past privacy policies in case users have old versions
  - Enforce access control policies inside your company to prevent unnecessary employee access to data
  - Answer privacy-related inquiries / concerns from users
  - Keep up to date with legal/regulatory developments

User Feedback

- Take user feedback!
  - Provide a way for users to contact you about security and privacy concerns
  - Either through an in-app form, a forum, or email

- Reply to user feedback!
  - If you answer users honestly, they'll appreciate it, and probably continue to be your customers

Laws & Regulations

Federal/State Privacy Laws

- In the US, privacy laws only apply to certain types of data, but if you handle these data, you must comply (and probably need a lawyer)
  - Credit reports (FCRA)
  - Electronic communications (FTC, CAN-SPAM)
  - Education records (FERPA)
  - Bank records and financial information (GLB)
  - Video rental records (VPPA)
  - Health information (HIPAA)
  - Children's information (COPAA)
- Other laws in other countries

New Developments

- It's the developer's job to keep current on any legal developments, to keep policies and protections up to date
  - Ex: Do Not Track will likely be extended from browsers to mobile apps in the near future
  - Ex: device identifier use and policies have been changing drastically in recent years

Resources

- Most of the material I just went through is from a really great document published by the Future of Privacy Forum and the Center for Democracy & Technology
  - "Best Practices for Mobile Application Developers", available at cdt.org

- Also, see:
  - "Mobile App Developers: Start with Security", ftc.gov
  - "42+ Secure mobile development best practices", viaForensics.com

Key Take-Away Points

- With proper awareness of the threatscape, developers can provide pretty decent protection for their users and themselves
- Developers must consider the unique features and intricacies of the OS and app framework
- Although mobile is more difficult, following best practices can go far

Nov 24:
Fun with Mobile Networks