Mobile Security

Fall 2015

Patrick Tague

#16 – Best Practices (cont'd);
Discuss Final Deliverables, Wrap-up

Class #16

- Wrap-up 'best practices' material from last class
- Discussion of final deliverables
  - Final project presentations on Dec 3, 8, & 10
  - Final project report due Dec 17
  - Open Q&A about deliverables, expectations, etc.
- Semester wrap-up

Best practices for security and privacy in mobile app development

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

Questions?

Final Project Presentation

Final Project Presentation

- Final presentations will be in class on December 3, 8, and 10
- Each team will have MAX 12 minutes, including Q&A
- Presentation should include:
  - Re-hash problem statement, goals, etc.
  - Detailed discussion of your approach, findings, results
  - Demo, screenshots, figures, etc.
  - Brief discussion of challenges faced, how overcome, etc.
  - Brief discussion of future work

Presentation

- Q: Does everyone on the team have to present?

- A: Yes, team members that don't present will get fewer points. Try to have a roughly even split of time across team members.

Presentation

- Q: Any style guidelines on the presentation?

- A: Not really, but pictures/figures are always better than text.

Presentation

- Q: Can we do a demo?
- A: Absolutely! Live demos or recordings are both great. However, be warned about live demo gremlins, so test and test again.

Questions about the presentation?

Final Project Report

Final Project Report

- Final project reports are due on December 17, one week after the last day of class

- Final report includes three things:
  - Conference-style paper
  - Conference-style poster
  - Short demo video (1-2 minutes)

- No extensions will be given

Paper

- Q: What format should the paper be in?

- A: IEEE 2-column format (same as other assignments) – page limit is 10 + references.
  - If you submit in a different format, we'll ask you to reformat it. If you don't, we'll take off lots of points.
  - Don't feel obligated to fill 10 pages. We ***really*** don't mind if it's shorter, as long as it's complete.

Paper

- Q: What should be included in the paper?
- A: Overall introduction to and description of the problem, motivation and expansion beyond related work, a hypothesis / goal, adversary model and assumptions, detailed description of the approach, technical details, any simulation or testing, results, conclusions, future work, challenges, figures, references, ...

Poster

- Q: What content should go in the poster?

- A: I like posters with lots of pictures/figures, relatively little text, but enough to tell the story.
  - I shared posters from last year. Some are better than others.

Poster

- Q: What format should be used for the poster?

- A: We posted a template to BB, but you can use whatever style you prefer and customize content as needed.
  - Please keep similar size/ratio.

Poster

- Q: What are you going to do with the poster?

- A: If you've seen my office door, you know the answer. Also, recall that I gave you posters from F14 at the start of this class.

Paper / Poster

- Q: Publication?

- A: If you're interested in submitting your work to a workshop, conference, etc., or releasing your work under an open-source license, please talk to your project mentor (and me) ASAP.

Video

- Q: What should be in the demo video?

- A: Video should be sort of a brief "commercial" for your project and a hint at the goals and value of the work.
  - Video should be 1-2 minutes, focusing on the problem, not the results
  - I may show these in future classes

Sponsor Deliverables

- Q: Does my sponsor want anything other than the paper, poster, or video?

- A: I don't know. Ask your sponsor.

Questions about the report?

Any last questions about final deliverables?

Just a few last words…

Team Effort Reports

- As part of the final project report submission, I need the following from every individual:
  - Send me an email with a task and percent breakdown of how much contribution <u>you feel</u> each team member did
  - Ex:
    - From: Jordan
    - Jon and I wrote all the code, Joey did a lit survey and helped in the app design, Donnie designed the server infrastructure, Danny came up with privacy specifications
    - Jordan = 25%, Jon = 18%, Joey = 22%, Donnie = 20%, and Danny = 15%

Feedback

- I really appreciate feedback about the course:
  - What you liked, what you didn't like, what should be added/removed, etc.
  - This course is constantly evolving, and we're looking for constructive comments/criticism (we can take it)

- Please do a course evaluation
  - Please, please, please…

Android Phones

- For those of you who borrowed Android phones for the course, we need those back!
  - Pgh students: return to Jeff in ECE hub by Dec 18
  - SV students: return to Stephanie or Cindy in B19 1052 by Dec 18
  - If anything is missing, broken, etc., you will receive an *Incomplete* grade in the course, which will only be changed when you replace it
  - Don't worry about software / contents, we'll completely wipe all memory and flash to stock

Questions?
Comments?

Dec 3, 8, & 10:

Final Presentations

Dec 17:

Final Project Report Due

Thank you!