



Presented by:
Jeremy Allen

November 17th

OWASP Atlanta - 2011

HOWTO: Mobile Application Assessments

OWASP Mobile Top 10

#1 Insecure Data Storage

- Android just coming out with KeyChain API
- Apple already has KeyChain and Data protection
- Risk assessment is your friend
 - See: Why is this the #1 risk?
 - Any Guesses?

Data Storage Demo

#2 Weak Server Side Controls

- Web applications are still important
- Traditional WAPT Stuff
- OWASP resources are immensely useful

#3 Insufficient Transport Layer Protection

- Pretty much means SSL if you are doing it right
- Use SSL unless you really know what you are doing
- SSL is hard enough to get right

Insecure transport layer security demo

#4 Client Side Injection

- You can still have SQL Injection in your application
- SQLite is exceedingly popular on iOS and Android
- Data validation, data validation, data vali....also watch our for UIWebView and the equivalent on Android

#5 Poor AuthN and AuthZ

- Shared client/server issue
- Using the mobile device number is not a very good authentication token?
- How did SoundCloud handle this?
 - Discussion on authentication tokens
 - Oauth is somewhat intricate, but nice

#6 Improper Session Handling

- Never trust the client
- Maintain everything on the server

#7 Security Decisions via on Untrusted Inputs

- Skype vuln allowed URL handling to make calls
- What URLs do popular apps expose?
- Other Inputs: SMS popular on Android

#8 Side Channel Data Leakage

- App Snapshots
- SoundCloud demo app would leak this data
- Keystroke logging via accelerometer
- 3rd Party Libraries
- File system, many other places

#9 Broken Crypto

- So many ways to fail
- Very few ways to win
- Use platform APIs
- Understand the risk and hire people who understand crypto

- Encoding, obfuscating, storing, mixing and or trying to hide data does not provide confidentiality
- You probably need authentication AND confidentiality

#10 Sensitive Information Disclosure

- Client side secrets.....
- Another application assessment favorite
 - Backdoors, trade secrets, hard coded server authn, private keys ... I have seen some real crufft in the code
- Yes, I can see your code.

Yes, even if you obfuscate it

Yes, even if you compile it

Last thing...

Secure your apps?

Happy fun demo time