Why You Should and Shouldn’t Worry About Mobile App Security

What's the Problem?

- Mobile apps use a fundamentally different architecture than PC-based apps
- Security in mobile apps is in its infancy
- We think of smart phones as phones, not portable computers
- We think of smart phones as portable computers, not phones
- Limited control or visibility of how apps use our personal data
- Privacy Violations due to hidden, confusing, and "evil" policies and one-sided control (hint: not the user)

The Mobile Architecture

- Hardware = Software = Network
  - Can you mix and match hardware with OSes?
  - Can you connect a device of your choice to the network of your choice?
- For PCs, YES and YES – by design
- For Smartphones, NO and Sometimes
- Result
  - Increased sharing of information between HW, SW, and Network owners – often hidden from user
  - Greater centralization of control (away from user)
    - e.g., Network provider can lock hardware and update OS, user updating OS may void network contract

Evolving Mobile Security

- Security is complicated and takes time and effort even by the most knowledgeable experts to get right
- Mobile security has not had the necessary time and effort by experts to mature
  - Focus is currently on “What can I do” with this new technology
  - First iterations take shortcuts to get to market, security fixed later for important apps
  - Security through obscurity (i.e., no security at all)

Smart Phones are Not Phones...

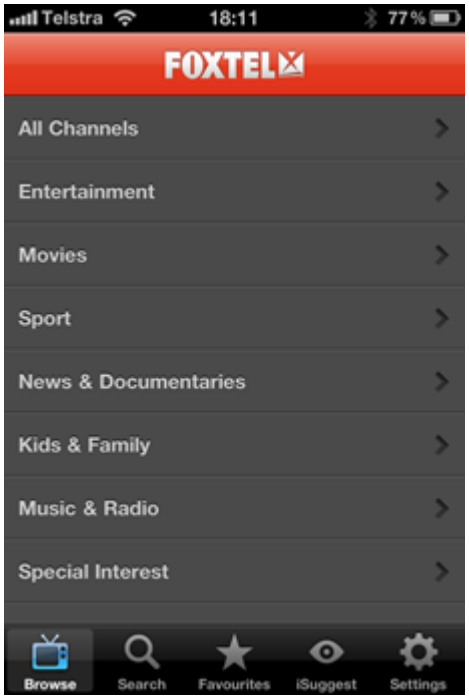
- The “phone” mentality doesn’t work:
  - phones have few security exploits
  - phones don’t run applications
  - phones don’t have Internet access always on
- Result:
  - We don’t take proper security precautions when we think of these devices as phones

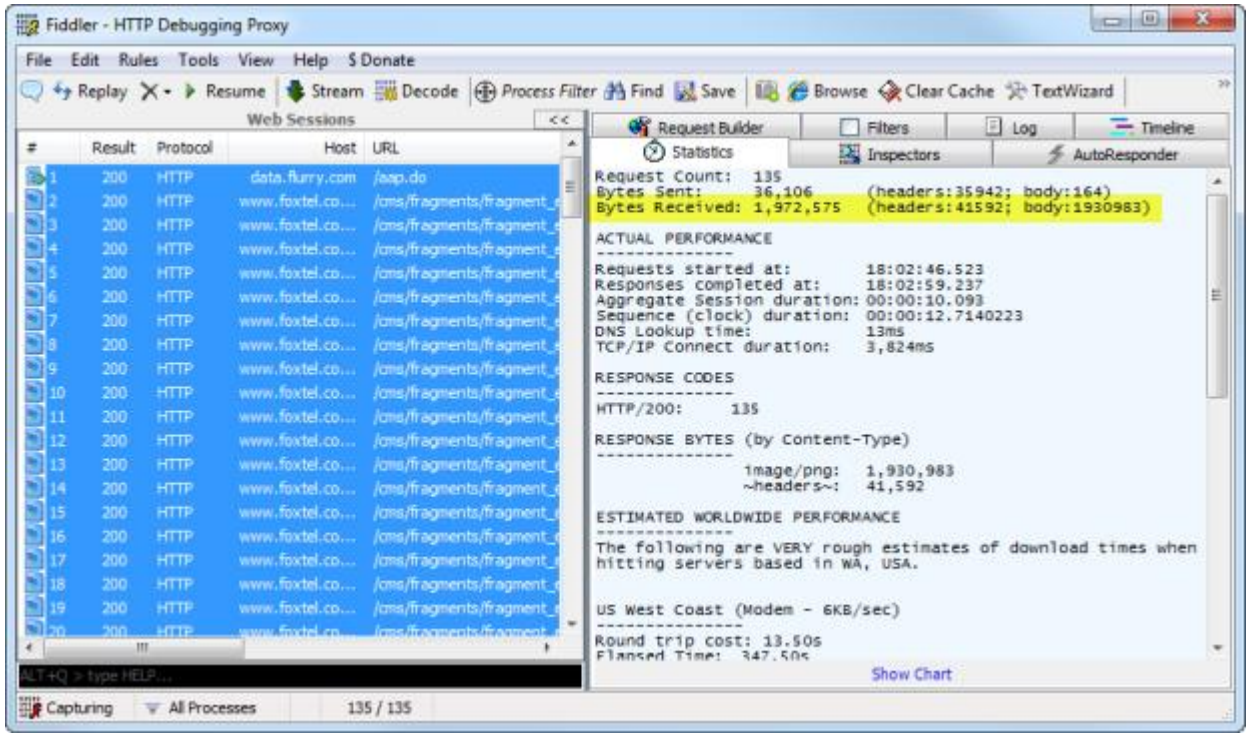
Smart Phones are Not Computers...

- The “computer” mentality doesn’t work:
  - Your computer is not tied to your identity through your wireless contract
  - Your computer doesn’t follow you around all day while connected to the Internet, recording where you go and when
  - Your computer HW and SW is controlled by you, not shared with the network provider
  - Your computer has enough excess power, local resources, and network bandwidth to do security protocols and scans
  - Your computer lets you change security settings (e.g., proxies, network configuration, trusted CAs)
- Result: Traditional computer security precautions do not address mobile security issues
  - Increased threat of confidentiality problems
  - Melding of personal and professional lives on one device can be problematic
  - Not enough power, CPU, or network bandwidth to do security and apps effectively
  - Very limited ability to change security settings – e.g., no easy way to change trusted CAs for SSL, filter traffic to blacklisted sites

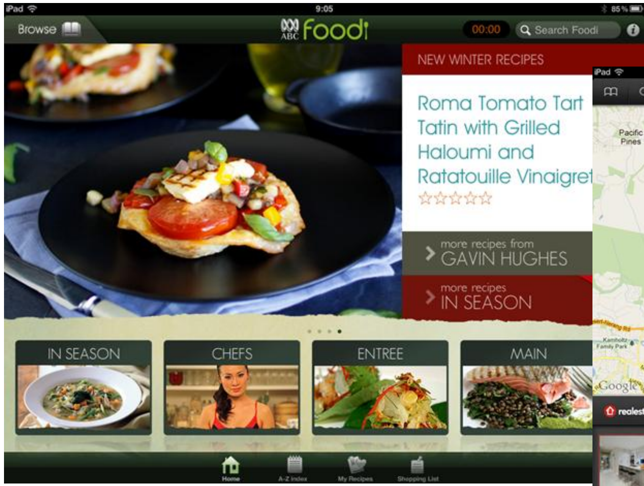
Data.Flurry.com??

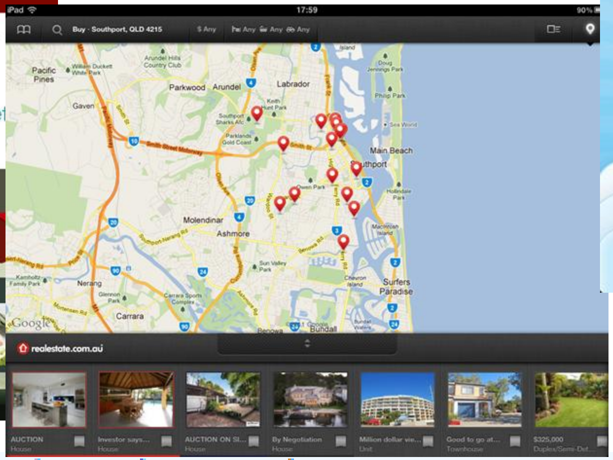
- Ever heard of flurry.com? They've heard of you.

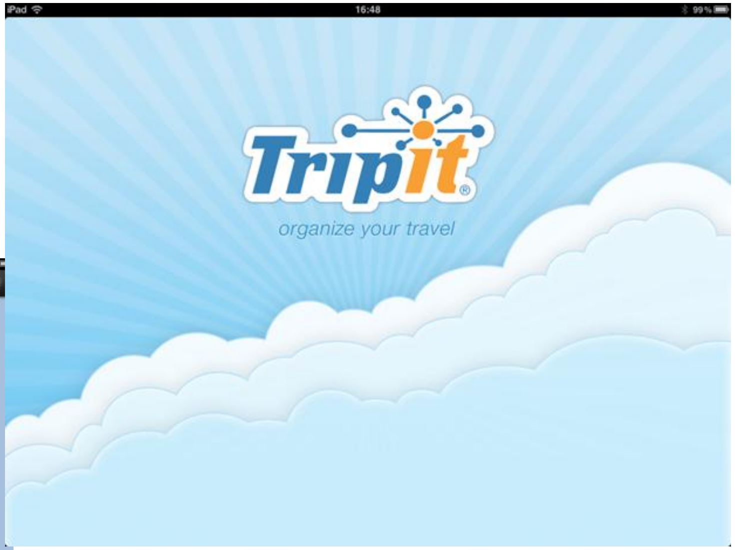




HTTP Request








```
POST http://data.flurry.com/aap.do HTTP/1.1
Host: data.flurry.com
User-Agent: Foodi/1.4 CFNetwork/485.13.9 Darwin/11.0.0
Content-Type: application/octet-stream
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Pragma: no-cache
Content-Length: 319
Connection: keep-alive
Connection: keep-alive

◆▯ ◆◆◆◆◆◆◆◆◆◆◆◆◆◆▯ ◆0◆◆▯ 2◆▯▯ ◆◆▯ 75RBTFRLHA8TEDG64RBF◆▯ 1.4
◆◆◆.IPHONEdc2fe26bf8[illegible]929◆◆▯ .◆◆◆▯ ◆◆▯ 2◆▯▯ ◆◆▯ ◆▯ device.model.1
◆▯ iPad2,1◆▯ ◆▯ ◆▯ 1.4◆◆▯ 2◆▯ 5
◆◆◆◆◆◆▯ ◆▯ ◆◆◆◆◆◆▯  ◆▯ en_AU◆▯ Australia/Sydney▯ ◆◆▯ ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆▯ ◆▯ Home item
tapped◆◆◆▯ ◆▯ ◆▯ Home item tapped◆▯ ◆▯ item◆▯ main◆◆◆◆◆▯ ◆
◆◆◆◆◆◆◆◆▯ ◆◆◆◆◆◆◆◆
```

Data Control by Mobile Apps

- Poor granularity of control over data
  - Coarse controls
    - limits access to Internet, email, texting, etc.
    - No limits on when, how much, how these can be used
  - All or nothing decision
    - Use our app (and let us use your data) or don't use it
    - No way to run with limited access
- Undisclosed usage
    - App owner knows how app works
    - User must make tradeoff between functionality and security
- 3rd party aggregation
    - Apps use common 3rd party libraries (flurry, Google Analytics)
    - Libraries send personal data to 3rd parties without user knowing
    - "ubercookies": 3rd parties know about *all* sites you visit, not just activity at a single site

Privacy Issues

- One-sided policies
  - App owner decides on the policy
    - e.g. “HumancentiPad” episode of South Park
  - Need better visibility and informed consent
- False weighting of importance
  - Bad logic: national interests vs. individual interests
    - e.g., catching terrorists vs. *my* privacy
    - false logic: Fighting for privacy means I’m doing something illegal
  - Proper logic: (national goals) vs. (individual goals * 3,000,000)
    - catching 100 terrorists vs invading 3,000,000 people’s privacy
    - Privacy is important for its own sake and for a healthy an civil society

Why You *Shouldn't* Worry

- Privacy is dead already
  - Considering the trends, can you imagine that in 20 years we will be able to hide anything for any significant length of time? Then why live in tomorrow's past today?
- All these problems will be solved, just like they were for other technologies
  - Better to adopt early with risks than adopt late without operational experience
- People are the ultimate problem (and solution)
  - Most serious exploits still require the human in the loop
  - Accountability, training, and policy can address most serious security problems
  - Need to let computers do what they're good at and people do what they're good at, and hope this covers everything

The Solution

- Add up all benefits of using mobile technology
- Add up all costs
  - location data, contacts, and other data leaks
  - human error
  - data aggregation by 3rd parties
  - etc.
- Compare, knowing that your calculations are wrong
  - emergent benefits are hard to quantify
  - costs are often hidden and unknowable by most users
  - consider the cost of surprises when deciding

What to Do Now

- Training and education about what is OK, what is not, what is risky, and what is recommended
  - This will change rapidly over time, so training is ongoing, not a one-time event
  - Similar to annual DoD IA Training material
- Separate work from personal as much as possible
  - Example: Good Technologies app has encrypted partition that can be used for work and wiped remotely
  - DISA vision: personal devices, government SIM
- Secure App Marketplace
  - Trusted government apps from government source
  - List of trusted personal apps from public sources

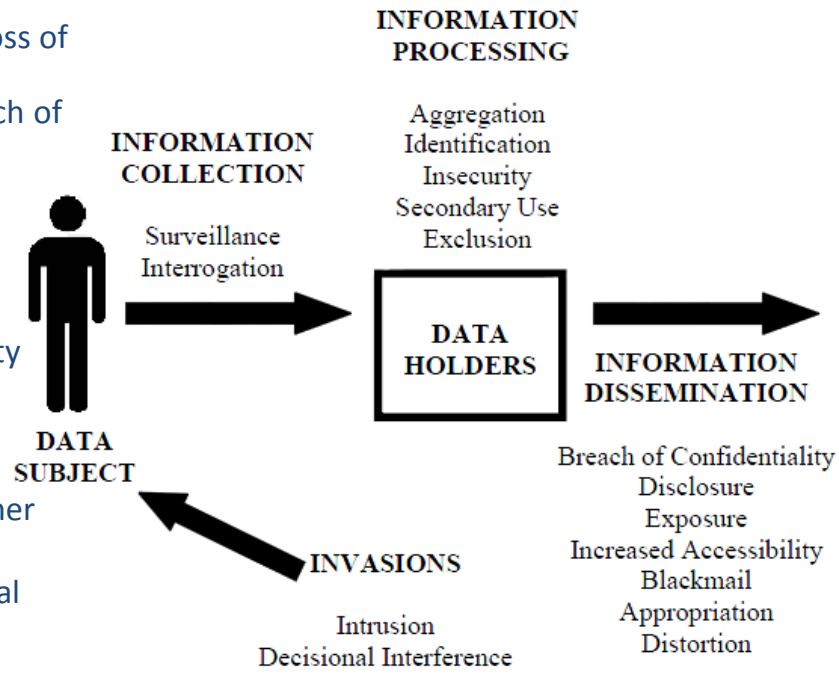
Goals for Later

- Make the mobile platform secure
  - Relying on users for security is going to fail
  - Default must be secure option (not currently possible, but maybe eventually)
  - DISA STIG for mobile devices, certification for common apps (soon?)

Backup Slides

Privacy: Beyond "I've Got Nothing to Hide"

- Information Collection
  - Surveillance ==> limited risk taking, creativity, individuality
  - Interrogation ==> innacurate or incomplete information, not answering can be incriminating
- Information Processing
  - Aggregation ==> learn detailed private information from public sources
  - Identification ==> attachment of unwanted information to person
  - Insecurity ==> identity theft, disclosure, distortion, loss of anonymity
  - Secondary Use ==> betrayal of expectations, mismatch of info with use
  - Exclusion ==> propagation of false information
- Information Dissemination
  - Breach of Confidentiality ==> release of confidential information, undermining of trust
  - Disclosure ==> distortion, limited risk taking, creativity
  - Exposure ==> embarassment, humiliation
  - Increased Accessibility ==> unwanted availability of information
  - Blackmail ==> threat of distortion, control over another
  - Appropriation ==> unwanted notoriety, exploitation
  - Distortion ==> loss of social status, disruption of social relations
- Invasion
  - Intrusion ==> disturbance, loss of solitude
  - Decisional Interference ==> inability for personal choice



Daniel J. Solove, *A Taxonomy of Privacy*, University of Pennsylvania Law Review, Vol. 154 No.3, January 2006, pp.477-560