DENIM GROUP

build | integrate | secure

# Mobile Applications and Application Framework Security

**Dan Cornell**

# My Background

- Dan Cornell
- Founder and CTO of Denim Group
- Software developer by background (Java, .NET, etc)

- Denim Group
  - *Build software with special security, performance, reliability requirements*
  - *Help organizations deal with the risk associated with their software*
    - Code reviews and application assessments
    - SDLC consulting
    - Secure development training

# Tradeoffs: Value versus Risk

- Mobile applications can create tremendous value for organizations
  - *New classes of applications utilizing mobile capabilities: GPS, camera, etc*
  - *Innovating applications for employees and customers*
- Mobile devices and mobile applications can create tremendous risks
  - *Sensitive data inevitably stored on the device (email, contacts)*
  - *Connect to a lot of untrusted networks (carrier, WiFi)*

- Most developers are not trained to develop secure applications
  - *Fact of life, but slowing getting better*
- Most developers are new to creating mobile applications
  - *Different platforms have different security characteristics and capabilities*

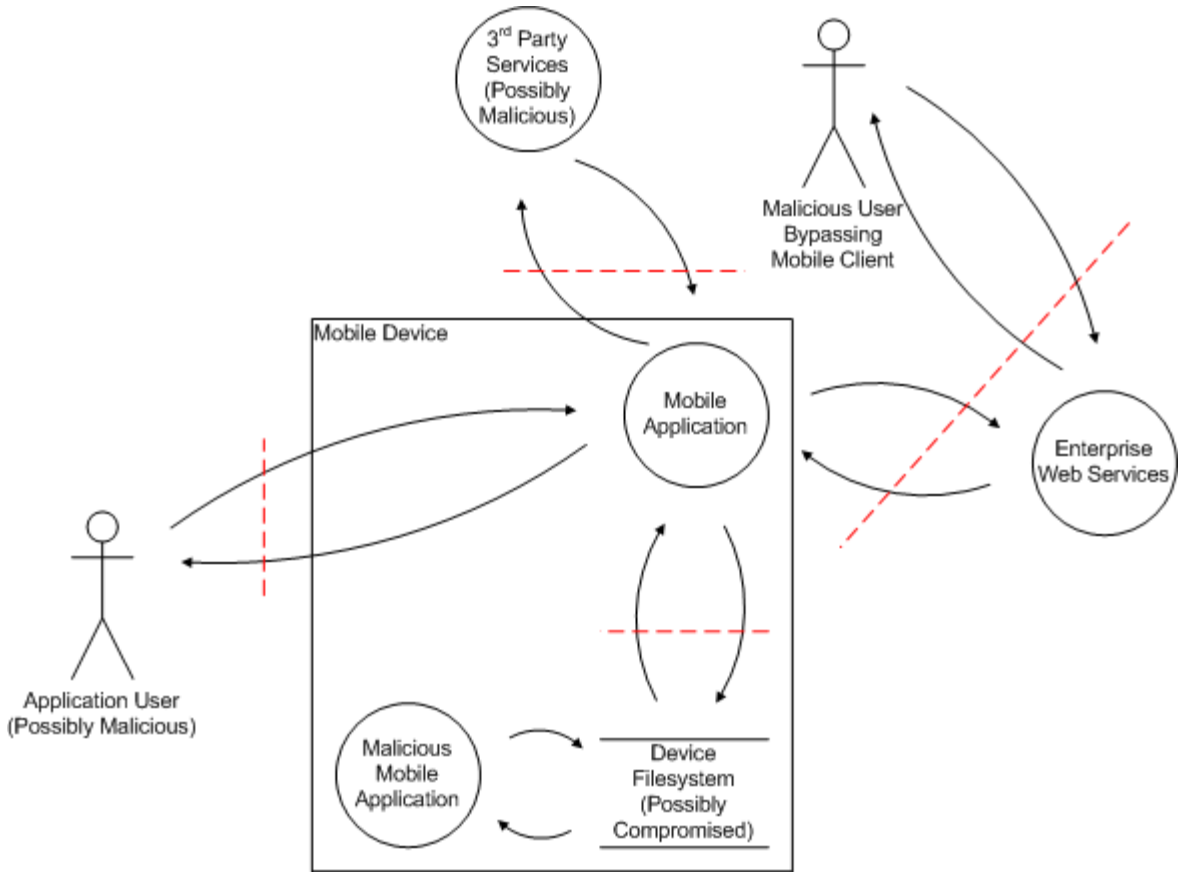
# Some Assumptions

- Mobile applications are essentially thick-client applications
  - *That people carry in their pockets*
  - *And drop in toilets*
  - *And put on eBay when the new iPhone comes out*
  - *And leave on airplanes*
  - *And so on…*
- Attackers will be able to access:
  - *Target user (victim) devices*
  - *Your application binaries*
- What else should you assume they know or will find out?

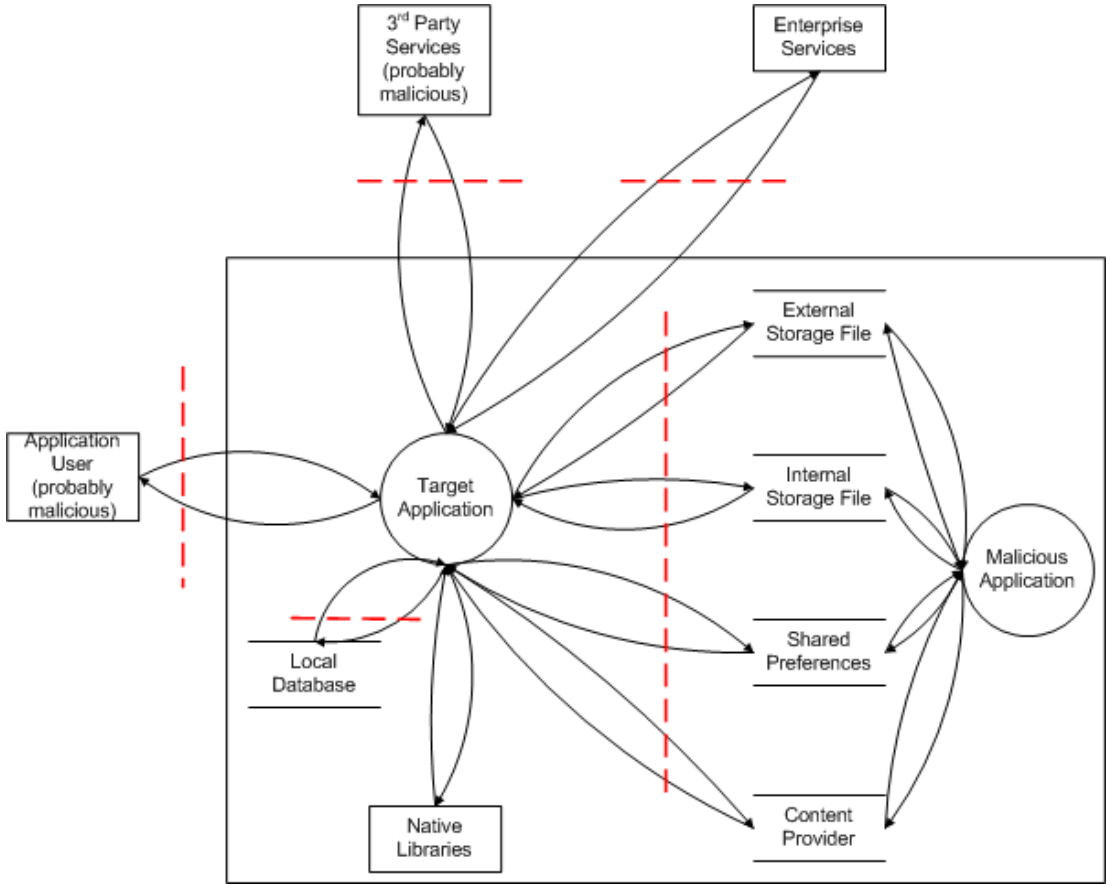
# Mobile Application Security Stakeholders

- Infrastructure Security Administrator
  - *Responsible for securing the IT environment for in-house corporate users.*
- Application Development Manager
  - *Responsible for building mobile applications*
- IT Auditor
  - *Responsible for compliance*
- User
  - *Uses mobile devices and applications*

# Generic Mobile Application Threat Model



# Generic Android Application Threat Model



# What Are the Concerns?

- Infrastructure Security Administrator
  - *"Remote-wipe" lost or stolen devices*
  - *Control mobile device access to corporate networks*
  - *Keep mobile devices on networks uncompromised*
- Application Development Manager
  - *Avoid introducing vulnerabilities into mobile applications*
- IT Auditor
  - *Maintain compliance*
  - *Do not get in trouble with external auditors*
- User
  - *Do not send sensitive data to unauthorized parties (location, photos, emails, etc)*
  - *Be reasonably safe if a device is lost or stolen*

# Specific Platforms

- iOS (iPhone, iPad)
- Android
- Blackberry
- Windows Phone 7
  - *Windows Mobile 6.5?*
- Symbian?

# Guidance for Developers

- Secure Mobile Developer Reference
- Topic Areas
  - *Overview of Application Development*
  - *Overview of Secure Development*
  - *Defeating Platform Environment Restrictions*
  - *Installing Applications*
  - *Application Permissions Model*
  - *Local Storage*
  - *Encryption APIs*
  - *Network Communications*
  - *Protecting Network Communications*
  - *Native Code Execution*
  - *Application Licensing and Payments*
  - *Browser URL Handling*

# So What Should Developers Do?

- Threat model your smartphone applications
  - *More complicated architectures -> more opportunities for problems*
- Watch what you store on the device
  - *May have PCI, HIPAA implications*
- Be careful consuming 3rd party services
  - *Who do you love? Who do you trust?*
- Be careful deploying enterprise web services
  - *Very attractive target for bad guys*
  - *Often deployed "under the radar"*

# So What Should Security People Do?

- Find out about smartphone projects
  - *Not always done by your usual development teams*
  - *R&D, "Office of the CTO," Marketing*
- Assess the security implications of smartphone applications
  - *What data is stored on the device?*
  - *What services are you consuming?*
  - *Are new enterprise services being deployed to support the application?*

# Online

- Code, slides and videos online:

*www.smartphonesdumbapps.com*

# Questions?

Dan Cornell
dan@denimgroup.com
Twitter: @danielcornell

www.denimgroup.com
(210) 572-4400