Android Security

CryptDB

Android Security

Sergio Benitez

What's in an app?

- Applications are separated into components.
  - No main() function.
  - Specified in a manifest file.

- Four types of components:
  1. Activity (UI, one activity per screen)
  2. Service (background processing)
  3. Content Provider (data storage, SQL-like)
  4. Broadcast Receiver (message mailboxes)

Component Interaction

- Primary ICC is through intents.
  - A description of an event to be performed.
  - A message containing address, action, data.

- Android APIs take action using intents:
  1. startActivity(Intent)
  2. startService(Intent)
  3. sendBroadcast(Intent)
  4. bindService(Intent, ServiceConnection, int)

Interacting with Components

- Broadcast Receivers: sendBroadcast(Intent)
  - Receivers subscribe to actions, filter intents.
- Services: start/bindService(Intent)
  - Expose RPC interface usable after binding
- Activities: startActivity(Intent), service callbacks
- Content Providers: via authority in URI strings
  - each associated with *authority* describing contents
  - Of form: content://<authority>/<table>/[<id>]

Security Enforcement

- Two Levels:
  - Unix: Each app under unique user, jailed.
  - ICC: Monitor messages, enforce MAC.
- Focus is on ICC mediation.
- In short, manifest file contains MAC policies.

ICC Mediation

- Labels assigned to apps and components.
  - Labels are just permission names.
  - XML manifest file contains assignments.
  - Components usually only get one label.
- During ICC, from source to target, check that:
  - Target's permission label in source’s app’s set
  - I.E.: Source inherits app's permissions

Security Refinements

- Developers added a whole bunch of stuff after.
  - Probably have added more since then (2009).
- **Private Components**, Implicitly Open Components, Broadcast Intent Permissions, Content Provider Permissions, Service Hooks, **Protected APIs**, **Extra Permission Protection Levels**, Pending Intents, URI Permissions

Private Components

- Some components are application specific.
  - IE, shouldn't be accessed by any other app.
- Can set these to **private** to enforce this.
  - In the manifest file, of course.

Protected APIs

- Not all communication through components.
- Android exposes APIs accessibly by everyone.
  - To use API, app needs specific labels.
    - Examples: Network, camera, contacts.
- Labels check aren’t special, though.
  - Any app can have them. Until they added…

Permission Protection Levels

- Labels assigned to one of four protection levels:
  - Normal: Developer defined, regular labels.
  - *Dangerous*:
    - UI prompts user to accept label.
  - *Signature*:
    - Only granted to apps signed by same key.
  - Signature or System: Like signature; legacy.

- Defined in manifest file, of course.

CryptDB

Sergio Benitez

board…