black hat®
USA 2015

Who are we?

Penetration Testers at LinkedIn

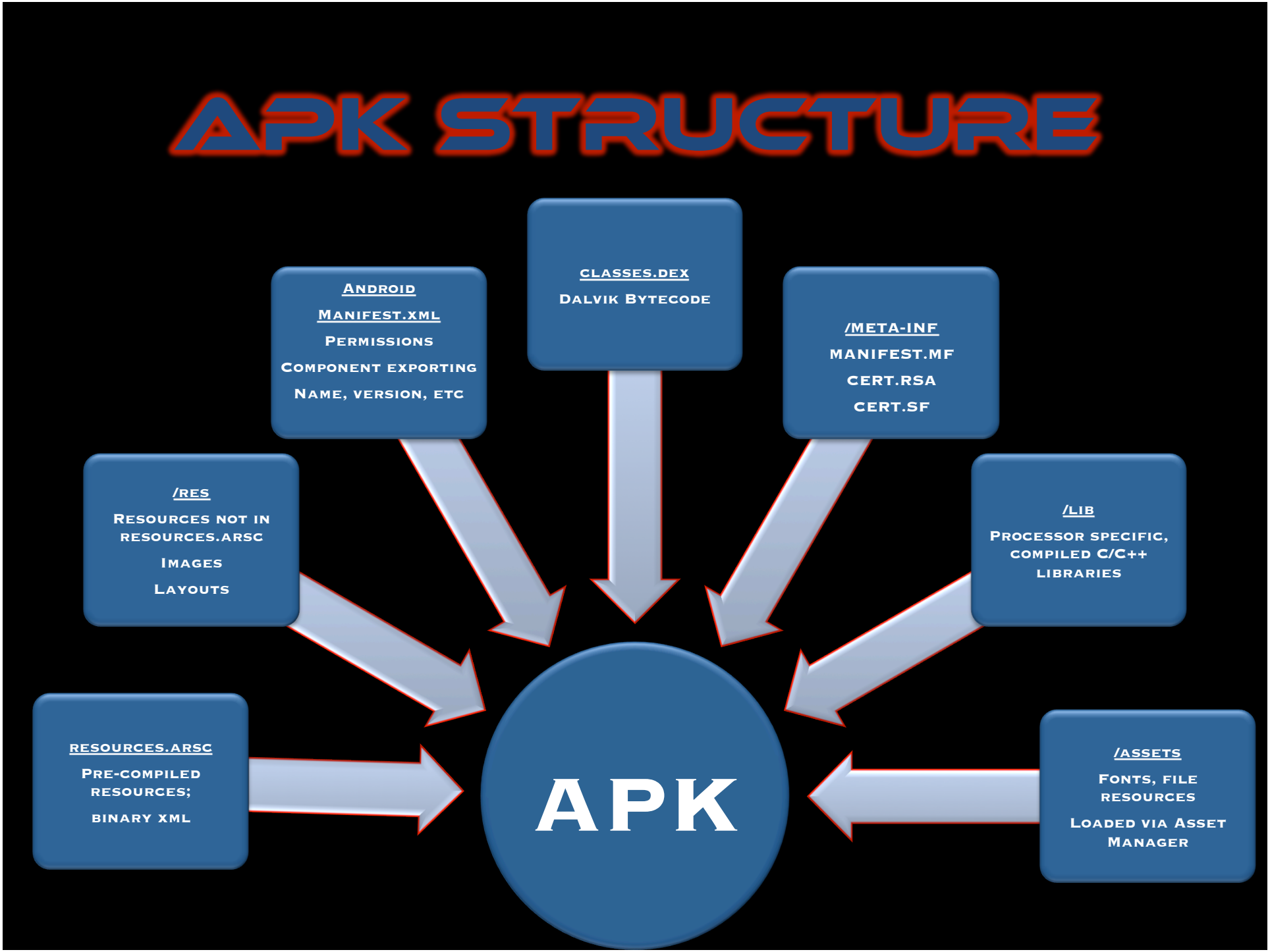
Tony Trummer

- Staff Information Security Engineer

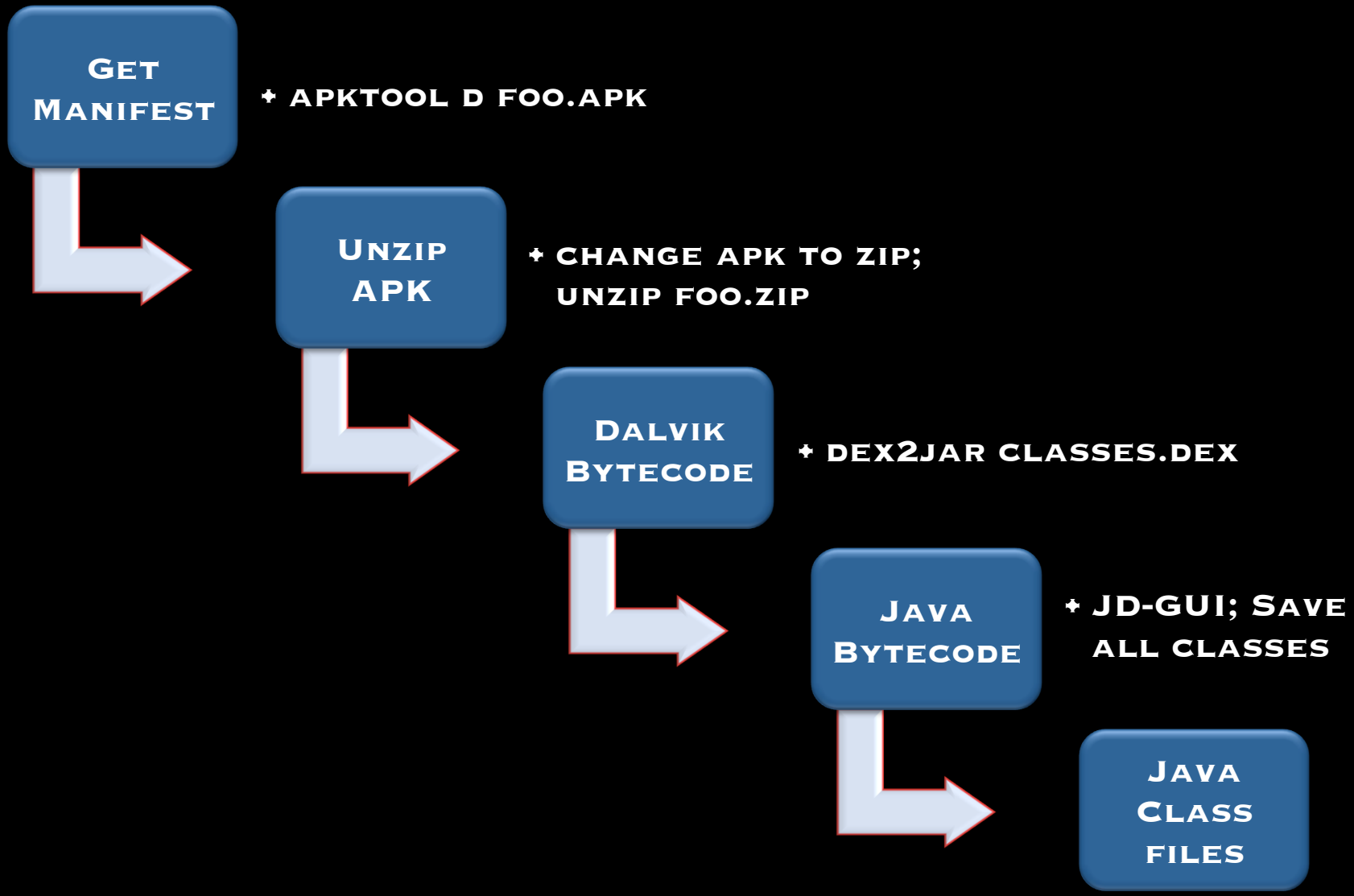
Tushar Dalvi

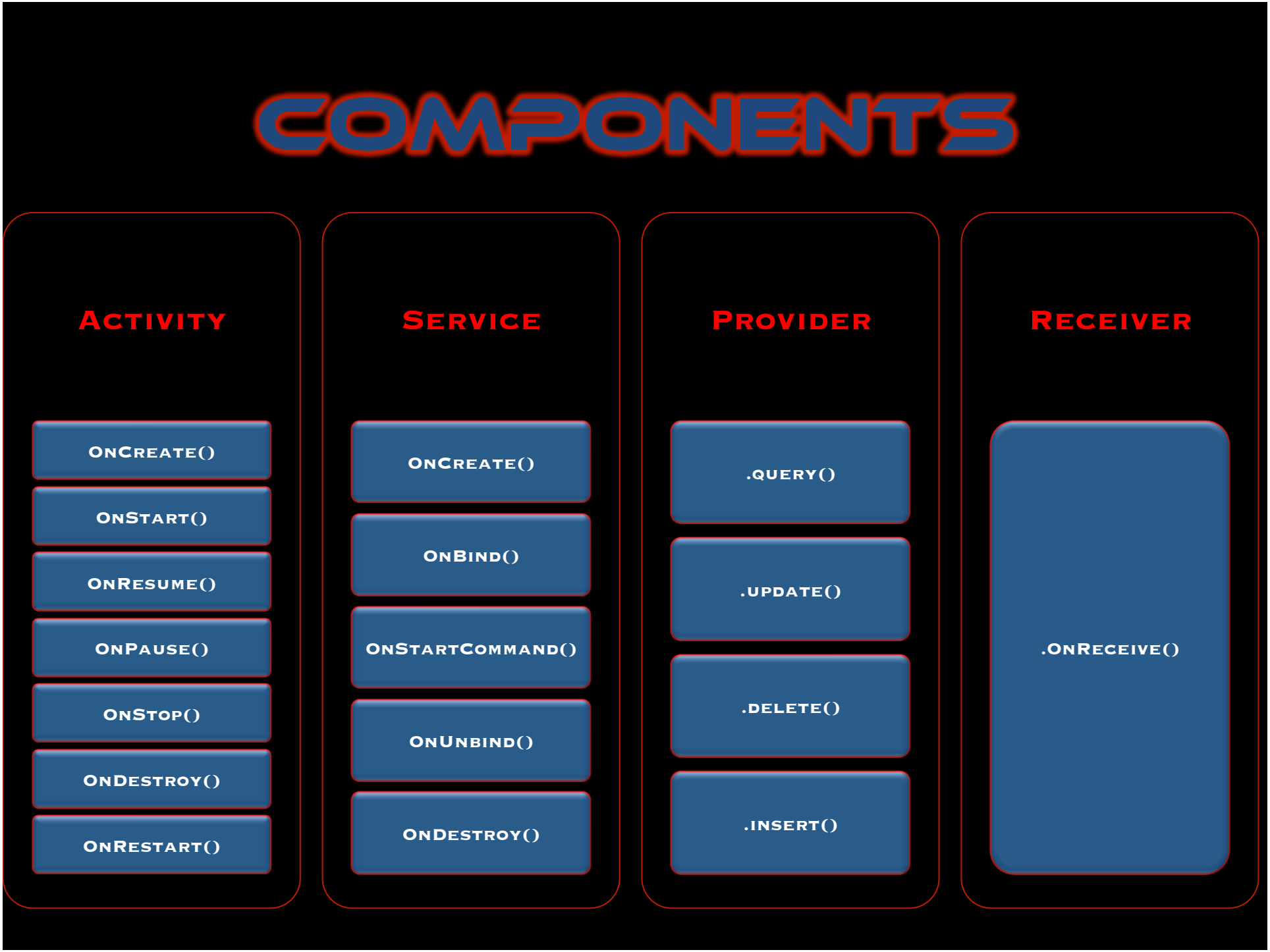
- Senior Information Security Engineer

APK STRUCTURE

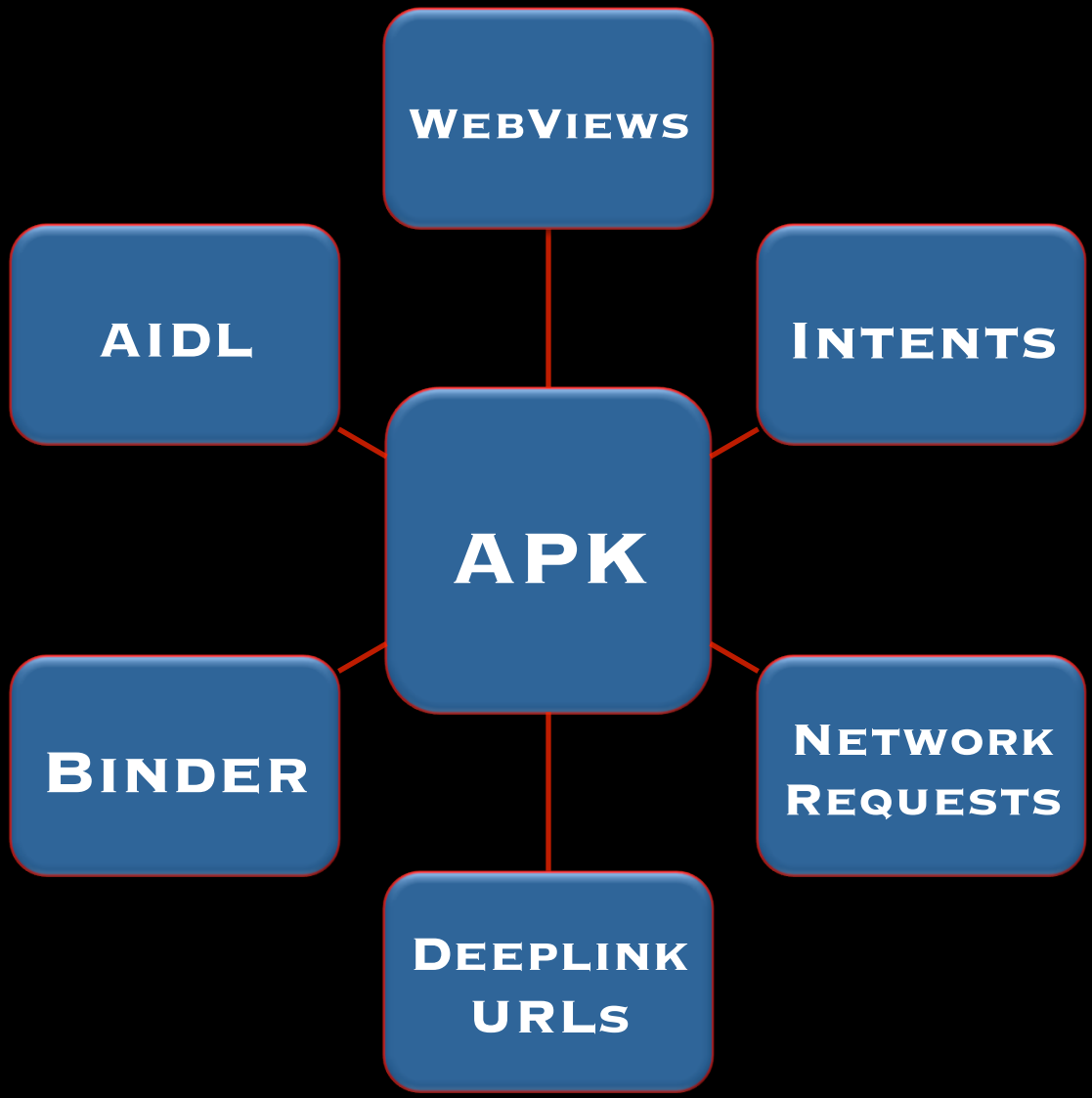


Reversing APKs




COMPONENTS
Activity
onCreate()
onStart()
onResume()
onPause()
onStop()
onDestroy()
onRestart()
Service
onCreate()
onBind()
onStartCommand()
onUnbind()
onDestroy()
Provider
.query()
.update()
.delete()
.insert()
Receiver
.onReceive()

COMMUNICATION



Android Issues

- Many sources – all the web bugs ++
- SSL/TLS fail – no ssl/tls & cert validation
- Lots of old devices – slow updating
- client-side fail – no one will ever know...

WHAT IS QARK?

- Quick Android Review Kit
- An improvement on other ideas/tools
- Lots of (horribly written) Python
- A pinch of innovation
- An auditing and attack framework

QARK MOTIVATION

We're lazy	Our boss is lazy	Developers are extremely lazy and ignore warnings
We ~~don't like~~ hate repeating bugs	We have lots of apps to protect	Lots of small dev shops (aka no security)

QARK'S MISSION

- Raise the bar for Android security
- Knowledge sharing
- Free SCA with validation
- Community involvement
- Motivate Google?

UNDER THE HOOD

- Parsing: PLYJ, BeatifulSoup, Minidom
- REVERSING: Procyon, JD-CORE,dex2jar, apktool
- Code: Python
- Tools & Building: ANDROID SDK

Data Acquisition

- Automates APK retrieval
- Decompresses APK
- Converts AndroidManifest.xml to text
- Parses AndroidManifest.xml

Parse Structure

- Identifies permissions issues, exported components, supported versions, etc.
- Parses Java classes
- Maps Manifest to classes
- Locates “entry point” methods
- Looks for sources of user-supplied data

SOURCE TO SINK

FOLLOW POTENTIALLY TAINTED INPUT

LOOK FOR MODIFIERS

RECORDS ANY “SINKS” ENCOUNTERED

REVIEW COMMS

Combines the information gathered with manifest details for later use

Examines WebView configurations and provides templated HTML files for validation of vulnerabilities

Looks for vulnerabilities originating from within the app, inspecting Broadcast, Sticky and Pending Intents

FINAL CHECKS

- Looks for WORLDREADABLE and WORLDWRITEABLE files
- Looks for tapjacking defenses
- Looks for X.509 certificate validation issues
- Creates a "deliverable" HTML report of findings

DEMO TIME !!

UNIQUE FEATURES

- Multiple decompilers to provide better results
- Builds an APK for manual testing
- swiss-army knife style set of functionalities
- creates ADB commands to exploit discovered vulnerabilities
- custom exploit APK facilitates point-and-click pwnage

QARK IS (NOT) YET

- A Forensics Tool
- A dynamic analysis tool
- perfect
- finished

FUTURE PLANS

- Dynamic analysis functionality
- Contribute to improve libraries and tools
- ~~Handle obfuscated code~~
- Smali inspection
- ~~Native code support~~
- Ask for your help

Where to get Qark?

LinkedIn's Git repo

https://github.com/linkedin/qark

Acknowledgements

- MWR Labs for Drozer (inspiration)
- Rafay Blaloch, et al, for the WebView exploits
- NVisium for the TapJacking code
- The authors and maintainers of all the opensource projects used in QARK
- Jason Haddix, Sam Bowne, et al, for supplying some vulnerable APKs

CONTACT INFO

www.secbro.com

Tony Trummer

+ www.linkedin.com/in/tonytrummer

@SecBro1

Tushar Dalvi

+ www.linkedin.com/in/tdalvi

@tushardalvi