Android Device Testing Framework

Blackhat USA 2014 Arsenal

Jake Valletta

August 07, 2014

https://github.com/jakev/dtf

Who Am I

- Consultant at Mandiant/FireEye
- Mobile security research and tool development
  - www.thecobraden.com/projects/
  - www.github.com/jakev/
- @jake_valletta

What is dtf?

- "Android Device Testing Framework"
  - Modular and extendable
- Written in Python and Bash
- Not a vulnerability scanner
  - Think of it as "lead generation"
- *Someone hands you a phone – Where are the vulnerabilities?*

Example Vulnerabilities

- Information disclosure
  - Can a malicious application or user "pillage" system or personal data?
- Privilege escalation
  - Can a malicious application or user escalate their privileges on the device?
- Denial of service
  - Can a malicious application cause denial of service like conditions to a device?

What it does Out of the Box

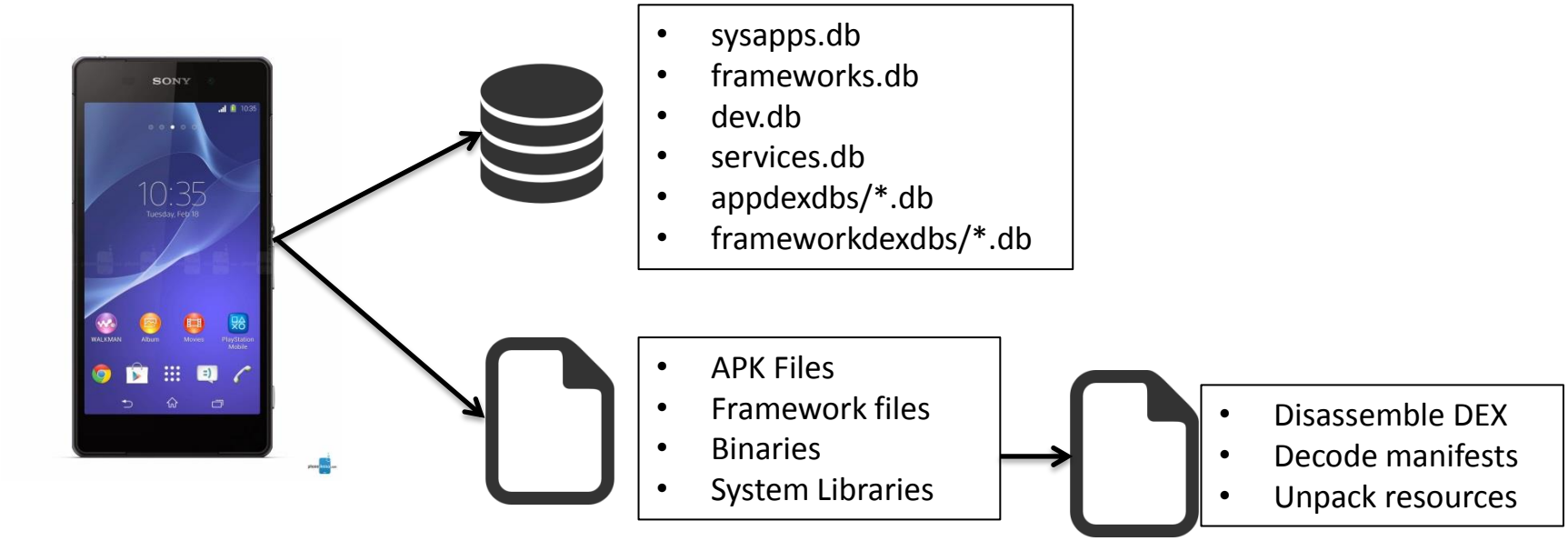
- Not much.
- Provides project management
- Package installer and module support
  - Modules perform all the exciting functionality!
  - dtf <module_name>

Modules?

- Python or Bash scripts
- I'll be releasing my collection of modules for testing
- Can also write your own ☺

My Modules…

- Collect information from device
- Unpack data and process into databases
- Provide APIs and modules to interact with the data



What's the Goal?

- Rapidly answer the questions:
  - What changed in Android Open-Source Project (AOSP) applications?
  - What is exposed in new OEM/carrier applications?

Blackhat Setup

- Two test devices
  - ZTE Open C with ZTE Kit Kat 4.4.2
  - Amazon Kindle HD with "FireOS 3.0"
- Physical access
- USB Debugging enabled
- No root access

Demos!

Closing Thoughts

- Device OEMs and carriers have a lot to learn
  - 1999 style issues
- Issues are extremely apparent, given the correct tools
- Be careful how much trust you put in your device!

Future Plans

- Remove Bash dependency
- Cross-platform support
- Continue to release modules and expand functionality
  - More automation?
  - GUI?

Questions?

https://github.com/jakev/dtf

Contact

- Twitter: @jake_valletta
- Email: javallet@gmail.com
- Site: www.thecobraden.com
- Blog: blog.thecobraden.com
- GitHub: www.github.com/jakev/dtf

Thanks!

https://github.com/jakev/dtf