Systematic Audit of Third-Party Android Phones

Michael Mitchell, Guanyu Tian, Zhi Wang

Motivation

- Android dominates the smartphone market
- Unlike iPhone which is made solely by Apple, many manufacturers make Android-based smartphones
  - ➥ hundreds of similar products
- Vendors are eager to differentiate their products through deep customization
- Such customization introduces **security issues not present in the official Android system**


Samsung

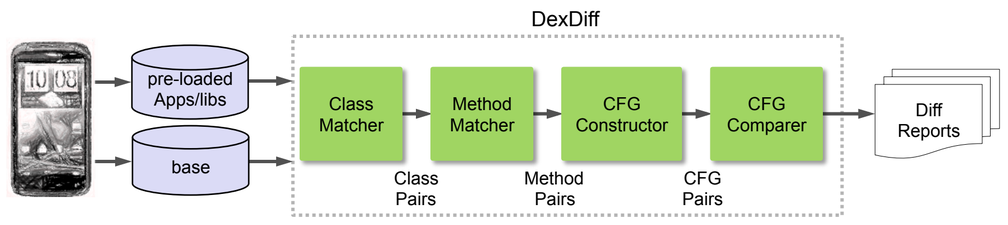

HTC

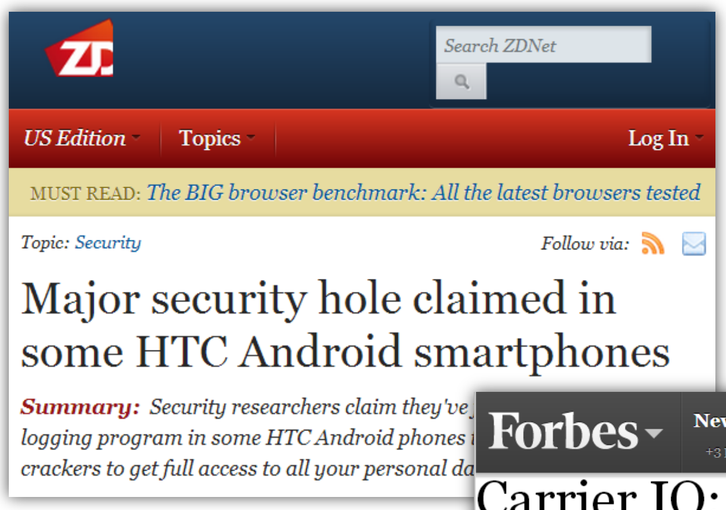

Motorola


LG

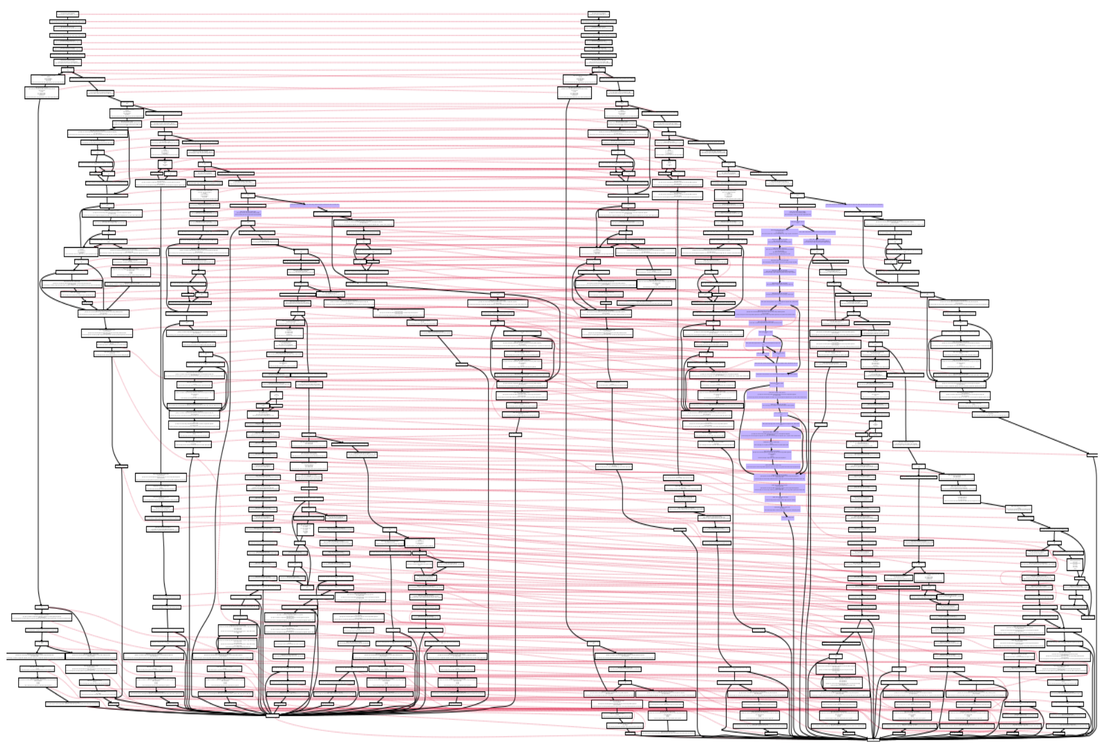
System Overview

- Input: two Android apps
- Output: fine-grained differences between these two apps
  - parse the apps into Java classes
  - convert Java classes into their graphic representation
  - compare them using **graph isomorphism**





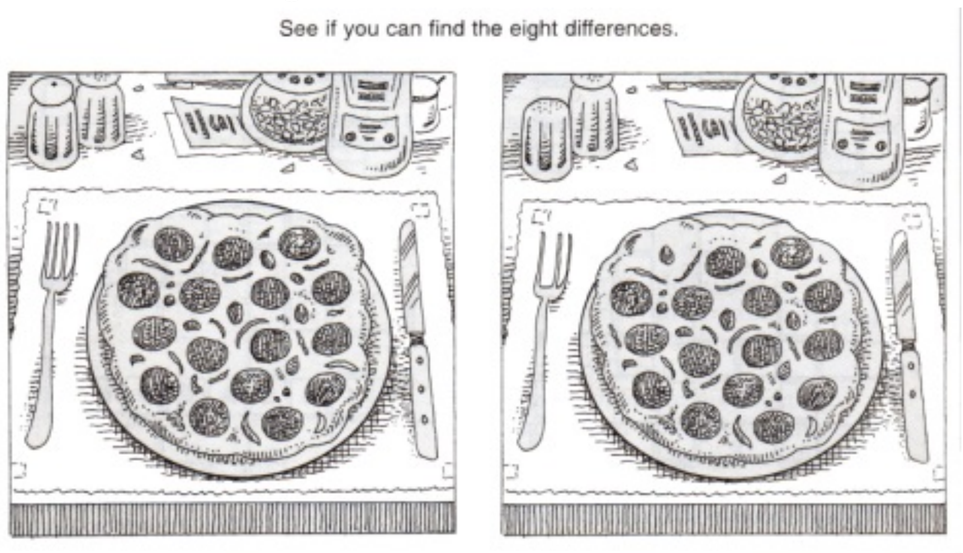
Example vulnerabilities introduced by vendor customization



Sample output of DexDiff
(there are much more complicated cases)

Our Approach

- Systematically compare third-party Android phones to Google's original Android system
  - what changes have been made?
  - are these changes safe?



Conclusion

- DexDiff can pinpoint fine-grained differences between Android apps
- Vendor customization tenders to introduce vulnerabilities not presented in the official Android system
- Using DexDiff, we
  - discovered new vulnerabilities in a HTC phone
  - revealed the details of very intrusive Carrier IQ software
- DexDiff can also be used to study Android malware
  - legitimate Android apps are often repackaged to piggyback malware
  - DexDiff can be used to dissect these malicious add-ons

4th ACM Conference on Data and Application Security and Privacy