



UCL Department of Computer Science
CS M038/GZ06: Mobile and Cloud Computing
2010–2011, Term 2
Kyle Jamieson and Brad Karp

One-pager: TaintDroid (Enck et al., 2010)

Due: Start of lecture, 9th March 2011

Instructions: in your own words, answer the following question as succinctly as possible (in 200–500 words, but shorter answers within this range are encouraged). Quoting figures or text from the assigned reading or from any other source is specifically prohibited.

TaintDroid disallows application developers from including their own native-code libraries in Android applications. Suppose instead that TaintDroid allowed apps to use native-code libraries, but was otherwise unchanged.

Describe how an app designer could trivially leak sensitive data to the network without TaintDroid's detecting the leak in this scenario. Justify your answer with relevant details of how TaintDroid propagates taint in native code. (Assume TaintDroid uses the same techniques for an app's native-code libraries as it does for system-provided native-code libraries.) Why did TaintDroid's designers taken such a false-negative-prone approach?