Master's Thesis Proposal

Analyzing, Inducing, and Capitalizing on Memory Faults in Android Systems

Name: Richard Roberts (ricro@seas.upenn.edu)

Thesis Advisor: Dr. Nadia Heninger
Thesis Reader: Dr. Jonathan M. Smith

Proposal

Capitalizing on faults in hardware is a popular attack vector for security researchers [4]. The rowhammer effect is one such fault, in which rapidly accessing a location in DRAM can result in the discharge of nearby capacitors and lead to soft memory errors [3]. Manipulating physical memory is a powerful attack vector in environments where an attacker controls a process that is co-located with target victim processes, such as two virtual machines hosted by the same cloud provider server.

For my Master's Thesis, I intend to investigate the effectiveness of these techniques in Android environments. Mobile phones are ideal candidates for fault attacks; malicious applications can easily run parallel to victim processes, and the mobile phones compact DRAM increases the likelihood of faults occurring. Creating payloads for fault-based attacks on physical hardware is rendered difficult by the unpredictability of such attacks; iterative testing is an expensive process, both in time and money, as hardware faults can easily lead to the destruction of test devices. I will create a systematic method of predictably testing malicious, fault-based Android payloads. This framework will then be used to test the effectiveness of previously unexplored targets of fault attacks, such as blockchain signatures [1]. Successful payloads would then be executed on real hardware.

Not all mobile memory faults come from malicious software. The cell phone is subjected to unique environmental conditions that may lead to soft memory errors that would not normally affect desktops or servers, such as rapid fluctuations in wireless transceivers. Excessive heat has also been shown to cause memory errors in desktop environments [2] but not yet on mobile phones; resource hungry processes can easily drive a phones temperature up, especially if the phone is kept in close proximity to the owners body. My thesis will include research into the effectiveness of these possible new methods of inducing memory errors in Android phones, including their predictability, reliability, and potential to be used as attack vectors for the aforementioned payloads.

References

[1] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, Eric Wustrow. *Elliptic Curve Cryptography in Practice*. Proceedings of the 18th International Conference on Financial Cryptography and Data Security, March 2014, pp. 157-175

[2] Sudhakar Govindavajhala, Andrew W. Appel. *Using Memory Errors to Attack a Virtual Machine*. IEEE Symposium on Security and Privacy, May 2003

[3] Yoongu Kim, Ross Daly, Jeremie Kim, Chris Fallin, Ji Hye Lee, Donghyuk Lee, Chris Wilkerson, Konrad Lai, Onur Mutlu. *Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors*. International Symposium on Computer Architecture 41, June 2014

[4] Tal G. Malkin, Francois-Xavier Standaert, Moti Yung1. *A Comparative Cost/Security Analysis of Fault Attack Countermeasures*. Proceedings of the 3rd International Workshop on Fault Diagnosis and Tolerance in Cryptography, October 2006, pp. 159-172