Title: Snatching Defeat From the Jaws of Victory: How to Do Everything Right and Still Design Hardware That Is Easy to Get Into

Speaker: Ron Minnich, Senior Staff Software Engineer, Google

Abstract:

One of the most commonly-used techniques for managing architecture and implementation limits is to provide a special processor mode which has special privileges. While this mode is intended to be used to implement infrequently-used operations in software instead of hardware, reducing overall cost, it is most commonly used to implement complex schemes to protect "core IP" or DRM management.

In this talk, I will present a representative set of examples of the use and abuse of these techniques, and how their initial, seemingly simple, nature, inevitably metastasizes into complex, buggy, code that frustrates any attempt to secure a platform. I'll close with a quick look at how a group of us are trying to address the problem.

Bio: