

Formal Methods in Computer Security? **The very idea!**

Once upon a time – as recently as the early 1990s, perhaps -- it was thought that someday we would be able to formally verify an entire computer system for security. Nowadays, however, you seldom hear about applications of formal methods to security beyond proving, say, protocols. In fact, even suggesting that formal methods have a place in security can get one laughed at. What happened to formal methods?

In this talk, I will give my opinion about why formal methods fell out of favor, and attempt to reassert why they have a larger place than just in proving the correctness of protocols, after all.

Oh, and some of you have been wondering what I am working on at Promia. I will talk about that, too. Call that part of the talk "So, will learning about Intrusion Detection help me get a job?"