I am a graduate student entering my PhD at University of Toronto, having just wrapped up my Masters. During my Masters, my research focused on mobile security, specifically on protecting sensitive applications from memory attacks (e.g. cold boot attacks) by using safe on-chip memory available on commodity ARM architectures. A large part of the evaluation in my Masters work forms the basis of the evaluation in a paper to appear in ASPLOS 2015, created in collaboration with individuals at Microsoft Research. Our paper focuses on providing an AES implementation on the ARM platform that is safe against DRAM attacks, such as cold boot attacks. With this AES implementation as an underpinning, we encrypt the user address space of sensitive applications when the phone suspends. When the phone is in use by an authenticated user (i.e. the PIN code of the screen is entered successfully), we decrypt pages on-demand. My work showed that the impact on battery life and the latency experienced during user interaction is negligible. Collaborators at Microsoft research also focused on supporting background applications which need to run impenetrable to DRAM attacks by never leaving plaintext data in DRAM. In my Masters work, I extend this idea to support background applications on the phone, such as receiving an email or listening to internet streaming services like Pandora. We run these applications entirely encrypted by decrypting pages into safe on-chip memory. Since the size of on-chip memory is limited, newly accessed pages can replace previously accessed pages by taking their spot, encrypting old pages back to DRAM. Further, I extended the ideas of a safe AES implementation to provide a secure execution environment for any cryptographic algorithm in the Linux crypto API without modification. In my PhD work, I would like to build on my experience in the mobile systems space, but also take this opportunity to branch out into areas such as virtualization. As such, I am interested in an opportunity to collaborate with the great minds at AT&T, and to extend my own expertise to tackle today's difficult research problems.

Regards,
James Gleeson