STATEMENT OF PURPOSE
as part of Professional Readiness Portfolio
submitted in Partial fulfillment of the requirements for a PhD
Information and Computer Sciences
University of Hawaii at Manoa
Nancy Mogire
nmogire@hawaii.edu

31 Dec 2015

Background

My primary research interest is in the area of security which is my current specialization for my PhD studies at UH Manoa. Specifically my current focus is security protocols. I believe that security will remain one of the most important aspects of computing technology because every new technology comes with a set of safety and security hazards. Each technology interacts with people, other technologies and the physical environment in a unique way. It is from this interaction that various safety hazards and security loopholes may be activated. Ill-meaning persons may attempt to launch attacks taking advantage of security loopholes on a system with intention to vandalize it, deny other users access to it or violate other users through the system various ways.

Security studies and research enable us to develop and test different controls on systems so that those in charge of such systems can be able to mitigate the safety and security risks that could arise during usage. Specifically security controls can: prevent unauthorized persons from accessing information not intended for them; prevent attacks that could damage systems or deny legitimate users access to it; reduce cases of unforeseen failure of systems and ensure that existing fail-over systems act in a timely and expected manner on occasions of failure caused either by human interference other accidents.

Protocols form an important part of security controls because through protocols the interactions of systems with other systems, users and the environment can be specified and in turn testing of such systems is more precise and more likely to reveal any loopholes for attack and safety hazard.

Security Protocols for Cyberphysical Space

Cryptographic protocols for interaction between systems on cyberspace can be specified and enforced during the engineering of the system and their testing can be and is often automated. However as computing has become more integrated in day to day life, computation has continued to happen more in physical space and systems consist of large and often amorphous interactions between computers, items with embedded computers, people and the natural environment. Reading recent security protocols literature, it becomes apparent that analyzing how systems interact with people and other objects is and will in the foreseeable future continue to be an important direction in security work with interesting problems in which I could make a contribution. This was my motivation for working on this specific subject area of security protocols for cyberphysical space.

Career goals

My professional goal ultimately is a career in industry. I would like to grow into developing security tools for use in the industry as well as work in security research and development. This goal may be pursued without going through the PhD route. However because I entered the computing career at masters degree level i knew that if I went into industry soon after i would always have the disadvantage of rushing through acquainting myself with important theoretical computing details. This would have taken from the time i would otherwise spend in developing deeper expertise in a specialized area. It would have also reduced my chances of accessing interesting jobs in the computing and particularly the

security industry. Hence I went this path primarily because I want to develop my expertise through intense reading and research that PhD time affords me. I ended up with the additional advantage that during my time i have gained decent exposure to theoretical and general computing by way of taking both graduate and undergraduate courses.

Progress

Classes I took include *discrete math*, *theory of computation*, *analysis of algorithms*, special topics courses on *security and economics* and on *integrated development environments*, a reading course on *cryptographic protocols* as well as an *introduction to scripting* course. Additionally I was able to make time to study other computing theory courses offered for free as *MOOCs* including *introduction to cryptography* on coursera.

I've also had the chance to participate in focused work in the area of security by way of reading, trying various security modelling techniques during my research assistantship as well as doing teaching assistantship for the *Security & Trust* course. Additionally I was a TA in software engineering for three semesters which gave me valuable skills I could combine with security knowledge to become a more skilled professional in my career. In 2015 I also had the chance to attend with my advisor Dusko a project review meeting in Washington DC where together with him i did my first research presentation talk on the actor networks formalism for modelling cyberphyscial space. I am optimistic that we are on track to publishing papers in cyberphysical protocols area in 2016.