September 13, 2015

Program Director
National Science Foundation (NSF)
Washington DC, USA

Dear NSF Program Director,

I am a senior researcher in the Office of the CTO at Intel Security. My research has been focusing on building the use case of Intel® Software Guard Extension (SGX), and analyzing the potential malware that uses Intel® SGX since 2013. I am also the technical point of contact of Dr. Lin's Intel® SGX malware analysis project supported by Intel®.

I am pleased to write this letter elaborating my collaboration commitment with Dr. Kim and Dr. Lin on their proposed SGX research. Since August 2015, SGX has been publically available, enabling new hardware level support in securing both data and instructions from unauthorized access. Previously, securing code against users heavily relied on trust of the operating system platform. By enabling the use of secure enclaves within the CPU instruction set, the operating system no longer needs to be trusted to maintain integrity of code execution. Intel® SGX provides the ability to secure code and data but further research into practical applications, special considerations, new security concerns and new software development models is needed. I am excited to learn that Dr. Kim and Dr. Lin are proposing developing open source "systems, tools and techniques for executing and securing SGX programs", which also gives me and my team members an opportunity of collaborating with the two PIs on some of their proposed research tasks.

Specifically we would be very much interested in being the first set of users to test all of the developed prototypes including their systems support, the tool chains, the sgxlib, and SGX execution sandbox. Second, my team and I would like to continue collaborating with Dr. Lin on SGX malware analysis. In particular, we would like to contribute our expertise and work together with the two PIs on extracting the best set of available features that can characterize the enclave program execution, an open problem to be solved in SGX program execution. Finally, of particular note is that I like the new proposed SGX program execution model that requires explicit system call specification. I believe this is a practical SGX execution model, and I would like to be engaged deeply in this proposed task.

To conduct this research, our Intel researchers including me plan to meet regularly with the PIs and their students, to discuss the technical details, and evaluate the proposed systems and tools.

I believe Dr. Kim and Dr. Lin's proposed project is very useful and may have significant impact on SGX software development. If you have any questions, please feel free to contact me.

Sincerely,

Charles McFarland

Charles McFarland
Senior MTIS Research Engineer
Office of the CTO
charles.mcfarland@intel.com
(972) 963-7140