Privacy-Aware Malware Detection
Sanghyun Hong, Parsa Saadatpanah, Mingfei Gao, and Andrew James Pachulski
\{shhong, pars, mgao, ajp\}@cs.umd.edu

Overview
In cloud-infrastructure, cloud service providers (e.g. Amazon Web Service, IBM Cloud, Microsoft Azure) are not allowed to access the content of customer virtual machines. In consequence, it is hard for the providers to protect their infrastructure from malware infections. As the virtual machines are usually created from a limited set of standard images and likely share many vulnerabilities, malware can propagate rapidly through cloud-infrastructure and cause damage a much larger scale.

Intellectual Merit
[4, 1, 3] have attempted to detect attacks in cloud-infrastructure. However, their methods need to introspect virtual machines, which potentially leads to privacy issues. Demme et al. [2] and Ozsoy et al. [5] proposes sub-semantic indicators effective in malware detection. In our project, we will introduce those indicators practically effective. Our privacy-preserving method will open new doors to cyber-security research in cloud environments.

Broader Impact
Researchers has introduced various advanced techniques to detect malware in customer virtual machines. Nonetheless, they require to access the context in virtual machines, which potentially leaks sensitive information of users. Our proposed framework prevents the issue fundamentally. It can spot malicious behaviors with high-accuracy using virtualization signals. With our approach, we can not only naturally protect privacy of users in our detection process, but we guarantee safe and robust cloud-infrastructure.

Cost, Time, and Risk
We believe that this project will take two full years to complete with an estimated total budget of $250,000 per year. Our project will be led by four PhD students, under the supervision of one member of faculty. The primary costs will be in funding the salaries of the faculty and students. Also, the system will require dedicated hardware which will need to be purchased, but is off-the-shelf at a modest cost. The potential risk to this project is competition in between commercial and academic sectors. Cloud service providers such as Amazon, Google, and Microsoft, has been working on similar technologies, but the risk will be mitigated by the fact that our solution is compatible to their current technologies.

References