Belief-Space Planning for Automated Malware Defense

Justin Svegliato, Sam Witty, Amir Houmansadr, Shlomo Zilberstein

College of Information and Computer Sciences

University of Massachusetts Amherst

{jsvegliato,switty,amir,shlomo}@cs.umass.edu

Malware detection and response is critical to ensuring information security across a wide range of devices. There have been few attempts, however, to develop security systems that exploit the benefits of different malware detection techniques. We formally introduce an automated malware defense framework and represent it as a belief-space planning problem that optimally reduces the impact on the performance of a system. Using the framework, we then provide an example automated malware defense system for email worm detection and response. Finally, we show in simulation that the system outperforms standard security techniques that have been used in practice. The result is a novel belief-space planning approach to auto- mated malware defense designed for robust, accurate, and efficient use in large networks of resource- constrained devices.

The full paper is available online. Please use the following link. I am sorry I could not create a PDF/A version and was not able to upload the file.

http://rbr.cs.umass.edu/shlomo/papers/SWHZijcaiAI4IoT18.pdf