BitAV: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning

Noyes, Charles

The prevalence of malicious computer viruses has exploded in recent years. Anti-malware software, the natural defensive corollary, has not innovated on the same level, leading to the need for a better alternative. This project centers around the design and implementation of BitAV, a novel anti-malware software environment that is far more efficient and effective than any other currently available solution. BitAV uses a novel variant of the Bitcoin blockchain to effectively decentralize its network of users and contributors. This allows for the trustless transacting of the identifiers of new malware variants between peers while maintaining the verifiability of the overarching network through distributed consensus. The scanning of suspect files using the information garnered by the networking module is based around a novel pattern matching mechanism that we call a feedforward bloom-bloomier filter. This scanning scheme operates in verifiably constant time across all inputs. The results of tests conducted against currently available industry anti-virus solutions showed an average decrease of 500% in time taken to identify novel malware variants. The pattern matching module was able to scan files 14x faster than the industry solutions, and this speed increase rose to over 20x when massively parallelized over CUDA. Besides being the most promising solution for the current problem with widespread malware, the novel underlying architectures in BitAV are widely applicable. The blockchain variant we designed is the first that could host purely informatory networks, meaning that things like blockchain-resident artificial neural networks are made easily possible. All code associated with this project has been open-sourced to further development in the area.

Awards Won:

First Award of $5,000

Intel ISEF Best of Category Award of $5,000

Philip V. Streich Memorial Award to the London International Youth Science Forum