Name(s)
Charles S. Noyes

Project Number
S1419

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

Abstract

Objectives/Goals
Anti-malware software is responsible for the protection of some of our society#s most important infrastructure. I have designed and implemented a novel anti-malware system (BitAV) that performs considerably better than all industry solutions I was able to test. Through the use of novel consensus protocols (adapted from those defined in the Bitcoin whitepaper) and fast, bit-vector-based scanning mechanisms I was able to greatly increase the speed of update propagation and malicious file identification.

Methods/Materials
Networking software was written in Python and the scanning mechanism in C++. Blockchains were chosen for their ability to be shared across a P2P network with assurances of canonicity and their ability to store arbitrary (but cryptographically verifiable) data. Bloom filters (and their derivatives) were chosen as data structures to be used in the feedfoward bloom-bloomier scanning mechanism for their speed in probabilistic pattern matching.

Results
Two tests were performed, one that measured propagation time of new malware identifiers and one that measured time taken to scan different malware samples. Scanning time showed the largest gain in performance, with an average increase of over 1,400% in speed ($p < 0.0001$, three sigma confidence), increasing by a factor of 2 to 3 with realistic input file-sets. Finally, the identification and propagation of novel malware variants happened, on average, 500% faster ($p < 0.00001$, four sigma confidence). All tests were conducted against (between 10 and 46) industry standard and OSS solutions.

Conclusions/Discussion
Ultimately I accomplished what I set out to achieve with this project. Further applications include over-the-air malware filtering and decentralized STIX/MAEC-over-TAXII networks, both of which are made possible with this software architecture. Additionally, my novel blockchain variant can be easily adapted to work with distributed associative memory networks, which make things like blockchain-resident neural networks, decentralized prediction markets, etc. a very real possibility.

Summary Statement
I created an application that efficiently protects users against malicious pieces of software, which works trustlessly across a peer-to-peer network using protocols similar to Bitcoin's.

Help Received
VirusTotal allowed me to use their databases of known malware and industry standard anti-virus solutions to compare the performance of my solution against currently available competitors. Chi So, professor of information security at USC, provided useful, tangentially related, discussion but was not involved in any