EXFILT   
Data Security Solution

Chapter 1

EXFILT will begin as a software-based set of technologies to prevent sensitive information from traveling outside of a computer network. The intent of the initial version is to create Intellectual Property and a prototypical Proof of Concept to be used for fundraising. As such, hardware/firmware based implementations involving FPGA’s, microprocessors and other embedded logic controllers are out of scope; but might be developed at a later date. Extensibility and interoperability with potential future non-software based implementations are not of major concern when building the initial prototype version.

Version 0.0

The goal for this iteration is to construct a FTP server and host, transfering files in between, establishing a ear program to calculate the SHA1 hash. The process will use deep packet inspection to detect a transfer of sensitive information by looking for the presence of a SHA1 hash. To allow us to focus on the complexities of getting a basic plugin functioning, the only protocol and transfer type addressed by this version will be an FTP Copy operation; and test data will simply be unencrypted plain-text files. Other formats and modes like .docx and .pdf files, or email attachments will be addressed in later iterations.

When the plugin detects sensitive information it will log the date/time, origin IP, destination IP, and other details depending on availability and usefulness. At this stage it will not attempt to terminate or block the transmission of data.