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 SNORT plugin (in C) for use with Wireshark. The plugin 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.

Version 0.1

This iteration involves the construction of a proxy server-like buffer (in Java) for accumulating the entire set of packets in a transmission, for subsequent inspection of file attributes (such as file type), and syntactic analysis against a cohesive file. The buffering system at this point does not need to implement any filtering/detection methods. It simply needs to be able to accumulate the packets in a transmission, then either stop the transmission by sending it forward, or forward the transmission on to its final destination.

Version 0.2

This iteration of the prototype will include one or more of the following, depending on priorities, time, resources and discoveries as they stand at the completion of Version 0.1:

1. An interface for end users to define syntactic filters (words, phrases and patterns) to be used for detecting sensitive information in transmissions accumulated in the Buffering system built in v0.1
2. Automated redaction of sensitive information through replacement of detected sensitive information patterns with innocuous text prior to re-transmission to the final destination
3. Support for file formats other than plain text (e.g.: .docx, .pdf, .xls, etc…) Open source, Java-based readers for various file formats might be used for this effort. Since the goal of Version 0 is a functional Proof Of Concept, proprietary document readers with lower latency can be built in later development efforts.
4. Support for filtering email attachments, as well as communication protocols other than FTP. This effort could encompass changes to both the Buffering and Filtering system and the SNORT plugin built in version 0.0.