Internet Infrastructure Services Corporation

Value Engineering – We bring Results and Speed

www.iis-corp.com

Founded in 2000, IIS is a small business located in New Jersey servicing the financial markets, the Regulated Utility, the evolving financial and healthcare compliance market place, and the Government Enterprise Architecture transformation requirement. Our team provides over 150 years of combined experience in process and operational management, technology innovation, and supply chain solutions. We achieve repeatable success in cultural change from concept to operations, acceptance of business/technology solutions, and exacting business profits.

File Verification

IIS has created a File Verification software solution. A JAVA based engine along with XML data/file format/standards descriptions provides an automated means to take one or more input files and

- Identify parseable known/published file/data format standards file types contained in the input files
- Locate specific byte ranges corresponding to defined fields in the format standard

The system processes each byte of each input file sequentially and provides means for random access for backwards references. The method supports static files or streaming data.

Configuration files are designed to handle all features of binary file structures including

- Fixed and variable length fields
- Starting/ending signatures and patterns
- Forward/backward offsets to data in the same or different file (sidecar file)
- Loops of fixed length or defined by input data
- Branching conditional logic
- Inherited endianness

Output of the analysis is a hierarchical tree showing each identified part of a known file format and corresponding byte locations in the data input file(s). Byte ranges which are not matched to any defined file format or which correspond to multiple different known formats are noted.

Output can be used directly to identify

- Metadata tampering, reordering, duplication, or invalid or unexpected format construction
- Areas of unused/unassigned bytes or areas which are parseable under multiple formats

Software may be further used as part of a hardened file (pre)parser by enforcing that only data meeting the published specification may be used by higher level software functions. For instance, when processing a file which is expected to be an image type, only byte ranges corresponding to the data format for that image type will be available outside of this software. This forces multiple personality files (eg: Image+JavaScript) to perform as a single personality file.

Software may be used as part of a larger security system. Machine learning can use identified part hierarchy to learn how a particular file generation software/process writes out fields which is then used to detect tampering or data stream substitution

The approach can be used as a malware mitigation strategy by automatically reordering fields without altering data to prevent a known offset data injection attack. It can be further used as a malware/exfiltration mitigation strategy by writing out a new file only including data assigned to known fields for a selected particular file format allowing for automatic adjustment to byte offsets for individual parts.

Currently, the patent-pending software is at TRL-3 and has been tested with various formats including JPEG, EXIF, and TIFF Headers for the purposes of metadata and source tampering detection.

Contact John Cavanaugh **|** Office (973) 252-6575 **|** Mobile (973) 960-6100 **|** johncavanaugh@iis-corp.com