5D-01

エントロピー実行形式検索技術のメモリイメージへの適用に関する一考察

高田　慎也　中村　亨　大田　幸由
NTT セキュアプラットフォーム研究所
takada.shinya@lab.ntt.co.jp

1.はじめに

類似するファイルを高速かつ高精度に見つけ出すことに対するニーズは高く、こうした技術分野で使用されるファイル類似度の評価方法としては、例えば、ファイルのエントロピー値を比較することで類似度を測定する方法の研究が盛んに行われている[1][2][3][4]。これに対してファイルを分割し、エントロピー値をファイルの区分ごとに計算し、得られるスペクトルに DP マッチングを施すエントロピー実行形式検索技術を提案してきた[5]。これにより類似度をより高精度に評価できることを示した[5]。この応用として非正規の実行形式がファイルを不正に操作するアプリケーションスプーフィングの防止への適用を提案した。一方、マルウェアなどの実行形式ではファイルの状態ではパッキングされているため、効果的な類似度評価を行うことが難しい。このため本稿では実行形式をメモリに展開し、そのメモリイメージをダンプして類似評価を行う手法について検討する。

2. エントロピー値の計算方法

エントロピー値は閉域系における順序性の程度の指標値である。エントロピー値の計算方式は、

$$\mathrm{E} = -\sum_{\mathrm{i}=0}^{255} \mathrm{P_i} \log_2(\mathrm{P_i})$$

で定義される。

3. ファイル分割による実行形式検索技術

これまで検討してきたエントロピーを用いた実行形式ファイル類似度評価方式について簡単に紹介する。これまでの検討で実行形式ファイル全体のエントロピー値を使って類似度を評価する方式は、誤検出が多いという結果が得られた。そこでファイルを分割し、区間ごとの差を比較する方式を考案した。

$$\text{類似度(差分平均)} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} |\mathrm{Ex_i} - \mathrm{Ey_i}|}{\mathrm{n}}$$

この式では、比較対象の 2 つの実行形式ファイルを区分に分割し、各区分での区分エントロピー値をそれぞれ（Exi, Eyi）求め、得られた値の差を取り、これを実行形式ファイルの最後まで繰り返した後、差分平均を計算することで類似性を評価する。差分平均が 0 の時 2 つのファイルは一致し、差の増大とともに 2 つのファイルの類似度は低くなり、最大値は 8 となる[3][4]。

しかしながらこの方式でも実行形式ファイルのエントロピースペクトルに発生するピーク位置のズレが誤差となることが判明したため、スペクトルの比較に DP マッチングを加えた比較方式を導いた。ここで DP マッチングは以下の式で表現される。

$\mathrm{X} = (x_1, x_2, \ldots, x_n)$、$\mathrm{Y} = (y_1, y_2, \ldots, y_n)$について

動的計画法により以下を計算

$$\mathrm{D(X,Y)} = f(n,m)$$

$$f(\mathrm{t,i}) = \|x_t - y_i\| + \min \begin{cases} f(t, t-1)\ X\ Stutter \\ f(t-1, i)Y\ Stutter \\ f(t-1, i-1)\ noStutter \end{cases}$$

$$f(0,0) = 0, \qquad f(t,0) = f(0,i) = \infty$$

DP マッチングを施した結果、Adobe 社 Acrobat の実行形式ファイルの Ver9.3.0、Ver10.1.0、Ver11.0.0 のマイナーバージョンの実行形式ファイル抽出を適合率、再現率ともに高スコア(≒100%)で実現することができた[5]。

4. マルウェア等の実行形式への応用上の課題

これまでに検討してきた評価方式は、一部がパッキングされたマルウェアについては、その類似性を良く評価できる。すなわちマルウェアのファイルの中でパックされている部分で局所的に高いエントロピー値を示し、このスペクトルは Windows の正規プログラムやアーカイブファイルでは見られないため、近年のパックされたマルウェア検体について、類似性を評価できる。一方フルパックされたマルウェアや自己解凍型の実行形式ファイルでは、スペクトル全体が高エントロピー値(＝８)に張り付いてしまうため、ファイルから類似性を評価することは難しい。

5. 改良方式案

４章で挙げた問題を解決するため、実行形式の類似評価をファイルではなく実行形式がメモリに展開された、プロセスのメモリイメージについて行うことを検討する。プロセスのメモリイメージのダンプには Microsoft 社が公開している、Toolkit Version 8.0 に含まれる User Mode Process Dumper Version 8.1 やタスクマネージャのダンプ機能を使用した。

6. 改良方式案のテストとメモリ評価の傾向

図 1 はテストとして行った Adobe Acrobat の Ver9.3.0 と Ver9.3.1 のメモリイメージのエントロピースペクトルを比較したものである。行ったテストから得られた、ファイルに対する分析との違いや傾向を表 1

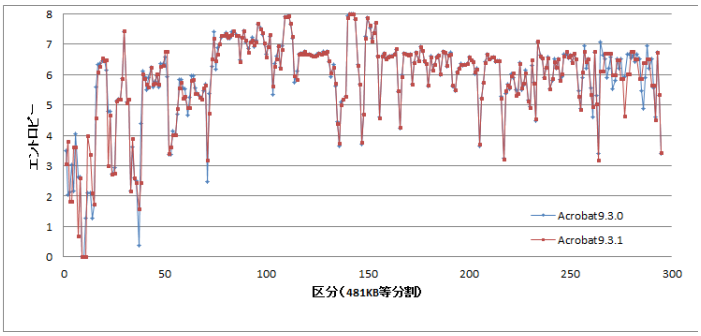

図 1　メモリイメージのエントロピースペクトル

表 1 ファイル分析とメモリイメージ分析の比較

	Acrobat9.3.0⇔Acrobat9.3.1	
	ファイル	メモリイメージ
ファイルサイズ	340KB程度	124MB程度
類似度(差分平均)	0.005	0.039
検索時間	0.003秒程度	0.03秒程度

にまとめた。一般的にファイルよりもメモリイメージの方が、容量が大きいため、分析に時間がかかることが分かった。また図のようにメモリイメージのエントロピースペクトルは全体的にスパイク状でありピーキーである。このため類似度(差分平均)の値はファイル解析の時と比べて、DP マッチングを施した場合であっても、類似性の高い実行形式においてさえ値が大きくなる傾向があることが分かった。また、一方で、一般的にプロセスではメインの実行形式から、dll といったライブラリが読み込まれる。プロセスのメモリイメージではファイルを対象に分析していた時ではできなかった、1 つのメイン実行形式に関係する複数の実行形式ファイル群の比較を総合的に行うことができると期待される。

7.メモリイメージの類似度評価の適用性

メモリイメージに対するエントロピー実行形式検索技術を使った類似度評価の適用性について述べる。ファイルの場合と異なり、類似検索対象群となるメモリイメージのダンプは数が限られる。このため非類似のメモリイメージのダンプを類似と誤判定してしまうケースが発生しないかを十分に検討することは難しい。従ってここでは、簡易に Windows で標準的に起動されているプロセス群のメモリイメージと検索対象となる Adobe 社 Acrobat の複数のマイナーバージョンのメモリイメージについて、類似性を誤検出なく評価できるかを調べた。結果を表 2 に示す。表 2 のようにベースとなる環境において、ファイル解析の時と同様に類似実行形式群(マイナーバージョン)を抽出できることが分かった。マルウェアの亜種についても同様のメモリイメージの解析から、類似検索できることが期待される。

表 2 Windows 標準プロセス中の Acrobat の抽出結果

adobe9.3.0に対する類似度(差分平均)	
adobe9.3.1	0.039
adobe9.3.2	0.107
adobe9.3.4	0.154
adobe9.3.3	0.162
csrss	0.347
IMECMNT	0.538
conhost	0.540
WmiPrvSE	0.701
explorer	0.722
lsass	0.754
wininit	0.791
svchost	0.801
sidebar	0.823
spoolsv	0.836
winlogon	0.885
taskhost	0.917
unsecapp	0.989
CCC	1.034
IMEDICTUPDATE	1.088
SearchIndexer	1.137
lsm	1.143
services	1.172
cmd	1.223
smss	1.589
dwm	2.160

7.複数ブラウザの類似度評価

本提案の方式を用いてブラウザ(Firefox、Google Chrome、IE)の類似性を評価した。表 3 に結果を示す。Firefox から見た場合(すべて Google の Web ページを 1 タブのみで表示した状態にした)、Chrome プロセス 1 との類似度(差分平均)が最も高く、Chrome プロセス 2 が最も低い値を取る結果となった。今回はブラウザの類似性について顕著な傾向はみられなかった。

表 3 ブラウザのメモリイメージの類似度評価

Firefoxに対する類似度(差分平均)	
chrome(プロセス1)	1.042
ie(プロセス1)	1.145
chrome(プロセス3)	1.360
chrome(プロセス4)	1.408
ie(プロセス2)	1.965
chrome(プロセス2)	2.430

8.今後の予定

本稿での検討の結果、エントロピー実行形式検索技術を実行形式のメモリイメージに対する分析に応用した場合、類似バイナリに対して限定的だが高い類似性を観察することができた。今後は、評価対象のメモリイメージの数を増やし、パックされた実行形式に対しても適用することで、期待通りの傾向が得られるか評価したい。

9.参考文献

[1] Mccreight et al. “System and method for entropy-based near-match analysis.” 国際特許 WO2010/107659 A1
[2]Davis et al.Guidance Software “Utilizing Entropy to Identify Undetected Malware”
[3]高田他”ファイルのエントロピー測定による類似度評価の新手法に関する提案” 第 60 回 CSEC 研究会
[4]高田他”ファイル類似度評価システムに関する考察” 第 76 回情報処理学会全国大会
[5]高田他”エントロピーと DP Matching を用いたファイル類似度評価システムに関する考察”第 77 回情報処理学会全国大会