DETECTING THREATENING INSIDERS WITH LIGHTWEIGHT MEDIA FORENSICS

Naval Postgraduate School & The University of Texas at San Antonio

Dr. Simson Garfinkel (NPS) & Dr. Nicole Beebe (UTSA)

8am, Wednesday November 13th, 2013
Team Profile

Naval Postgraduate School
• Simson L. Garfinkel
  Assoc. Prof
  Computer Science
  —simsong@acm.org
  —+1.202.649.0029

The University of Texas at San Antonio
• N. Beebe, Asst. Prof.
  Info Systems/Cyber Security
  —Nicole.Beebe@utsa.edu
  —+1.210.269.5647
The current approaches for finding hostile insiders are based on “signatures.”

Sample signature to find a problem employee:

(CERT 2011)

- if the mail is from a departing insider
- and the message was sent in last 30 days
- and the recipient is not in organization’s domain
- and the total bytes summed by day is more than X,

→ send an alert to security operator

These signatures are typically hand written.

—Brittle
—Don’t scale
—Miss new patterns
We propose a new approach for finding threatening insiders—storage profile anomalies.

Hypothesis 1:
Some insiders hoard before exfiltration

• Manning
• Snowden
Hypothesis 2:
Some illegal activity has storage indicators:

- Contraband software (hacking tools) and data
- Large amount of:
  ---- graphics
  ---- PII; PHI; account numbers
  ---- Encrypted data
- Stolen documents

Illegal employee activity is:
- Bad for business
- Exploitation threat
- Fraud risk

We also want to detect other kinds of illegal employee activity.
Our plan: look for storage devices that are different than their peers.

We build a “storage profile” from features:

- # of credit card numbers, phone #s; SSNs, DOBs, etc.
- % pictures; %video
- % Doc files; %PDFs;

“Different” relative to:

- User’s history
- User’s organization
- Others in role.

Our approach: Collect “storage profiles” and look for outliers.

We profile storage on the hard drive/storage device:
- Allocated & “deleted” files; Unallocated space (file fragments)

Statistical profile is collected:
- Frequently, at “random” times
- Securely — by going to raw media
- Centrally — at management console
We cluster the storage profiles to find “outliers.”

What’s an outlier?

- Something that’s different from its peers
- Something different from its own history
Outlier detection should have significant benefits:

- Not signature based
- Not reliant on access patterns
- Not reliant on policy definition, discovery, auditing

Design constraints:

- Agent must be scalable and cannot interfere with operations
  — Desktop: background process, samples disk data
  — Network load: small, aggregated data transfer
  — Management console: scalable algorithms used

- Must work with isolated systems
- Must be OS agnostic
- Must includes deleted data in collection/analysis
Our system has three parts:

1. Sample disk to collect desired data
   - bulk_extractor
     — a lightweight media forensics tool
     

2. Client-server, enterprise response framework
   - Google Rapid Response (GRR)

3. Anomaly detection agent
   - Univariate and multivariate outlier detection
Random sampling is a great way to analyze data.

Simple random sampling can determine % free space

Garfinkel, Simson, Vassil Roussev, Alex Nelson and Douglas White, *Using purpose-built functions and block hashes to enable small block and sub-file forensics*, DFRWS 2010, Portland, OR

Data characterization can determine the *kind* of stored data

Sector hashing can identify specific target files

It takes 3.5 hours to read a 1TB hard drive.

In 5 minutes you can read:

- 36 GB in one strip
- 100,000 randomly chosen 64KiB strips (assuming 3 msec/seek)

<table>
<thead>
<tr>
<th>Minutes</th>
<th>Data</th>
<th># Seeks</th>
<th>% of data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 TB</td>
<td>1</td>
<td>100%</td>
</tr>
<tr>
<td>208</td>
<td>36 GB</td>
<td>1</td>
<td>3.6%</td>
</tr>
<tr>
<td>5</td>
<td>6.5 GB</td>
<td>100,000</td>
<td>0.65%</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The statistics of a randomly chosen sample predict the statistics of a population.

US elections can be predicted by sampling thousands of households:

The challenge is identifying likely voters.

Hard drive contents can be predicted by sampling thousands of sectors:

The challenge is identifying the sector content that is sampled.
We think of computers as devices with files.
Data on computers is stored in fixed-sized sectors.

Data in a sector can be resident:

- **Files**
  - MagicPlan 1.5.ipa
  - MarbleMail 1.2.9.ipa
  - MarketDash 1.2.1.ipa
  - Memory Cards 4.3.0.ipa

- **Deleted Data**
  - MagicPlan 1.5.ipa
  - MarbleMail 1.2.9.ipa
  - MarketDash 1.2.1.ipa
  - Memory Cards 4.3.0.ipa

- **No Data**
  - blank sectors

Files can be “deleted” but the data remains.

Sectors can be wiped clean:

- **user files**
- **email messages**
- **[temporary files]**
Allocated data are the data you see from the root directory. e.g. “visible” files.
“Deleted data” are on the disk, but can only be recovered with forensic tools.
Some sectors are blank. They have “no data.”
Sampling can’t distinguish *allocated* from *deleted*.
Sampling can tell us about the content of the data

Sampling can tell us the proportion of...

—blank sectors; video; HTML files; other data types...
—data with distinct signatures...

...provided we can identify it
Challenge for sampling: interpreting each sector

—Easy:

```
0000000: ffd8 ffe0 0010 4a46 4946 0001 0201 0048 ......JFIF.....H
0000010: 0048 0000 ffe1 1d17 4578 6966 0000 4d4d .H..Exif.MM
0000020: 002a 0000 0008 0007 0112 0003 0000 0001 .*......
0000030: 0001 0000 011a 0005 0000 0001 0000 0062 ...........
0000040: 011b 0005 0000 0001 0000 006a 0128 0003 ...........j.
0000050: 0000 0001 0002 0000 0131 0002 0000 001b ..........1...
0000060: 0000 0072 0132 0002 0000 0014 0000 008d ...r.2........
0000070: 8769 0004 0000 0001 0000 00a4 0000 00d0 .i............
0000080: 0000 0048 0000 0001 0000 0048 0000 0001 ..H......H...
0000090: 4164 6f62 6520 5068 6f74 6f73 686f 7020 Adobe Photoshop
00000a0: 4353 2057 696e 646f 7773 0032 3030 353a CS Windows.2005:
00000b0: 3035 3a30 3920 3136 3a30 313a 3432 0000 05:09 16:01:42...
00000c0: 3000 0003 a001 0003 0000 0001 0001 0000 ............
00000d0: a002 0004 0000 0001 0000 00c8 a003 0004 ............
00000e0: 0000 0001 0000 0084 0000 0000 0000 0006 ............
00000f0: 0103 0003 0000 0001 0006 0000 011a 0005 ............
```

—Hard:

```
000a000: 0011 fa71 57f4 6f5f 00bd 15fb 5dfd ...qW.o.....]
000a010: a996 0fc9 dff1 ff00 b149 e154 97f4 efd5 .........I.T..
000a020: e3f5 7f47 71df 8ff8 d5d7 da9e d87f c12f ....Gq........
000a030: f8ff 00d8 b1f4 b1f8 ff00 c57e ab7a ff00 ........~.z..
```
We use two approaches for identifying data type.

1 - SVMs with multiple feature types
   • unigrams
   • bigrams (selected)
   • Other n-grams & complexity measures
   • compressibility
   • hand-tuned classifiers


2 - Known content
   • Database of “sector hashes.”
Sceadan provides the “type” of fragments.

**Additional model training has improved classifier accuracy from 71.5% to 73.5%**

**Sceadan v1.0**

73.5% Accuracy*

40 Classes

**NOTE:** 9 lowest performing types are significantly under-researched classes (e.g. Office2010, FS data)

**Number of Classes Predicted by Classifier**

*Additional model training has improved classifier accuracy from 71.5% to 73.5%*
Improved performance comes from feature set. Training is slow, but only needs to be done once.

Trigrams proved most accurate (70.19%)
- Much slower prediction time than competing alternatives

“FS5” (feature set 5) nearly as accurate (69.83%)
- Unigrams+Bigrams+Other
  - Other features: entropy, Kolmogrov complexity, mean byte value, Hamming weight, avg. contiguity between bytes, longest byte streak

<table>
<thead>
<tr>
<th>Features</th>
<th>Train.Time</th>
<th>Pred.Time</th>
<th>accuracy</th>
<th>Train.Time</th>
<th>Pred.Time</th>
<th>accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>unigrams</td>
<td>19m 9.518s</td>
<td>4.208s</td>
<td>55.99%</td>
<td>29m 46.439s</td>
<td>4.162s</td>
<td>48.20%</td>
</tr>
<tr>
<td>bigrams</td>
<td>5h 22m 21.391s</td>
<td>31.286s</td>
<td>68.12%</td>
<td>4h 34m 39.545s</td>
<td>32.649s</td>
<td>68.26%</td>
</tr>
<tr>
<td>trigrams</td>
<td>174h 46m 5.795s</td>
<td>7m 47.676s</td>
<td>62.76%</td>
<td>211h 8m 47.311s</td>
<td>7m 23.068s</td>
<td>70.19%</td>
</tr>
<tr>
<td>uni+bi</td>
<td>7h 39m 46.240s</td>
<td>36.019s</td>
<td>68.68%</td>
<td>3h 54m 36.043s</td>
<td>37.834s</td>
<td>67.06%</td>
</tr>
<tr>
<td>FS5</td>
<td>7h 51m 35.550s</td>
<td>35.111s</td>
<td>69.83%</td>
<td>7h 27m 34.618s</td>
<td>36.697s</td>
<td>68.92%</td>
</tr>
</tbody>
</table>
Some kinds of files have distinct contents.

Can you identify a JPEG file from reading 4 sectors in the middle?

```
JPEG File
```

```

Header

Icons

EXIF

Color Table

Huffman Encoded Data

Footer

[FF D8 FF E0] or [FF D8 FF E1]

[FF D9]
```
We can identify “distinct” sectors.

In a compressed or encrypted file, each sector is different.

- Header: [FF D8 FF E0] or [FF D8 FF E1]
- 4096 bytes not repeated elsewhere
- 41,572 bytes
- [FF D9]
Initial anomaly detection results are promising.

Successfully detecting univariate outliers

• Data by type most effective thus far
  — *File types* (e.g., *jpg*, *exe*)
  — *Data types* (e.g., *PII*, *CCN*)

• Median absolute deviation (MAD) based outlier detection with conditional scaling procedures

Multivariate and time-series based outlier detection — on-going

• Cluster based, SOM based, etc.
This heatmap of anomalies let an analyst easily identify clusters and outliers.
Current status — We’re making progress!

bulk_extractor updated v1.4 just released
• Added features & GRR integration preparation

Sceadan data type classifier updated v1.2 released

Extraction, transformation, loading of datesets
• M57 Patents (digitalcorpora.org) case

Progress on anomaly detection algorithm
• Real Data Corpus extraction, translation and loading near complete
• Theoretical development
• Empirical data descriptive analyses (test assumptions)
• Univariate anomaly detection performing well on synthetic data set
We are in year 1 of a 3-year effort.

<table>
<thead>
<tr>
<th>Year</th>
<th>NPS Lead</th>
<th>UTSA Lead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year 1</td>
<td>bulk_extractor upgrades</td>
<td>Outlier detection algorithm Synthentic data experimentation Real Data Corpus experimentation</td>
</tr>
<tr>
<td>Year 2</td>
<td>Integrate GRR Develop/test management console</td>
<td>Develop/test data outlier detection Develop/test visualization component</td>
</tr>
<tr>
<td>Year 3</td>
<td>Large-scale testing on partner net</td>
<td>Final dev. of outlier detection algorithm Final dev. of visualization agent</td>
</tr>
</tbody>
</table>
Many challenges remain.

“Anomalous” suggests “normal” exists
- Large, diverse, dislocated organizations
- High fluidity and variety in workforce
- Remote, mobile, multi-device access requirements
- Uninterruptible, critical computational operations

Clustering algorithm selection/development
- Accuracy and speed trade-off of extant algorithms
- Develop combinatorial algorithm to improve accuracy
- Need for automated parameter selection amidst noise
- Feature selection

Engineering of visualization component
In conclusion, we are developing a system that uses “lightweight media forensics” to find hostile insiders.

We use random sampling to build a storage profile of media.

We collect these profiles on a central server.

We cluster & data mine to find outliers.

Contact:
  • Simson L. Garfinkel simsong@acm.org
  • Nicole Beebe Nicole.Beebe@utsa.edu