Open-source Intelligence as a means to reveal Insiders and protect Critical Infrastructures

Dimitris Gritzalis

May 2014
Open-source Intelligence as a means to reveal Insiders and protect Critical Infrastructures

Dimitris A. Gritzalis (dgrit@aueb.gr, www.infosec.aueb.gr)
Professor and Director
Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory
Dept. of Informatics, Athens University of Economics & Business, Greece
Key concepts of the presentation

Asset:
- Critical Infrastructure

Threat:
- Insider

Defense:
- Open-source Intelligence

Data source:
- Social Media
The Threat and the Defense

Threat:
Insiders are persons who:
- are legitimately given access rights to a Critical Infrastructure
- misuse their privileges and violate security policy

Defense:
Open-source Intelligence (OSINT) is produced from publicly available information that is collected, exploited, and disseminated:
- in a timely manner
- to an appropriate audience
- for addressing a specific intelligence requirement
Insider threat impact

The Insider Threat

Internal Process Knowledge

High                  Low

High

Greatest Threat       Demonized But Insignificant

Low

Technical Literacy

High

Significant Threat    Insignificant

Low

Source: GartnerGroup Report 5605
Behavior classification model
The Social Media arena: What happens online in 60sec
Case 1
Scope: Revealing a potential Insider

### Tools used for the analysis

<table>
<thead>
<tr>
<th>Science</th>
<th>Theory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computing</td>
<td>Graph Theory</td>
</tr>
<tr>
<td>Sociology</td>
<td>Theory of Planned Behavior</td>
</tr>
<tr>
<td></td>
<td>Social Learning Theory</td>
</tr>
</tbody>
</table>
Case 1: Insider threat prediction based on narcissism

Twitter (Greece, 2012-13)

1.075.859 users
41.818 fully crawled users
7.125.561 connections among them.

Analysis framework based on:
- Theory of Planned Behavior
- Social Learning Theory

Medium graph-theoretic analysis by:
- Small World Phenomenon
- Indegree distribution
- Outdegree distribution
- Usage intensity distribution

User behavior analysis by:
- Social Medium Usage Intensity
- Social Medium Influence valuation
- Klout score (user influence)

---


Case 1: Insider threat prediction based on narcissism

- **Small World Phenomenon**
  - 99% of the users is ≤6 hops away from everyone else in the graph.

- **Indegree distribution**
  - Distribution of *incoming edges at each node*. Finding: 13.2 followers/user, on average.

- **Outdegree distribution**
  - Distribution of *outgoing edges at each node*. Finding: 11 followings/user, on average.

- **Usage Intensity distribution**
  - Distribution of the evaluation of usage intensity per user

<table>
<thead>
<tr>
<th>Category</th>
<th>Influence valuation</th>
<th>Klout score</th>
<th>Usage valuation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loners</td>
<td>0 - 90</td>
<td>3.6 - 11.1</td>
<td>0-500</td>
</tr>
<tr>
<td>Individuals</td>
<td>90 - 283</td>
<td>11.1 - 26.0</td>
<td>50-4500</td>
</tr>
<tr>
<td>Known users</td>
<td>283-1011</td>
<td>26.0 - 50.0</td>
<td>45-21000</td>
</tr>
<tr>
<td>News Media &amp; Personas</td>
<td>1011-3604</td>
<td>50.0 - 81.99</td>
<td>21000- 569000</td>
</tr>
</tbody>
</table>
Revealing an insider’s attitude

- Insiders have been found to be narcissists
- Narcissistic behavior is detectable using specific metrics
- OSINT produced from Twitter may reveal a narcissist
- CI management may take this finding into account
### Case 2
Scope: Revealing negative attitude against law enforcement

<table>
<thead>
<tr>
<th><strong>OSINT</strong></th>
<th><strong>Social Medium: YouTube</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tools used for the analysis</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Science</strong></td>
<td><strong>Theory</strong></td>
</tr>
<tr>
<td>Computing</td>
<td>Machine Learning</td>
</tr>
<tr>
<td></td>
<td>Data Mining</td>
</tr>
<tr>
<td>Sociology</td>
<td>Social Learning Theory</td>
</tr>
</tbody>
</table>
**Case 2: Revealing negative attitude against law enforcement**

**YouTube** (Greece, 2006-13)

<table>
<thead>
<tr>
<th>Classifier</th>
<th>NB</th>
<th>SVM</th>
<th>LR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classes</td>
<td>P/N</td>
<td>P/N</td>
<td>P/N</td>
</tr>
<tr>
<td>N</td>
<td>71%</td>
<td>83%</td>
<td>86%</td>
</tr>
<tr>
<td>P/N</td>
<td>70%</td>
<td>77%</td>
<td>76%</td>
</tr>
</tbody>
</table>

- **Precision**: Number of users correctly classified/number of users classified in the category.
- **Recall**: Number of users correctly classified/number of users classified in the category.
- **F-Score**: Harmonic mean of Precision and Recall. F = 2 * P * R / (P + R)
- **Accuracy**: The percentage of correct classifications.

**Analysis framework based on:**
- Social Learning Theory

**Behavior analysis based on:**
- Machine Learning
- Content Process
- User-generated content Classification

1 **NBP**: Naïve Bayes, **SVM**: Support Vector Machines, **LR**: Logistic Regression
2 **N**: Negative attitude, **P/N**: Positive/Neutral attitude
Revealing a negative attitude against law enforcement attitude

- Disposition towards law enforcement may be revealed through specific classifiers

- OSINT produced from YouTube may detect such an attitude

- CI management may take this finding into account
Generic conclusions

An **Insider** is a **major threat** to any **Critical Infrastructure**

**+** OSINT can be used to reveal insiders and persons with a negative attitude against the law

**+** Social Media are proved to be valuable data sources

**-** OSINT may lead to undesirable "**horror stories**"

**-** Ethical and legal issues are to be taken into account


