Holistic Information Security: Human Factor and Behavior Prediction using Social Media

Dimitris Gritzalis

January 2014
Holistic Information Security: Human Factor and Behavior Prediction using Social Media

Dimitris Gritzalis
Professor and Director
Information Security & Critical Infrastructure Protection Laboratory
Athens University of Economics & Business
Outline

- Insider Threat
- Threat Definition
- Malevolent User Needs
- Personal Factors
- Delinquent Behavior Prediction
- Narcissism Detection
- Predisposition towards Law Enforcement
- Divided Loyalty
- Group Homogeneity
- Ethical and Legal Issues
- Conclusions
Insider Threat

- Critical problem in cyber/corporate security
- Threats originating from people given access rights to systems and misuse privileges violating security policy
- Major fronts in the battle against insider threat:
  - Detection
  - Prevention/Deterrence
  - Prediction
    - Automated evaluations via social media and Open Source Intelligence
    - Examination of the predisposition towards malevolent behavior
    - Conclusions over users psychosocial traits to predict their behavior
Threat Definition

- Motive
- Opportunity
- Vulnerability
- Skills
Malevolent User Needs

- Opportunity
- Motive
- Ability to overcome inhibitions
- Stimuli/impulse.
Personal Factors (1/2)

- Introversion
- Social and Personal Frustrations
- Computer Dependency
- Ethical “Flexibility”
- Reduced Loyalty
- Entitlement – Narcissism
- Lack of Empathy
- Predisposition towards law enforcement
Personal Factors (FBI)

- Greed/Financial Need
- Anger/Revenge
- Problems at work
- Ideology/Identification
- Divided Loyalty
- Adventure/Thrill
- Vulnerability to blackmail
- Ego/Self-image (Narcissism)
  - Ingratiation
  - Compulsive and destructive behavior
- Family problems
Integrated

- Motive
- Opportunity
- Vulnerability
- Skills

Threat elements

Malevolent User Needs

- Opportunity
- Motive
- Ability to overcome inhibitions
- Stimuli/impulse.

Shaw’s Personal Factors

FBI Personal Factors

- Greed/Financial Need
- Anger/Revenge
- Problems at work
- Ideology/Identification
- Divided Loyalty
- Adventure/Thrill
- Vulnerability to blackmail
- Ego/Self-image (Narcissism)
- Ingratiation
- Compulsive and destructive behavior
- Family problems

- Introversion
- Social and Personal Frustrations
- Computer Dependency
- Ethical “Flexibility”
- Reduced Loyalty
- Entitlement – Narcissism
- Lack of Empathy
- Predisposition towards law enforcement
Behavior Prediction Theories

**General Deterrence Theory (GDT):** Person commits crime if expected benefit outweighs cost of action

**Social Bond Theory (SBT):** Person commits crime if social bonds of attachment, commitment, involvement and belief are weak

**Social Learning Theory (SLT):** Person commits crime if associates with delinquent peers

**Theory of Planned Behavior (TPB):** Person’s intention (attitude, subjective norms and perceived behavioral control) towards crime key factor in predicting her behavior

**Situational Crime Prevention (SCP):** Crime occurs when both motive and opportunity exist
Narcissism Detection

• **Twitter** Social Medium
• Graph: 1,075,859 users, 7,125,561 connections among them
• 41,818 fully crawled users
• Medium analysis via:
  – Strongly Connected Components
  – Node Loneliness
  – Small World Phenomenon
  – Indegree Distribution
  – Outdegree Distribution
• User analysis via:
  – Social Medium Usage Intensity
  – Social Medium Influence Valuation
  – Klout score
Predisposition towards Law Enforcement

- **YouTube** Social Medium
- Dataset: 2.043.362 comments, 207.377 videos, 12.964 users
- Identification of a user’s attitude towards law enforcement and authorities
- Utilize machine learning, content analysis and usage deviation
- Comment/user classification and flat data classification results converge

<table>
<thead>
<tr>
<th></th>
<th>NBM</th>
<th>SVM</th>
<th>LR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classes</td>
<td>P</td>
<td>N</td>
<td>P</td>
</tr>
<tr>
<td>Precision</td>
<td>71</td>
<td>70</td>
<td>83</td>
</tr>
<tr>
<td>Recall</td>
<td>72</td>
<td>68</td>
<td>75</td>
</tr>
<tr>
<td>F-Score</td>
<td>71</td>
<td>69</td>
<td>79</td>
</tr>
<tr>
<td>Accuracy</td>
<td>70</td>
<td>80</td>
<td>81</td>
</tr>
</tbody>
</table>

**Metrics**

- **Law Enforcement Predisposition**
  - Motive, Anger, Frustrations, Predisposition towards law enforcement
  - Social Learning Theory
Divided Loyalty

- **YouTube** Social Medium
- Same dataset
- Political profiling conclusion extraction
- Radical - Neutral - Conservative clusters
- Machine learning and content analysis of the dataset

### Algorithm: Multinomial Logistic Regression (MLR)

<table>
<thead>
<tr>
<th>Categories Metrics</th>
<th>Centre &amp; Centre-left</th>
<th>Neutral</th>
<th>Centre &amp; Centre-right</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precision</td>
<td>83%</td>
<td>91%</td>
<td>77%</td>
</tr>
<tr>
<td>Recall</td>
<td>77%</td>
<td>93%</td>
<td>78%</td>
</tr>
<tr>
<td>F-Score</td>
<td>80%</td>
<td>92%</td>
<td>77%</td>
</tr>
<tr>
<td>Accuracy</td>
<td></td>
<td>87%</td>
<td></td>
</tr>
</tbody>
</table>

**Motive, ideology, divided/reduced loyalty, predisposition towards law enforcement**

**Social learning theory, General Deterrence Theory**
Group Homogeneity

- **Twitter** Social Medium
- Group dynamics analysis via narcissism
- Group homogeneity analysis:
  - Newcomer fitting to an existing group
  - Existing group analysis
  - Social media behavior similarity to other users’ of the same profession

Group Homogeneity Analysis

Motive, Problems at work, narcissism, entitlement

Social Bond Theory, Social Learning Theory
Interdisciplinary capabilities

- **Narcissistic Behavior Detection**
  - Motive, Ego/Self-image, Entitlement
  - Theory of Planned Behavior, Social Learning Theory

- **Group Homogeneity Analysis**
  - Motive, Problems at work, narcissism, entitlement
  - Social Bond Theory, Social Learning Theory

- **Law Enforcement Predisposition**
  - Motive, Anger, Frustrations, Predisposition towards law enforcement
  - Social Learning Theory

- **Political Profiling**
  - Motive, ideology, divided/reduced loyalty, predisposition towards law enforcement
  - Social learning theory, General Deterrence Theory

*Horror story!*
Ethical and Legal Issues

- Aggregating/assessing content produced in different context and other purposes
- Ethics and democracy boundary of classification/predictability of human behavior
- Users do not have clear idea about actual reach of info they reveal
- Interfere with the right to informational privacy
- Associated with discrimination and prejudice risks
- Infringe fundamental rights (freedom of speech, conception of identity)
- Self-censorship and self-oppression
- Major problems both in workplace and social environment
- Derogations allowed:
  - On a manifest of public interest
  - Explicit, informed and written consent of the person concerned
  - Processing relates to data made public by the data subject
- Democracy test: “Is it necessary in a democratic state”? 
Conclusions

✓ Interdisciplinary approaches to fight the insider threat
✓ User/usage profiling leads to user classification
✓ Predisposition assessment identifies delinquent behavior
✓ Serious ethical and legal issues may arise
✓ Confined application to Critical Infrastructures
References


