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

Threat elements

Malevolent User Needs

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

Malevolent User Needs

Personal Factors (1/2)

Personal Factors (Shaw)

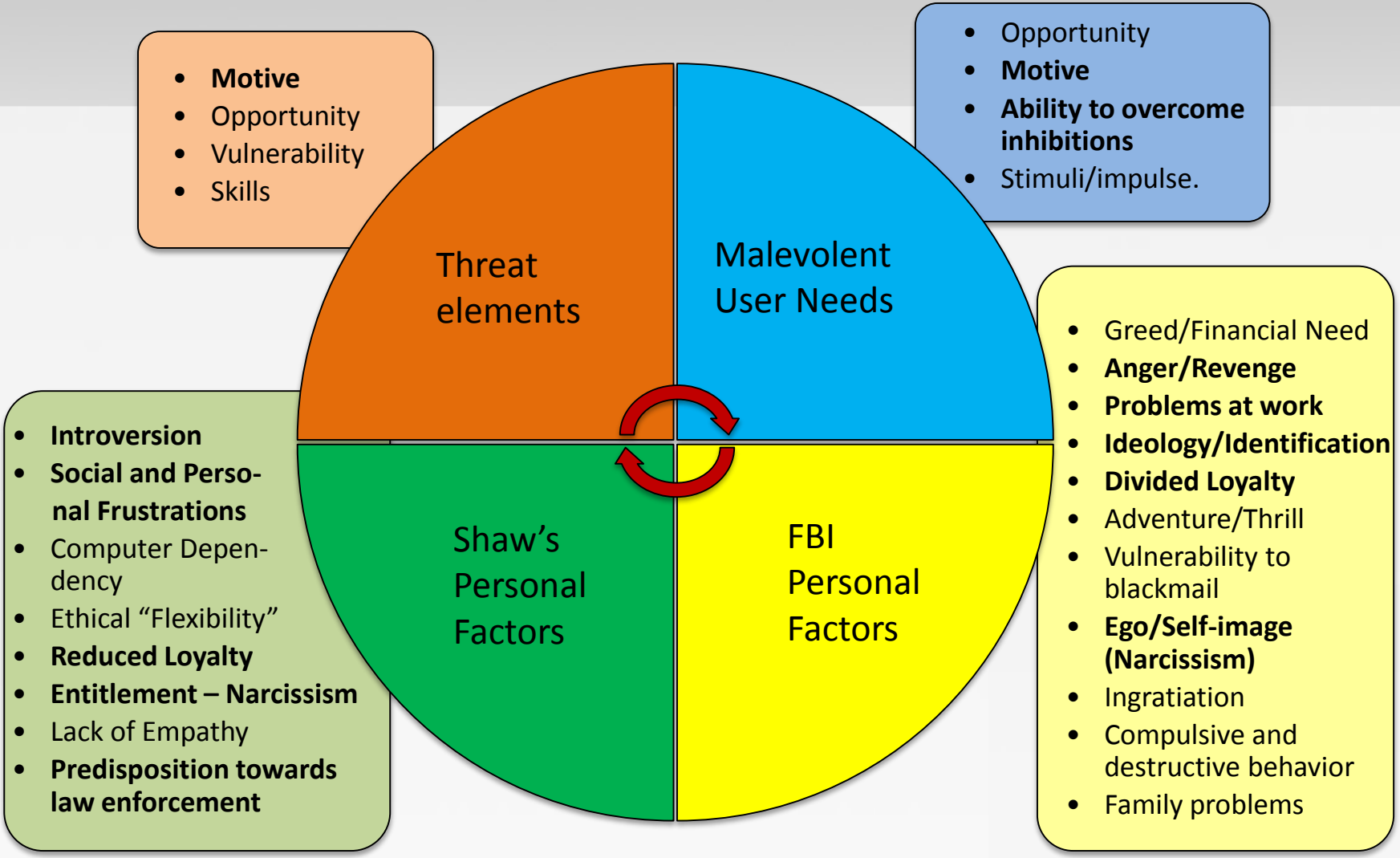
- **Introversion**
- **Social and Personal Frustrations**
- Computer Dependency
- Ethical “Flexibility”
- **Reduced Loyalty**
- **Entitlement – Narcissism**
- Lack of Empathy
- **Predisposition towards law enforcement**

Personal Factors (2/2)

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


Threat elements
Malevolent User Needs
Shaw's Personal Factors
FBI Personal Factors
• Motive
• Opportunity
• Vulnerability
• Skills
• Opportunity
• Motive
• Ability to overcome inhibitions
• Stimuli/impulse.
• Introversion
• Social and Personal Frustrations
• Computer Dependency
• Ethical "Flexibility"
• Reduced Loyalty
• Entitlement – Narcissism
• Lack of Empathy
• Predisposition towards law enforcement
• 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

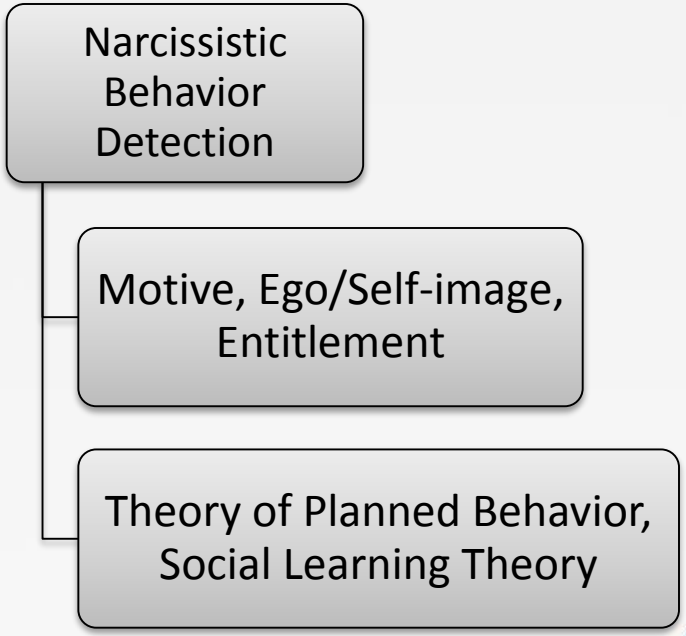
Behavior Prediction Theories

Human Behavior Prediction – Insider Threat Understanding Augmentation

- **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

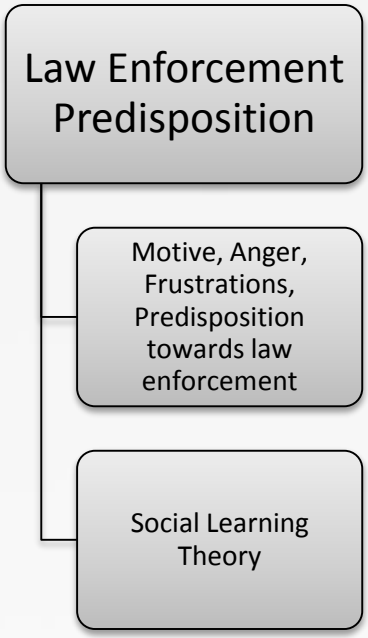
- **Twitter** Social Medium
- Graph: 1.075.859 users, 7.125.561 connections among them
- 41.818 fully crawled users
- Medium analysis via:
  - Strongly Connected Components
  - Node Loneliness
  - Small World Phenomenon
  - Indegree Distribution
  - Outdegree Distribution
- User analysis via:
  - Social 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

	Metrics					
Classifier	NBM		SVM		LR	
Classes	**P**	**N**	**P**	**N**	**P**	**N**
Precision	71	70	83	77	86	76
Recall	72	68	75	82	74	88
F-Score	71	69	79	79.5	80	81
Accuracy	70		80		81	

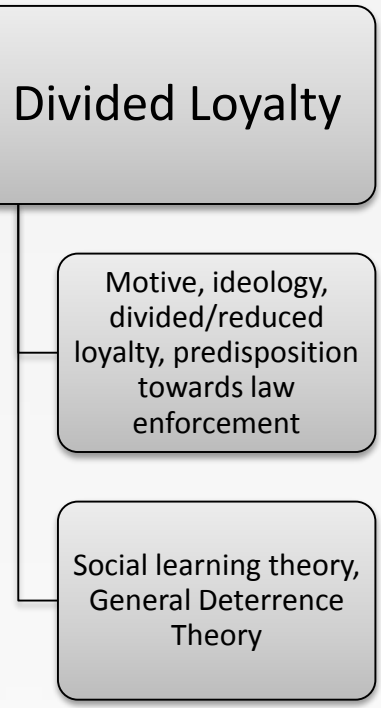


Divided Loyalty

Horror story!

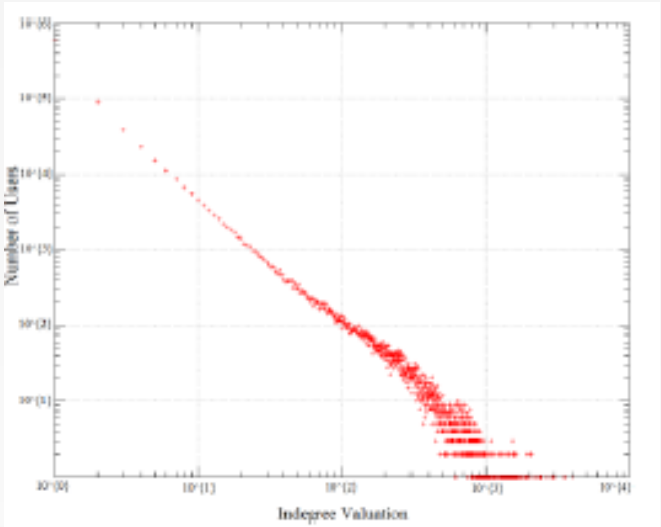
- **YouTube** Social Medium
- Same dataset
- Political profiling conclusion extraction
- Radical - Neutral - Conservative clusters
- Machine learning and content analysis of the dataset

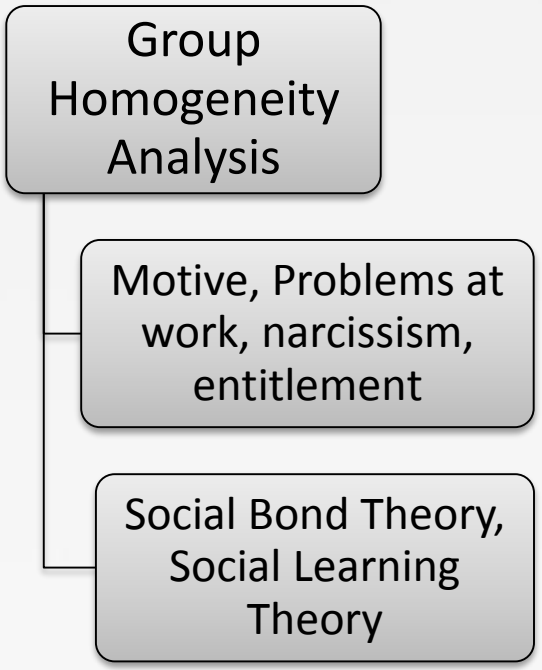
Algorithm: Multinomial Logistic Regression (MLR)			
Categories / Metrics	**Centre & Centre-left**	**Neutral**	**Centre & Centre-right**
Precision	83%	91%	77%
Recall	77%	93%	78%
F-Score	80%	92%	77%
Accuracy	87%		



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





Interdisciplinary capabilities

Horror story!

Narcissistic Behavior Detection	Group Homogeneity Analysis	Law Enforcement Predisposition	Political Profiling
Motive, Ego/Self-image, Entitlement	Motive, Problems at work, narcissism, entitlement	Motive, Anger, Frustrations, Predisposition towards law enforcement	Motive, ideology, divided/reduced loyalty, predisposition towards law enforcement
Theory of Planned Behavior, Social Learning Theory	Social Bond Theory, Social Learning Theory	Social Learning Theory	Social learning theory, General Deterrence Theory

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

1. Dritsas, S., Tsoumas, B., Dritsou, V., Konstantopoulos, P., Gritzalis, D., "OntoSPIT: SPIT Management through Ontologies", *Computer Communications*, Vol. 32, No. 2, pp. 203-212, 2009.
2. Gritzalis, D., Marias, G., Rebahi, Y., Soupionis, Y., Ehlert, S., "SPIDER: A platform for managing SIP-based spam over Internet Telephony", *Journal of Computer Security*, Vol. 19, No. 5, pp. 835-867, 2011.
3. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D., "An Insider Threat Prediction Model", in *Proc. of the 7th International Conference on Trust, Privacy, and Security in Digital Business*, pp. 26-37, Springer, Spain, 2010.
4. Kandias, M., Virvilis, N., Gritzalis, D., "The Insider Threat in Cloud Computing", in *Proc. of the 6th International Conference on Critical Infrastructure Security*, pp. 93-103, Springer, Switzerland, 2011.
5. Kandias, M., Galbogini, K., Mitrou, L., Gritzalis, D., "Insiders trapped in the mirror reveal themselves in social media", in *Proc. of the 7th International Conference on Network and System Security*, pp. 220-235, Springer, Spain, 2013.
6. Kandias, M., Mitrou, L., Stavrou, V., Gritzalis, D., "Which side are you on? A new Panopticon vs. privacy", in *Proc. of the 10th International Conference on Security and Cryptography*, pp. 98-110, SciTecPress, Iceland, 2013.
7. Kandias, M., Stavrou, V., Bosovic, N., Mitrou, L., Gritzalis, D., "Predicting the insider threat via social media: The YouTube case", in *Proc. of the 12th Workshop on Privacy in the Electronic Society*, pp. 261-266, ACM Press, Germany, 2013.
8. Kandias, M., Stavrou, V., Bozovic, N., Mitrou, L., Gritzalis, D., "Can we trust this user? Predicting insider's attitude via YouTube usage profiling", in *Proc. of 10th IEEE International Conference on Autonomic & Trusted Computing*, pp. 347-354, IEEE, Italy, 2013.
9. Mylonas, A., Tsoumas, B., Dritsas, S., Gritzalis, D., "A secure smartphone applications roll-out scheme", in *Proc. of the 8th International Conference on Trust, Privacy & Security in Digital Business*, pp. 49-61, Springer, France, 2011.
10. Mylonas, A., Kastania, A., Gritzalis, D., "Delegate the smartphone user? Security awareness in smartphone platforms", *Computers & Security*, Vol. 34, pp. 47-66, 2013.
11. Shaw, E., Ruby, K., Post, J., "The insider threat to information systems: The psychology of the dangerous insider", *Security Awareness Bulletin*, Vol. 98, No. 2, pp. 1-10, 1998.
12. US Dept. of Justice, Federal Bureau of Investigation, *The insider threat, an introduction to detecting and deterring insider spy*, USA, 2012.
13. Virvilis N., Dritsas S., Gritzalis D., "A cloud provider-agnostic secure storage protocol", in *Proc. of the 5th International Conference on Critical Information Infrastructure Security*, pp. 104-115, Springer, Greece, 2010.