

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

Dimitris Gritzalis

May 2014





5th European Union - United States - Canada Experts Meeting
on Critical Infrastructure Protection

Enhancing the Security and Resilience of Critical Infrastructures

May 2014, Athens, Greece

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

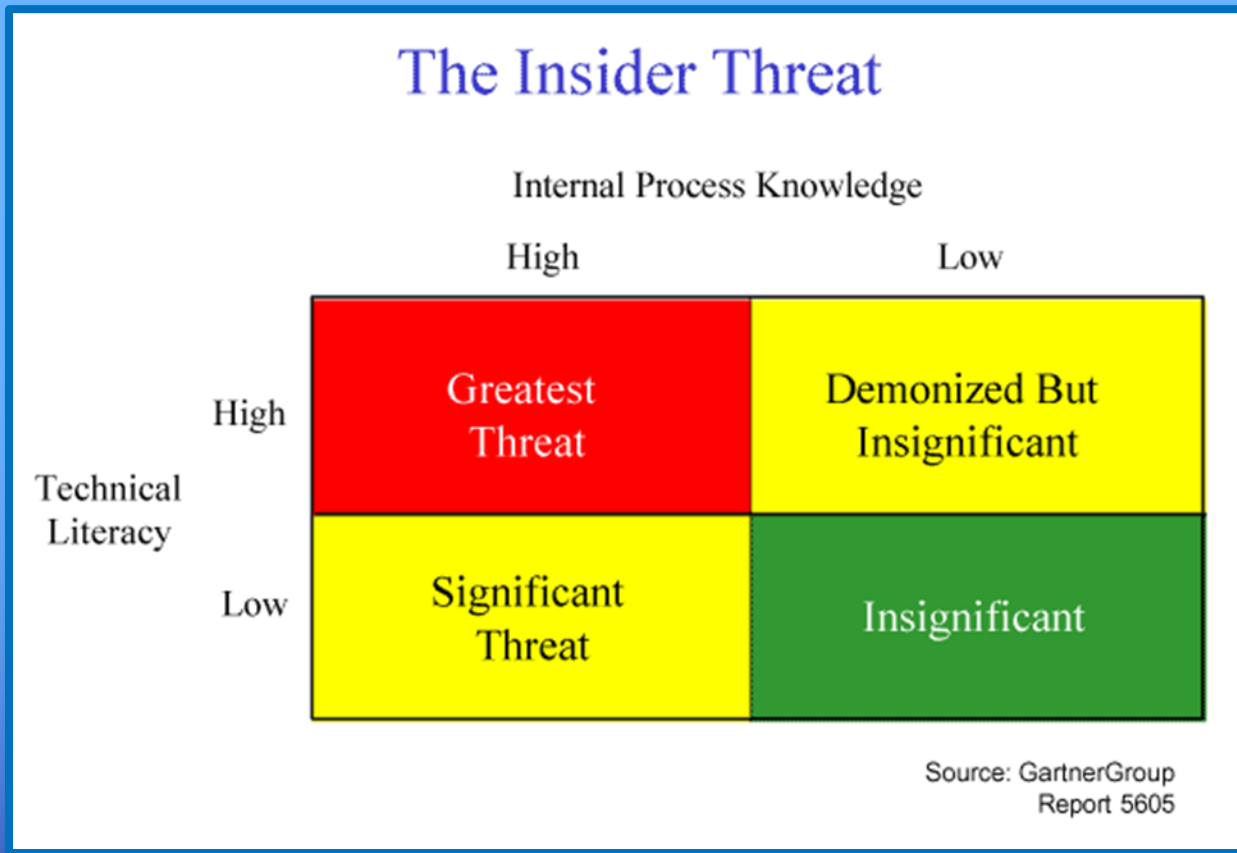
Defense:

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

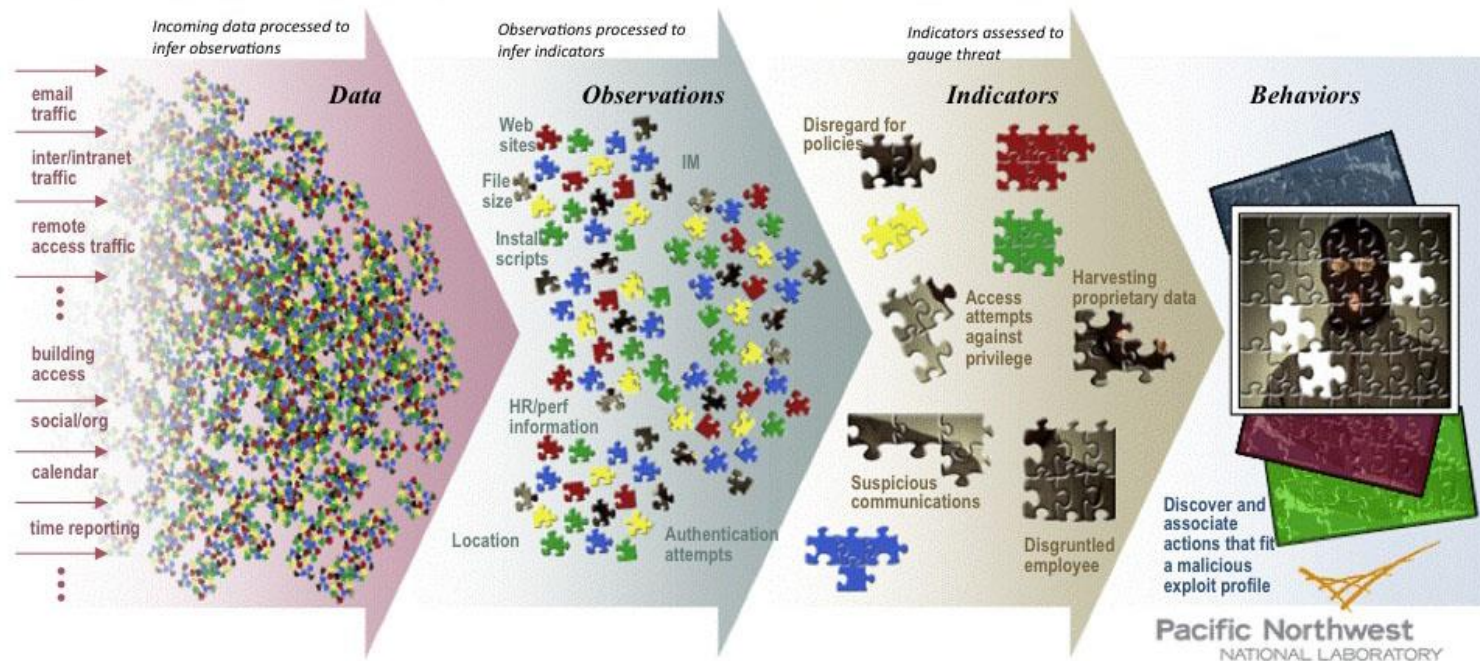
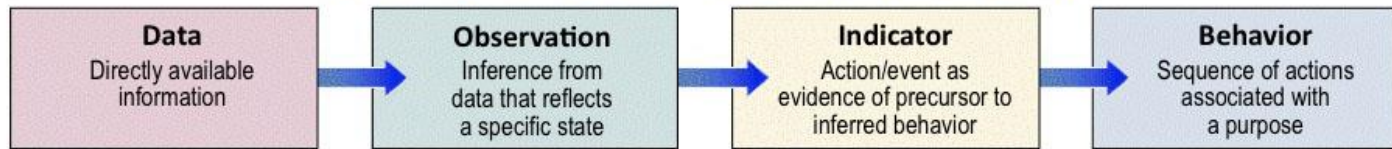


Insider threat impact



Behavior classification model

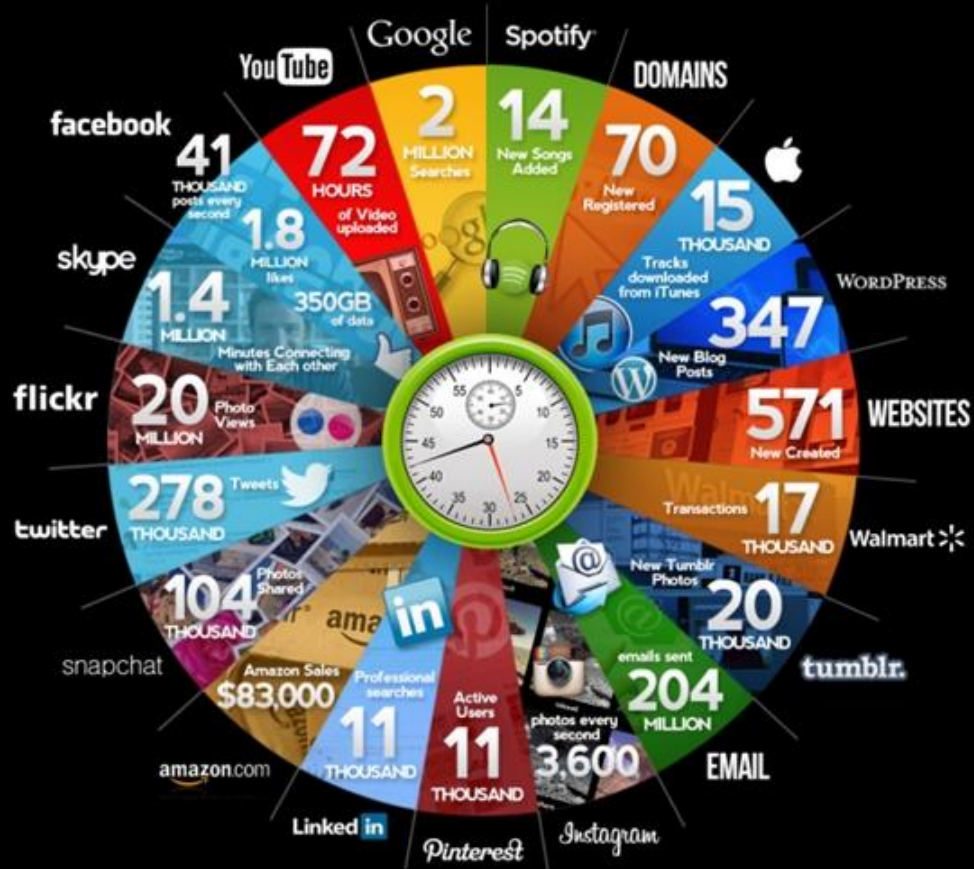
MODEL-BASED CLASSIFICATION



The Social Media arena: What happens online in 60sec


ONLINE IN **60** SECONDS

ON THE INTERNET, WE ALL KNOW THINGS CAN MOVE AT A LIGHTNING-FAST PACE. IN JUST A MINUTE, YOU CAN READ THROUGH AND COMPOSE A FEW TWEETS ALONG WITH LOOK AT DOZENS OF FACEBOOK PHOTOS. THAT SAID, WE'VE PULLED TOGETHER THIS INFOGRAPHIC TO GIVE YOU AN UPDATED VIEW OF EVERYTHING THAT HAPPENS ONLINE IN 60 SECONDS DURING 2013.



Case 1

Scope: Revealing a potential Insider

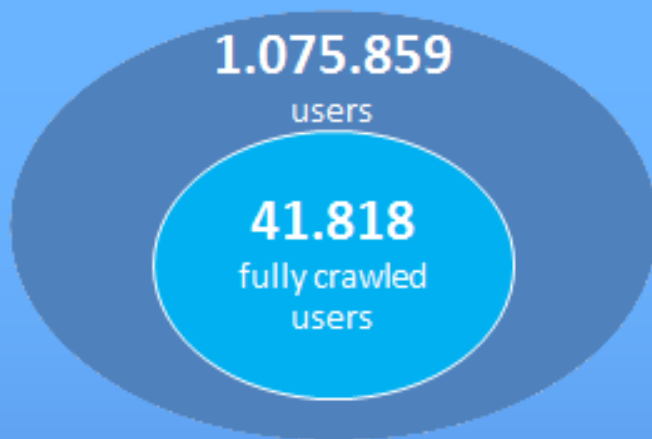
OSINT		Social Medium: Twitter 	
Tools used for the analysis			
Science		Theory	
Computing		Graph Theory	
Sociology		Theory of Planned Behavior	
		Social Learning Theory	



Case 1: Insider threat prediction based on narcissism¹



Twitter (Greece, 2012-13)



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 Intensity²
- Social Medium Influence valuation²
- Klout score (user influence)

¹ 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.

² 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, 2013.



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**

Category	Influence valuation	Klout score	Usage valuation
Loners	0 - 90	3.6 - 11.1	0-500
Individuals	90 - 283	11.1 - 26.0	50-4500
Known users	283-1011	26.0 - 50.0	45-21000
News Media & Personas	1011-3604	50.0 - 81.99	21000- 569000




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

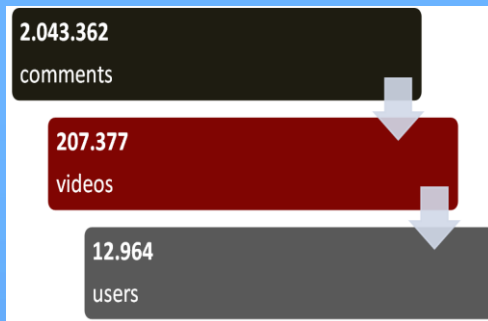
OSINT		Social Medium: YouTube 	
Tools used for the analysis			
Science	Theory		
Computing	Machine Learning		
	Data Mining		
Sociology	Social Learning Theory		



Case 2: Revealing negative attitude against law enforcement



YouTube (Greece, 2006-13)



Analysis framework based on:

- Social Learning Theory

Behavior analysis based on:

- Machine Learning

- Content Process

- User-generated content Classification

Classifier ¹	NB		SVM		LR	
	N	P/N	N	P/N	N	P/N
Classes ²						
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%	

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 και Recall.
 $F=2 * P * R / (P + R)$

Accuracy: The percentage of correct classifications.

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



References

1. Gritzalis D., Stavrou V., Kandias M., Stergiopoulos G., "Insider Threat: Enhancing BPM through Social Media", in *Proc. of the 6th IFIP International Conference on New Technologies, Mobility and Security*, IEEE Press, 2014.
2. Gritzalis D., Kandias M., Stavrou V., Mitrou L., "History of Information: The case of Privacy and Security in Social Media", in *Proc. of the History of Information Conference*, Law Library Publications, 2014.
3. 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, 2013.
4. 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, 2013.
5. 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 and Trusted Computing*, pp. 347-354, IEEE Press, 2013.
6. 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, 2013.
7. Kandias M., Mitrou L., Stavrou V., Gritzalis D., "YouTube user and usage profiling: Stories of political horror and security success", in *e-Business and Telecommunications*, Springer, 2014.
8. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Accessing n-order dependencies between critical infrastructures", *International Journal of Critical Infrastructures*, Vol. 9, Nos. 1-2, pp. 93-110, Elsevier, 2013.
9. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, in *Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection*, pp. 171-182, Springer, USA, 2013
10. Mitrou L., Kandias M., Stavrou V., Gritzalis D., "Social media profiling: A Panopticon or Omniopiticon tool?", in *Proc. of the 6th Conference of the Surveillance Studies Network*, Spain, 2014.
11. Mylonas A., Kastania A., Gritzalis D., "Delegate the smartphone user? Security awareness in smartphone platforms", *Computers & Security*, Vol. 34, pp. 47-66, Elsevier, 2013.
12. Pipyros K., Mitrou L., Gritzalis D., Apostolopoulos T., "A cyber attack evaluation methodology", in *Proc. of the 13th European Conference on Cyber Warfare and Security*, Athens, 2014
13. 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.
14. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based criticality analysis", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection*, Springer, USA, 2009.
15. Theoharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer Criticality Assessment methodology based on interdependencies", *Computers & Security*, Vol. 29, No. 6, pp. 643-658, 2010.

