



Conference on Safety & Security in Cyberspace:
Building up Trust in the European Union

March 2014, Athens, Greece



Know thy self and know thy enemy: Integrative security via proactive intelligence gathering and insider threat prediction

Dimitris Gritzalis

Professor and Director

Information Security & Critical Infrastructure Protection Laboratory
Dept. of Informatics, Athens University of Economics & Business, Greece



Outline

- Insider threat
- Know the threat, know the enemy
- Exploiting data from Social Media
- Behavior prediction potential
 - Case 1:** Insider detection based on Narcissism
 - Case 2:** Predisposition towards Law enforcement
 - Case 3:** Horror Story – Identifying political beliefs
- Conclusions

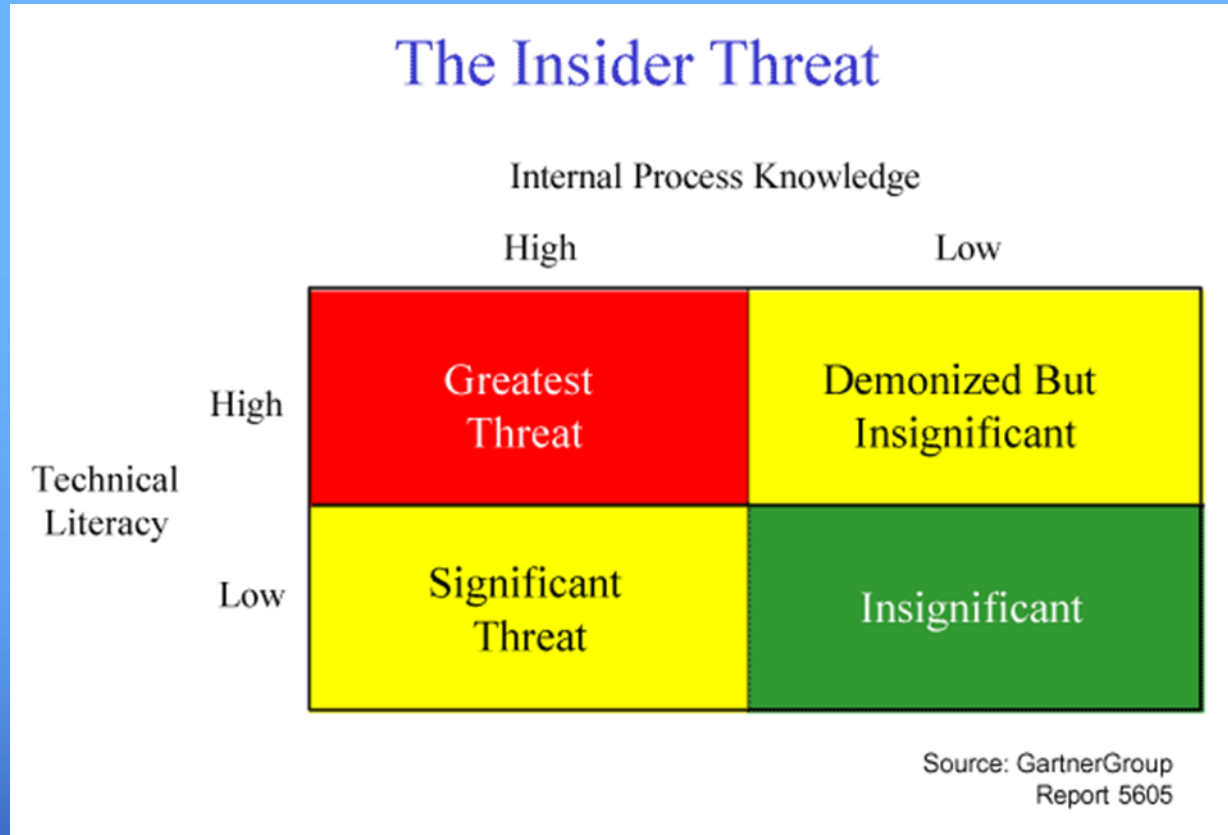


Insider Threat

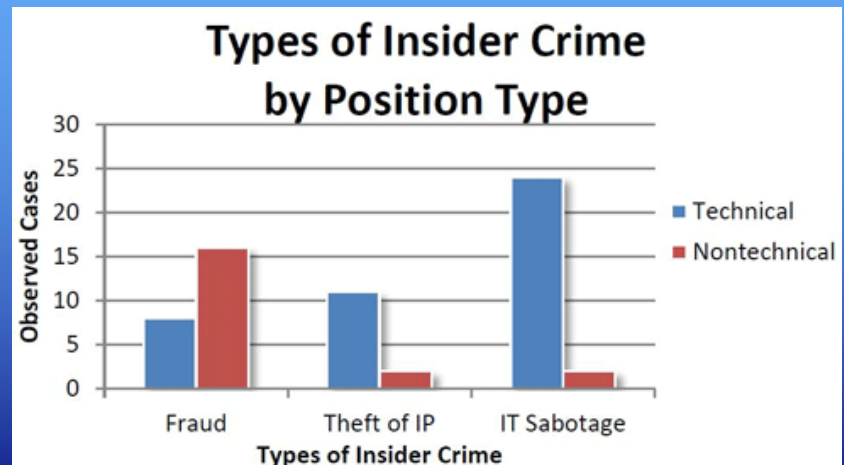
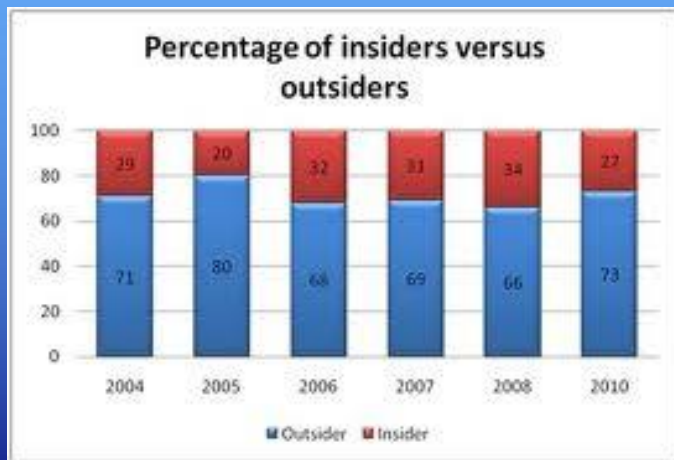
- Serious problem in cyber/corporate security
- Insider threat originates from persons who:
 - are legitimately given access rights to IS
 - misuse privileges and violate security policy



Insider Threat: When is its impact high?



How serious is the insider threat?



Know the Threat

- We have a threat if:
 - At least one attacker is motivated.
 - Opportunity exists.
 - At least one system is vulnerable.
 - Attacker has the skills.
- Given such a threat, a system is vulnerable.

- **Motive**
- Opportunity
- Vulnerability
- Skills

Threat consists of:



Know the Malevolent User

- Malevolent users
 - Opportunity to
 - Egosyntonic or e
 - In ca
 - over
 - App
- Under **every user is vulnerable to diverse**

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

ability to

Malevolent user needs:



Know the Enemy

- **Motive**
- Opportunity
- Vulnerability
- Skills

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

Threat consists of:

Malevolent user needs:

- **Introversion**
- **Social and personal frustrations**
- Computer dependency
- Ethical "flexibility"
- **Reduced loyalty**
- **Entitlement – Narcissism**
- Lack of empathy
- **Predisposition towards law enforcement**

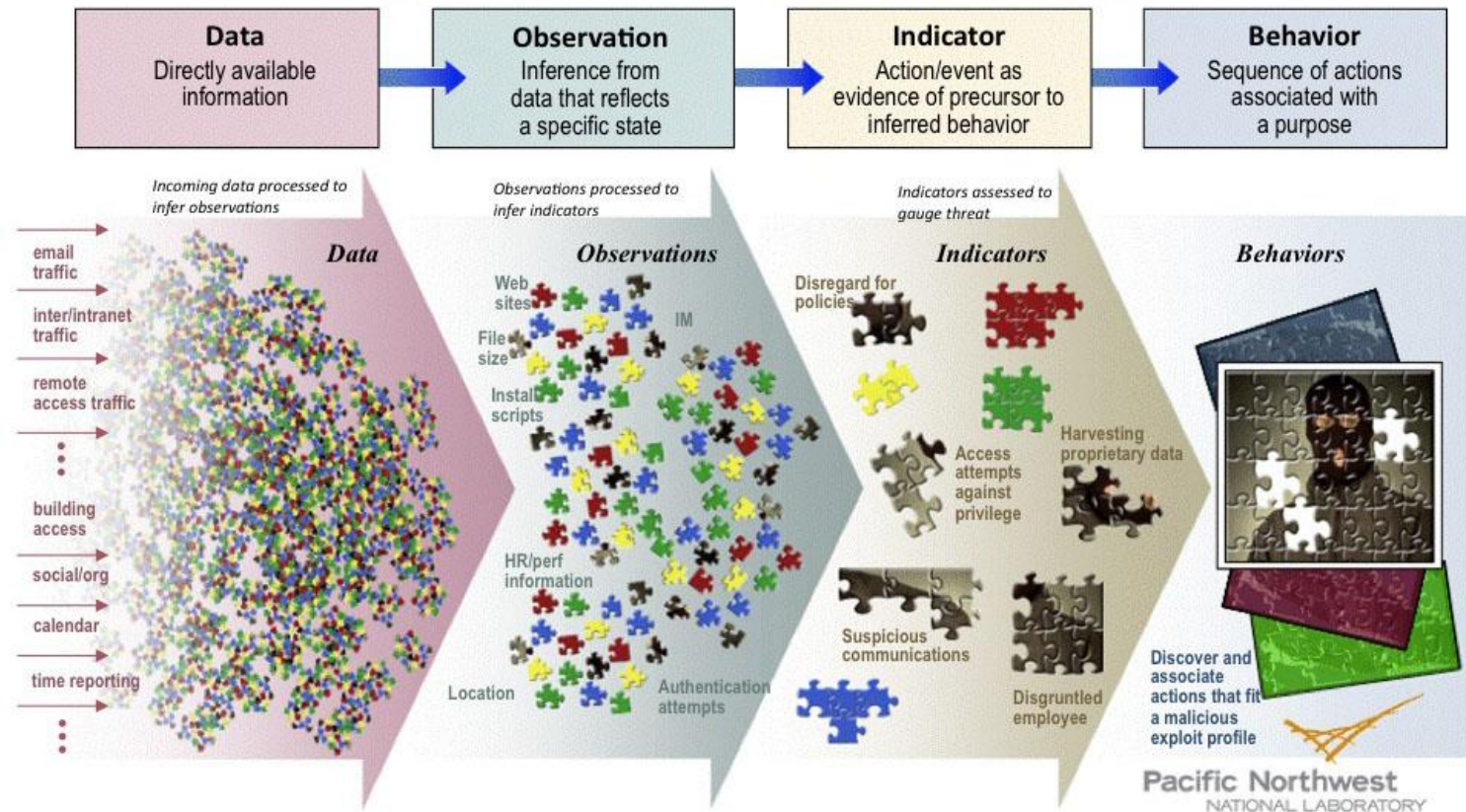
Shaw's Personal Factors

F.B.I. 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

A generic model for predicting threats

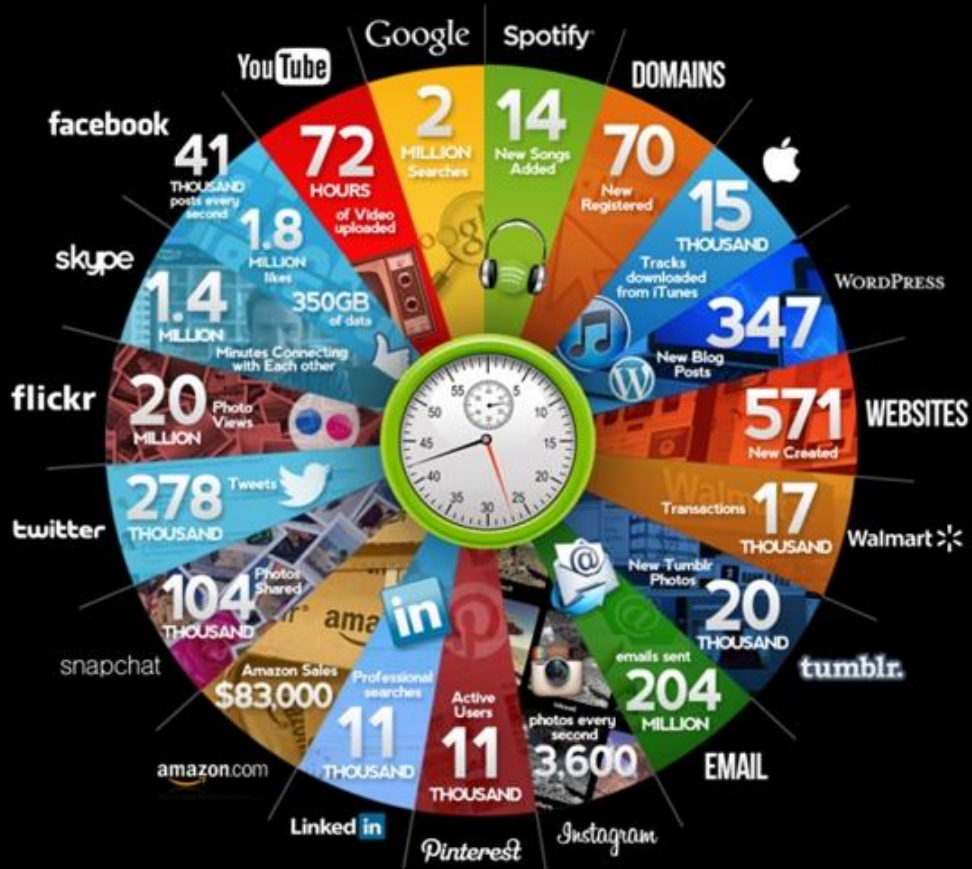
MODEL-BASED CLASSIFICATION



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 1a: Insider threat prediction based on Narcissism



Narcissistic
behavior
detection

Motive, Ego/Self-image,
Entitlement

Usage Intensity,
Influence Valuation,
Klout Score

Twitter

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
- Analysis based on Theory of Planned Behavior & Social Learning Theory.



Case 1b: 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. 13.2 followers/user on average.
- **Outdegree Distribution**
 - Distribution of outgoing edges at each node. 11 followings/ user on average.
- **Usage Intensity Distribution**
 - Distribution of the evaluation of usage intensity per user.
- **Taxonomy of users**
 - Ability to classify users into taxonomy and study them.

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



Case 2: Predisposition towards law enforcement



YouTube

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

Analysis based on Social Learning Theory



Law

Classifier	Metrics					
	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%	

law enforcement

Precision: Number of users correctly classified / number of users classified in the category.

Recall: Number of users correctly classified / number of users in the specific category.

F-Score: Harmonic mean of **Precision** και **Recall**.

Accuracy: Percentage of correct classifications.

Case 3: Horror story - Identifying political beliefs



YouTube

Same dataset

Political profiling conclusion extraction

Three indicative clusters:
Radical-Neutral-Conservative

Machine learning and Content Analysis of the dataset

Analysis based on:
Social Learning Theory

General Deterrence Theory



Algorithm: Multinomial Logistic Regression (MLR)

Categories	Centre & Centre-left	Neutral	Centre & Centre-right
Precision	83%	91%	77%
Recall	77%	93%	78%
F-Score	80%	92%	77%
Accuracy	87%		

enforcement

Precision: Number of users correctly classified / number of users classified in the category.

Recall: Number of users correctly classified / number of users in the specific category.

F-Score: Harmonic mean of Precision and Recall.

Accuracy: Percentage of correct classifications.

Content analysis,

Conclusions

- ✓ The insider threat is a **major threat** to modern IS
- ✓ Public data from **social media** can be used for prediction
- ✓ Identification of **narcissistic** behavior is a useful means
- ✓ **Predisposition** towards delinquent behavior is another one
- ✓ Social media data exploitation may lead to **horror stories**
- ✓ Several **ethical** and **legal issues** may arise (e.g. privacy)
- ✓ Intrusive nature dictates **limited** use (e.g. Critical Infrastructure)



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, Springer, 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. 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.
8. 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, 2011.
9. Mylonas A., Kastania A., Gritzalis D., "Delegate the smartphone user? Security awareness in smartphone platforms", Computers & Security, Vol. 34, pp. 47-66, Elsevier, 2013.
10. 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.
11. Theoharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", in Proc. of the 7th IEEE International Conference in Global Security, Safety and Sustainability, pp. 171-178, Springer, 2012.
12. Theoharidou M., Tsalis N., Gritzalis D., "In Cloud we Trust: Risk-Assessment-as-a-Service", in Proc. of the 7th IFIP International Conference on Trust Management, pp. 100-110, Springer, 2013.
13. U.S. Dept. of Justice, The insider threat: An introduction to detecting and deterring insider spy, FBI, USA, 2012.
14. 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, 2010.
15. Virvilis N., Gritzalis D., "The Big Four - What we did wrong in Advanced Persistent Threat detection?", in Proc. of the 8th International Conference on Availability, Reliability and Security, pp. 248-254, IEEE Press, 2013.

