

Security Data Science: Beyond Security

Miltiadis Kandias

March 2015



Optimum Intelligence
Connecting the dots. We know.



1st Annual ICT Security World Congress
Athens, March 2015

Security Data Science: Beyond Security

Banking gone viral!

Miltos Kandias

CEO, Optimum Intelligence S.A.

Senior Researcher, INFOSEC Lab, AUEB



Optimum Intelligence
Connecting the dots. We know.

Security Data Science is the application of advanced analytics to activity and access data to uncover unknown risks.

Outline

- Banking goes Social
- ...and then goes viral!
- Threats & opportunities
- Security Data Science solutions
- Security should pay, not cost
- Beyond Security
- More opportunities
- Our expertise



Banking goes social

- Major banks around the globe exploit OSN opportunities.
- ICICI Bank Twitter Banking.
- Barklays UK 6 Facebook Apps.
- ASB Bank Facebook payments
- Axis Bank 12 Facebook Apps.



The image shows a screenshot of the Axis Bank Facebook page. At the top, there is a banner for mobile apps with the text "FABULOUS", "ROCKSTAR", and "GENIUS" above images of smartphones displaying the Axis Bank app. Below the banner is the Axis Bank logo and the text "Axis Bank" with "1,648,125 likes · 28,302 talking about this". Below the profile information, there is a bio: "Bank Axis Bank was the first of the new private banks to have begun operations in 1994. We welcome you to the official fan page of Axis Bank". Below the bio, there are several app icons: "Photos", "Likes", "ProgressTogether...", "Youth Card", "Customer Sup...", "Plan Your Money", "Axis Bank Bra...", "Meri Zindagi K...", "Axis SpeedPay", "My Face My Tr...", "Buy Tickets", and "PicBadges".



...and then goes viral!

- GT Bank (<https://www.facebook.com/gtbank>):
 - 12 Facebook Apps
 - 2,359,205 likes
- ICICI Bank (<https://www.facebook.com/icicibank>):
 - 12 Facebook Apps
 - 3,510,663 likes
- Barclays UK (<https://www.facebook.com/BarclaysUK>):
 - 6 Facebook Apps
 - 557,968 likes
- HDFC Bank (<https://www.facebook.com/HDFC.bank>):
 - 10 Facebook Apps
 - 2,320,108 likes
- Axis Bank (<https://www.facebook.com/axisbank>):
 - 12 Facebook Apps
 - 3,070,646 likes



Threats

- Socioware man-in-the-middle
- OSN orchestrated DoS and DDoS attacks
- New age phishing - Social engineering attacks - Customer profile hijacking
- Data leakage
- Not otherwise specified attacks









Opportunities



- Detect socioware infections, protect your clients.
- Clients are good beta testers. Collect their intelligence.
- Aggregate crowd generated intelligence over your systems.
 - Evaluate performance and security.
- Utilize social media intelligence to enhance fraud detection.
- Manage and mitigate data leakage.
- Predict potential insiders.



Examples



To  e-banking της  χρησιμοποιεί [MD5](#) για message authentication....


 



★★★★★



Χειρότερο e-banking πεθαίνεις....

Like · Comment · about 6 months ago · 25 Reviews

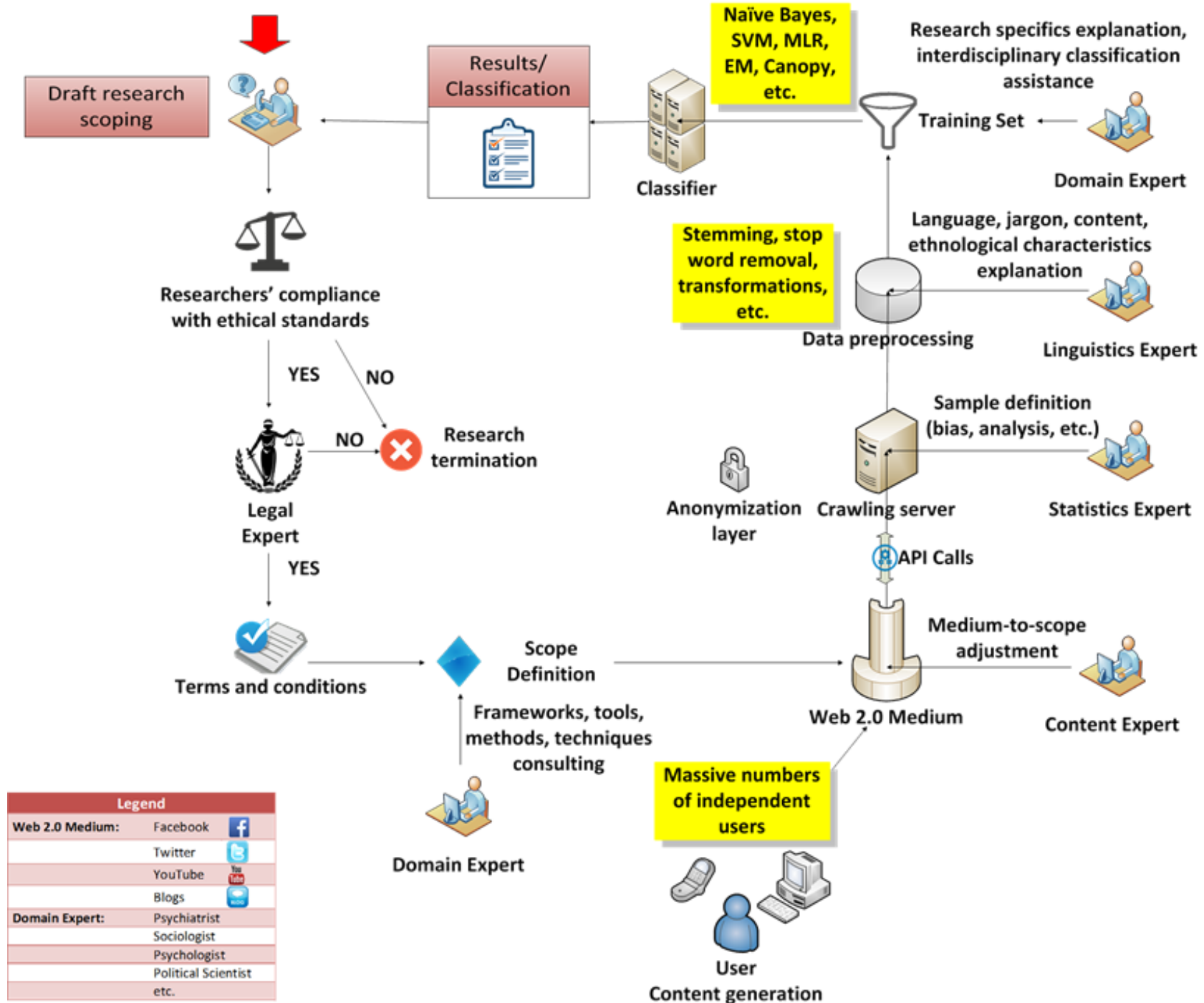
January 9 · 

 the slowest bank in !! Don't deposit here or else it'll be the year 3015 before you can get your money out again.

Share ·  3  3



Nereus Platform



Security should
pay, not cost.



Beyond Security

- Utilize results beyond ICT security.
- Enhance Business Intelligence.
- Gamify content.
- Focus on individuals and...
 - ...calculate and strengthen engagement
 - ...personalize offers
 - ..personalize content
- Know what people say, predict what people do.



What people say?



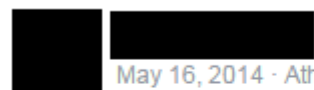
Εκεί στην [redacted] τερμάτισαν το θράσος .

Like · Comment · Share · 1



οταν τηλεφωνω στα customer service των τραπεζών [redacted] εχω την εντύπωση ότι μου μιλάει κάποιος που αργότερα θα τον μαστιγώσουν.

Share



May 16, 2014 · Athens · *

Η [redacted] με εξόργισε πέρα από κάθε όριο. Ανένδοτος αγώνας.

Like · Comment · Share · 3



· Athens · Edited ·

Τον [redacted] του [redacted] αποπλήρωσα ολοσχερώς και κατά [redacted] χρόνια νωρίτερα καταναλωτικό δάνειο και παρά τις διαμαρτυρίες μου η [redacted] ουδέποτε μου επέστρεψε τα ασφάλιστρα ζωής που αφορούσαν το δάνειο από [redacted] έως [redacted]. Σήμερα όμως μου απέστειλε σοβαρότατη επιστολή για να εξοφλήσω και τα ασφάλιστρα ζωής από [redacted] έως [redacted]. Να τους αφήσω να μου κάνουν αγωγή? 😊 [redacted]

Like · Comment · Share · 54



Πρό λίγο έκανα μια ανάληψη σε ευρώ από την [redacted] στη [redacted]. Το ποσό ήταν από συνάλλαγμα και ο υπάλληλος αντί να το περάσει στο κομπιούτερ μου το έγραψε χειρόγραφα και προσπάθησε να μου κλέψει 1000 ευρώ περίπου. Ευτυχώς το κατάλαβα και διόρθωσε το "υποτιθέμενο" λάθος του... Αν κάποιος ξέρει από αυτές τις διαδικασίες τον παρακαλώ πολύ να επικοινωνήσουμε για να με βοηθήσει στη καταγγελία που θέλω να κάνω, γιατί είναι σαφές τί πήγε να κάνει [redacted]

Like · Comment · Share · 1



Optimum Intelligence

Connecting the dots. We know.

Asking important questions

- ✓ How can I boost customers engagement?
- ✓ How can I take advantage of top influential social media users?
- ✓ How can I improve my products?
- ✓ How can I enhance customers' satisfaction?
- ✓ How can I meet customers' expectations?
- ✓ How can I effectively plan my marketing campaigns?
- ✓ How can I enhance the success of my marketing campaigns?
- ✓ How can I evaluate the results of my marketing campaign?
- ✓ When should I launch a new product?



A-Bank-in-a-Bank



- Every Bank has many vaults.
- How about yet another “vault”?
- The “vault” of data, transactions, and preferences for every client.
- So, why not in-depth-use of this data (where applicable, given informed consent of the user)?

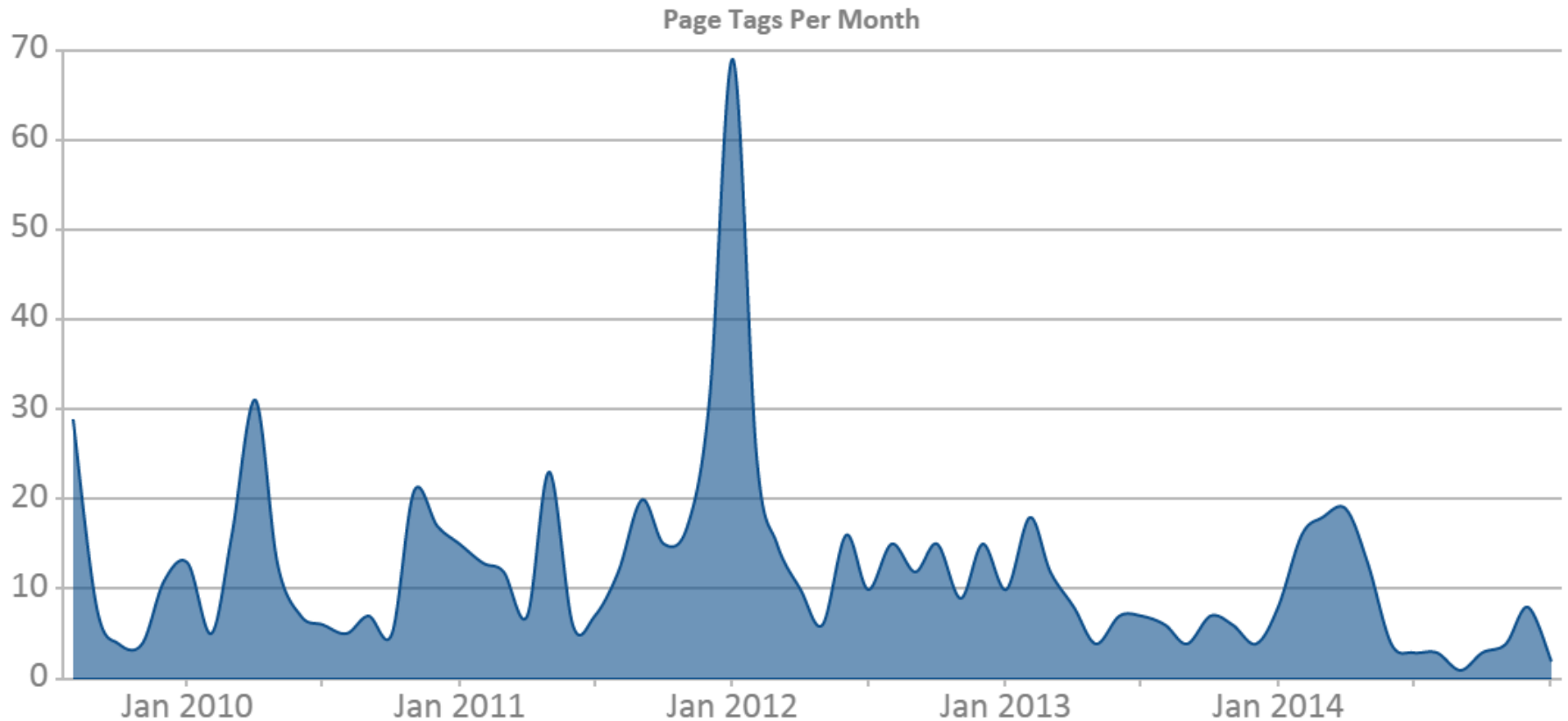


Our expertise

- Extract attitudes characteristics on an individual basis.
- Calculate specific OSN and BI metrics.
- Chronicity analysis.
- Sentiment analysis (individual basis, over the masses).
- Machine learning, data mining, big data, data analysis.



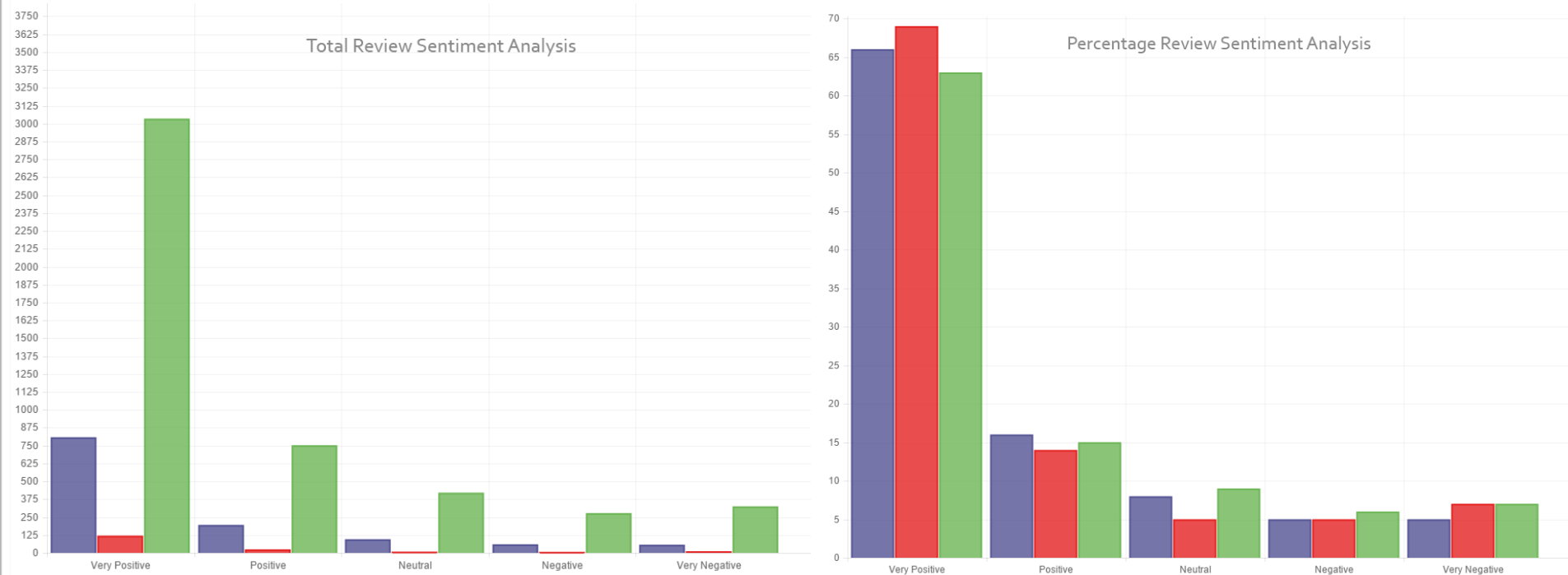
How many people talk about us?



Optimum Intelligence
Connecting the dots. We know.

Correlation between profile activity and user engagement.

Who do people like more?



- Three competitors
- Different popularity
- Similar sentiment



How about individuals?



Highly Influential

Narcissist

Mildly prone to high stress periods

Mildly predisposed towards law and authorities.

Economic Liberal

Individual of interest

Joined Twitter dd/mm/yyyy

Age 25

Location Greece

Profession Journalist



Individual of interest

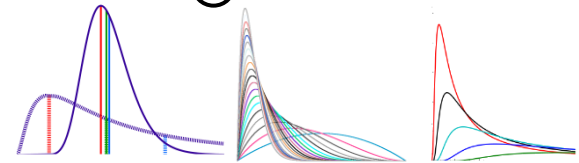
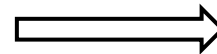


Optimum Intelligence
Connecting the dots. We know.

Followers' profiling on an individual basis.
Example: **Top influencer regarding bank.**

How about groups?

- Aggregate individuals' profiling results
- Calculate crowd behavior distributions
- Extract results on:
 - ✓ Target group detection
 - ✓ Target group evaluation
 - ✓ Time-to-launch identification
 - ✓ Any other question



More (answerable) questions

- ✓ When should I communicate with (potential) customers?
- ✓ When should I publish news/offers/coupons etc.?
- ✓ How can I exploit trends, so as to launch a new product campaign?
- ✓ How could I conduct content/gift/offer personalization?
- ✓ How could I engage customers on my service/product?
- ✓ How could I customize my products on each customer?
- ✓ What product should I promote to each customer based on her preferences?
- ✓ How should approach each customer according to her personality?



**You put the question.
We provide the answer!**



Optimum Intelligence
Connecting the dots. We know.

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 (NMITS-2014)*, Springer, UAE, 2014.
2. Gritzalis D., "Insider threat prevention through Open Source Intelligence based on Online Social Networks", Keynote address, *13th European Conference on Cyber Warfare and Security (ECCWS-2014)*, Greece, 2014.
3. 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, Athens, 2014.
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 (SECRYPT-2013)*, pp. 98-110, Iceland, 2013.
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 (NSS-2013)*, pp. 220-235, Springer (LNCS 7873), Spain, June 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 (CRITIS-2011)*, pp. 93-103, Springer (LNCS 6983), United Kingdom, 2013.
7. 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 (ATC-2013)*, pp. 347-354, IEEE Press, Italy, 2013.
8. Kandias M., Stavrou V., Bosovic N., Mitrou L., Gritzalis D., "Proactive insider threat detection through social media: The YouTube case", in *Proc. of the 12th Workshop on Privacy in the Electronic Society (WPES-2013)*, pp. 261-266, ACM Press, Germany, 2013.
9. Kandias M., Virvilis N., Gritzalis D., "The Insider Threat in Cloud Computing", in *Proc. of the 6th International Workshop on Critical Infrastructure Security (CRITIS-2011)*, Bologna S., et al (Eds.), pp. 93-103, Springer (LNCS 6983), Switzerland, 2011.
10. Kandias M., Mylonas A., Virvilis N., Theoharidou M., Gritzalis D., "An Insider Threat Prediction Model", in *Proc. of the 7th International Conference on Trust, Pri-vacy, and Security in Digital Business (TrustBus-2010)*, pp. 26-37, Springer (LNCS-6264), Spain, 2010.
11. 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.
12. Stavrou V., Kandias M., Karoulas G., Gritzalis D., "Business Process Modeling for Insider threat monitoring and handling", in *Proc. of the 11th International Conference on Trust, Privacy & Security in Digital Business (TRUSTBUS-2014)*, pp. 119-131, Springer (LNCS 8647), Germany, September 2014.
13. Virvilis N., Gritzalis D., "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?", in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing (ATC-2013)*, pp. 396-403, IEEE Press, Italy, 2013.
14. Virvilis N., Gritzalis D., "The Big Four - What we did wrong in Advanced Persistent Th-reat detection?", in *Proc. of the 8th In-ter-na---tional Conference on Availability, Reliability & Security (ARES-2013)*, pp. 248-254, IEEE, Ger-many, 2013.

