Exploiting user chronicity over Online Social Networks

Kostas Nikoloulis, Vasilis Stavrou, Miltiadis Kandias

{k.nikoloulis, stavrouv, kandiasm}@aueb.gr

Information Security and Critical Infrastructure Protection Research Laboratory

Dept. of Informatics, Athens University of Economics & Business (AUEB)

Introduction

- ❑ Insider threat: Major issue in cyber and corporate security
- ❑ Rapid explosion of participation and increase of user generated content in OSN
- ❑ Users transfer their offline behavior to the online world
- ❑ Open Source INTelligence (OSINT) in the service of profiling and data processing
- ❑ Exploitation of user chronicity to detect deviations in the digital world
- ❑ Deviations may be related to experiencing increased stress levels

User chronicity

- ❑ Chronicity refers to the usage deviations that users may exhibit within the context of OSN over time
- ❑ Detect usage pattern fluctuations of users' OSN generated content
- ❑ Split users' usage patterns into weekly time periods
- ❑ Form clusters based on the usage patterns manifested in user's digital life
- ❑ Clusters with the least populations indicate potential usage deviations

Accessed user information

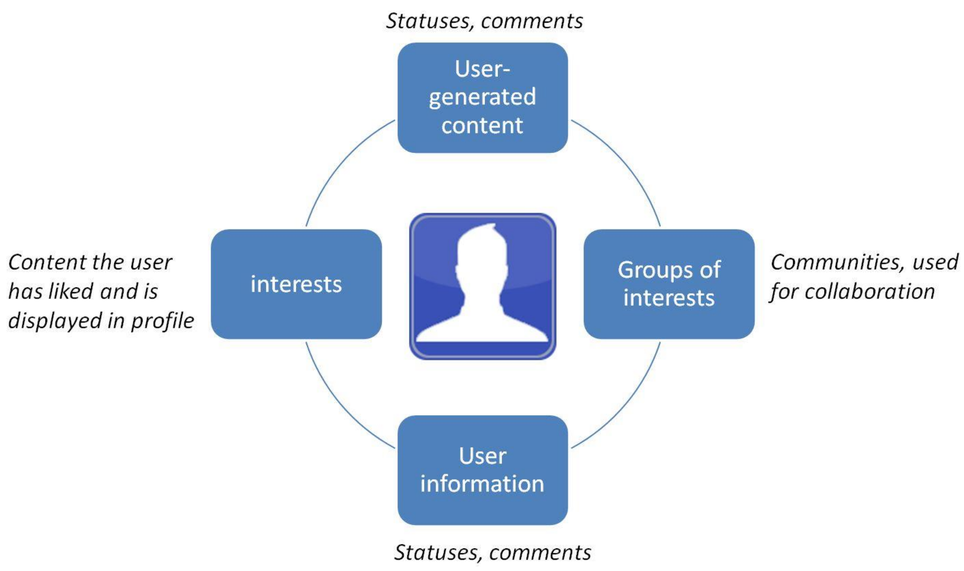

Figure 1: Accessed information

Facebook

- ❑ Detect usage deviations in user's digital life
- ❑ Examine usage behavior in time periods of one week
- ❑ Detect the least populated clusters as the deviating ones

Crawled Greek community consists of:

98.256 Liked objects	12.346 Groups	171.054 Status updates	250.027 Comments	405 Fully- crawled users

- ❑ Methodology:
  - ➢ Examine user's content in order to detect deviations over user's usage behavior
  - ➢ Classify content into predefined categories of interest
  - ➢ Analyze usage behavior based on chronicity metrics
  - ➢ Form clusters of similar usage behavior and detect the deviating ones

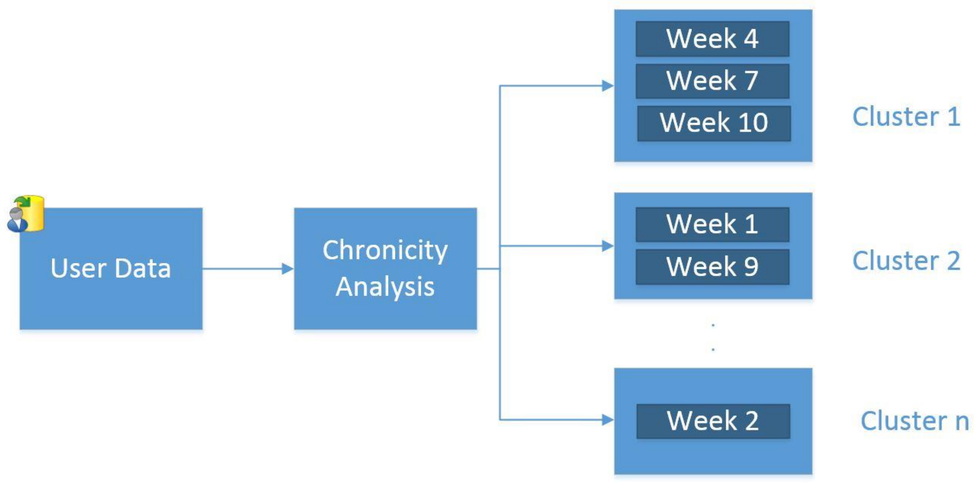

Figure 2: Chronicity analysis – Clusters of usage patterns

- ❑ **Content classification**:
  - ➢ Train classifier to detect content belonging to: (a) sports, (b) music, (c) politics, and (d) miscellaneous.

Metrics				
Classifier	SVM			
Classes	S	M	P	Mi
Precision	79	97	87	70
Recall	72	89	75	88
F-Score	75	93	81	78
Accuracy	81			

Figure 3: Support Vector Machines *metrics*

Frequency of posts regarding sports
Frequency of posts regarding music
Frequency of posts regarding politics
Frequency of posts regarding miscellaneous
Interest Shift per interest pair
Average frequency of posting
Average frequency of commenting
Major interests
Minor interest shift frequency
Frequency of uploading photos
CommentedBy ratio
StatusVarianceFlattened
CommentVarianceFlattened

Figure 4: Chronicity analysis metrics

- ❑ **Chronicity analysis**:
  - ➢ Usage chronicity is calculated via a set of ad hoc metrics.
  - ➢ Analysis is focused on the following areas: (a) user interests, (b) usage patterns over time, (c) multi-media usage and (d) aggressive language.

- ❑ Decision process:
  - ➢ Analyse each user's content using the SVM classifier and the chronicity analysis metrics
  - ➢ Perform clustering using a voter as depicted in Fig. 5

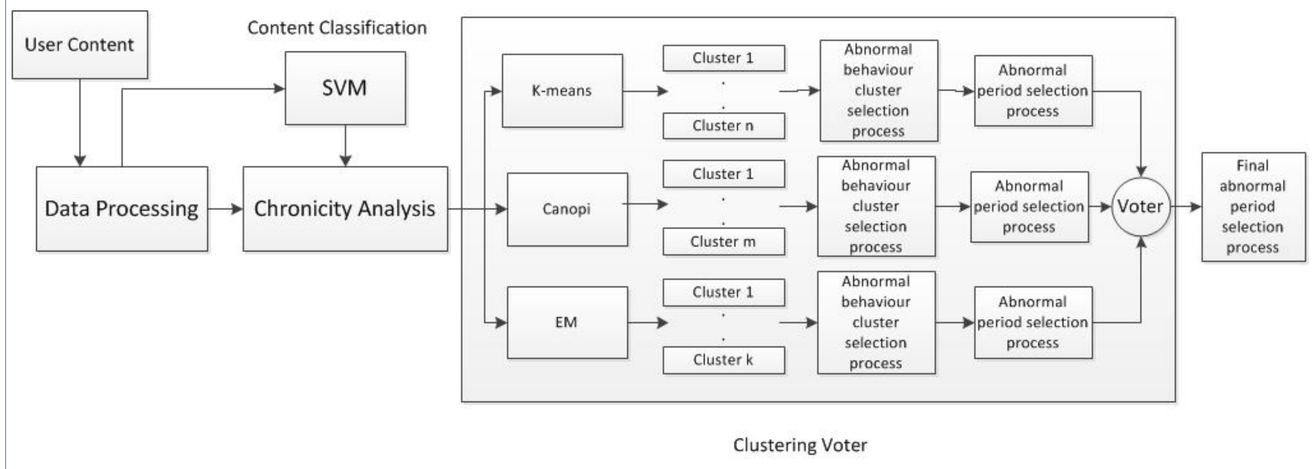

Figure 5: Overall decision process

Conclusions

- ❑ User classification facilitates user/usage profiling offered by OSINT.
- ❑ Ability to detect deviating time periods in user's online behaviour.
- ❑ Deviations in digital behaviour may indicate predisposition of delinquent behaviour.
- ❑ Perform chronicity analysis so as to mitigate the insider threat. However, it should be only applied to certain cases (e.g., critical infrastructures staff appointment).
- ❑ Proactive individuals/organizations protection capability.
- ❑ Ability to enhance protection against the insider threat in business process security management systems.

References

1. Amichai-Hamburger, Y., Vinitzky, G., *Social Network Use and Personality*, 2010.
2. Shaw, E., Ruby, K., Post, J., "The insider threat to information systems: The psychology of the dangerous insider", *Security Awareness Bulletin*, pp. 1-10, 1998.
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*, pp. 283-310, Law Library Publications, Greece, 2014.
4. Kandias, M., Stavrou, V., Bosovic, N., Gritzalis, D., "Proactive Insider Threat Detection Through Social Media: The YouTube Case", in *Proc. of the 12th Workshop on Privacy in the Electronic Society*, Berlin, 2013.
5. 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, Iceland, 2013.
6. 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 (LNCS 7873), Spain, 2013.
7. 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 (LNCS-6264), Spain, 2010.
8. 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 (LNCS 6983), 2011.
9. Mylonas, A., Tsoumas, B., Dritsas, S., Gritzalis, D., "Smartphone security evaluation: The malware attack case", in *Proc. of the 8th International Conference on Security & Cryptography*, pp. 25-36, SciTekPress, Spain, 2011.
10. 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*, pp. 119-131, Springer (LNCS 8647), Germany, 2014.
11. 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, UAE, 2014.
12. 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, Italy, 2013.