Detecting stress level of Facebook users as a means for insiders identification

Themistoklis Markopoulos, Miltiadis Kandias, Vasilis Stavrou

p3080111@dias.aueb.gr, {kandias, stavrouv}@aueb.gr

Information Security & Critical Infrastructure Protection Laboratory

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

Introduction

- ❑ Rapid explosion of Social Media, which contain user generated content
- ❑ Insider threat: Major issue in cyber and corporate security
- ❑ Stress and depression can be correlated to delinquent behavior
- ❑ Indications can be found in user profiles in Online Social Networks
- ❑ Open Source INTelligence (OSINT) in the service of profiling and data processing

Insider threat detection

- ❑ Insiders have been found to share common psychological characteristics
- ❑ Research has examined and detected these characteristics via Online Social Networks
- ❑ Although a user may not share any of these characteristics, it may be possible to manifest delinquent behavior due to suffering from high stress levels
- ❑ Ability to examined stress characteristics through Online Social Networks

Facebook

- ❑ **Security**: Identify the insider via her attitude towards stress levels
  - ➢ The stress may lead to delinquent behavior
- ❑ **Privacy**: Raise user awareness over:
  - (i) Profiling
  - (ii) Data processing for discriminative purposes

Crawled Greek community consists of:

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

Methodology:

- ➢ Application development for data collection
- ➢ Use of Beck's inventory for measuring clinical anxiety
- ➢ Perform clustering based on questionnaire results
- ➢ Detect common characteristics among the clusters
- ➢ Point out characteristics shared among users experiencin high stress levels

Insider Threat Identification:

- ➢ Perform clustering that detects similar user patterns behaviour

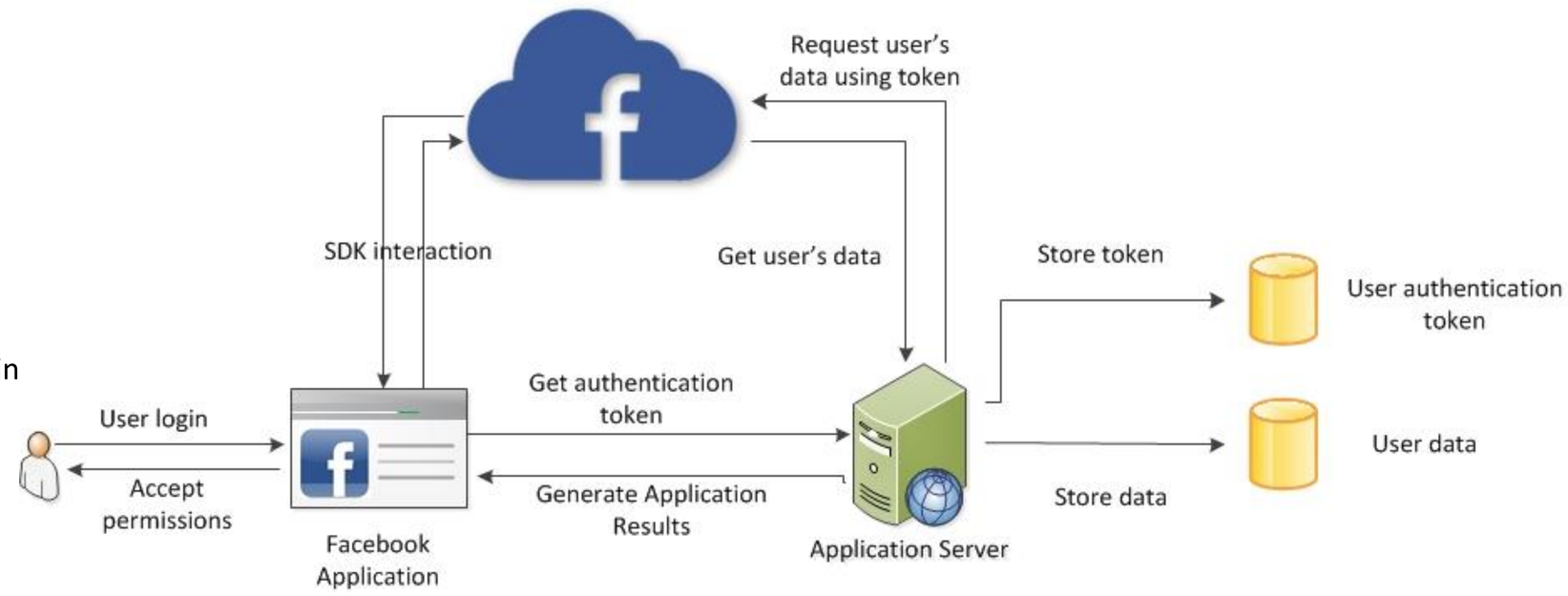

Figure 1: Data crawling architecture

Observations

- ❑ Users with stress levels beyond normal are likely to manifest malevolently
- ❑ Regarding their results, users can be classified into 3 broad categories of stress levels
- ❑ Types of art that belongs to alternative scene are preferred by users with medium and high stress levels

Figure 2: Population percentage of stress clusters

Conclusions

- ❑ User/Usage profiling leads to conclusions over delinquent behaviour
- ❑ Enhance business corporations and organizations to predict and protect against the insider threat
- ❑ Such approaches should be only applied to certain cases (e.g., critical infra-structures staff appointment)
- ❑ Users with high stress levels perform similar patterns of behaviour
- ❑ 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. Beck, A., Epstein, N., Brown, G., Steer, R., "An inventory for measuring clinical anxiety: Psychometric properties", *Journal of Consulting and Clinical Psychology*, pp. 893, 1988.
4. 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.
5. 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.
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, Iceland, 2013.
7. 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 & System Security*, pp. 220-235, Springer (LNCS 7873), Spain, 2013.
8. 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 & Security in Digital Business*, pp. 26-37, Springer (LNCS-6264), Spain, 2010.
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, SciTek-Press, 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 Intern. Conference on Trust, Privacy & Security in Digital Business*, pp. 119-131, Springer (LNCS 8647), Germany, 2014.
11. 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), 2013.
12. 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 & Security*, Springer, UAE, 2014.
13. 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 Intern. Conference on Autonomic & Trusted Computing*, pp. 347-354, IEEE Press, Italy, 2013.