The Insider Threat

Miltiadis Kandias, Vasilis Stavrou

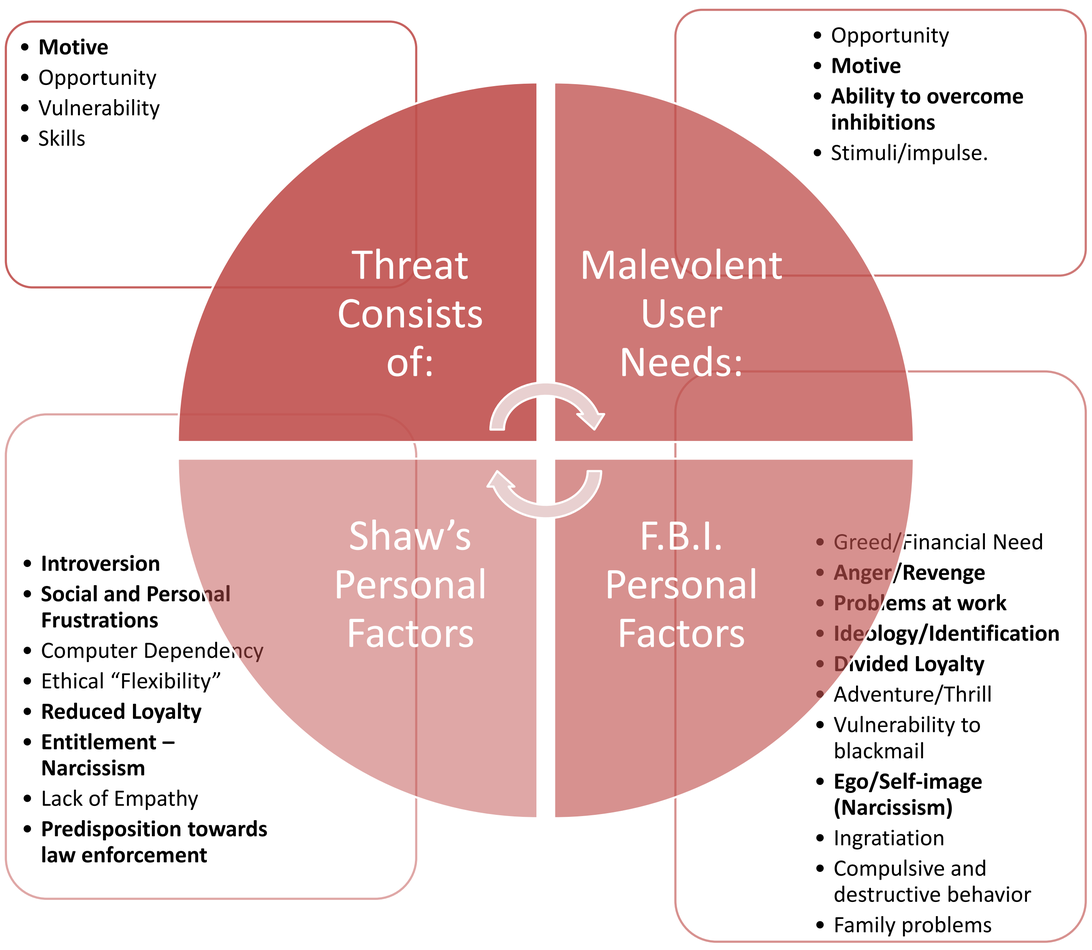
{kandiasm, stavrouv}@aueb.gr

Information Security and Critical Infrastructure Protection Research Group

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

Introduction

- **Insider threat:** Demanding problem in cyber/corporate security.
- **Malevolent insider:** Trusted user who violates security policy [1].
- Three major **fronts** in the battle against insider threat [2]:
  - Prediction
  - Detection
  - Prevention - Deterrence

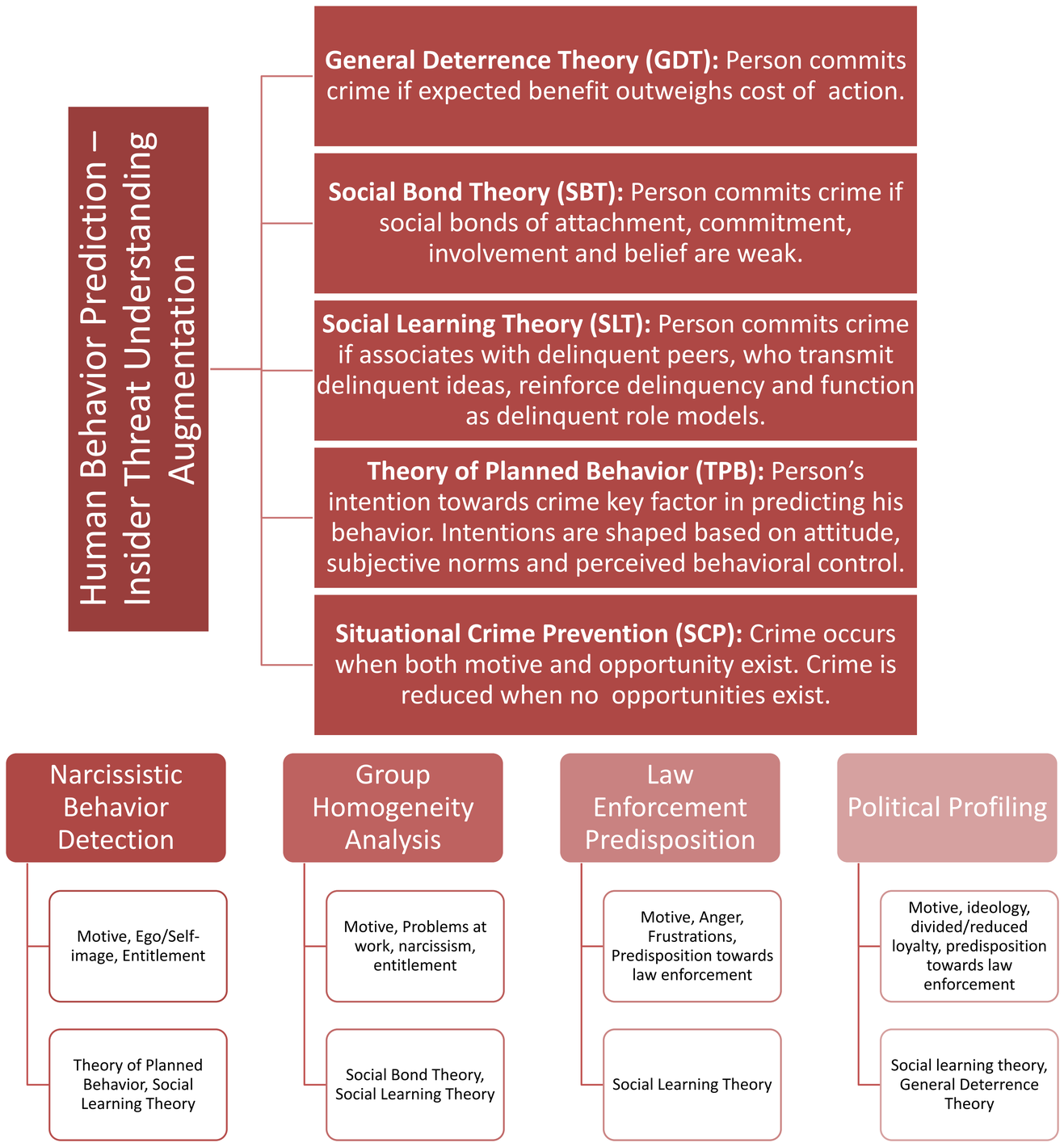


Detection

- Numerous ideas, methods and techniques have been proposed (IDSs, honeypots, honey tokens, network sensors, log file analysis etc.).

Prediction

- Perform automated evaluations via social media & Open Source INTelligence.
- Examination of the predisposition towards malevolent behavior via Social Media.
- Draw conclusions over users' psychosocial traits to predict their behaviour [3].



Twitter - Narcissism

- 41.818 fully crawled users (tweets, profile state, number of: lists, followings and followers, favorites, mentions, retweets).
- Predict the insider threat [4].
- Detect psychosocial characteristic of narcissistic behavior.
- Utilize usage deviation characteristics via graph theoretic analysis.
- Group homogeneity analysis.

YouTube

- 12.964 fully crawled users (profile, uploaded videos, subscriptions, favorite videos, playlists), 207.377 videos (license, number of likes/dislikes, category, tags) and 2.043.362 comments.
- Predict the insider threat.

Predisposition towards Law Enforcement

- Detect negative predisposition towards law enforcement and authorities [5].
- Utilize machine learning, content analysis and usage deviation.
- 2 different approaches:
- Comment/user classification and flat data classification results converge.

Ideology - Divided Loyalty

- Political profiling conclusion extraction [6].
- Radical – Neutral – Conservative clusters.
- Utilize machine learning and content analysis of the dataset.
- Achieved 87% accuracy.
- Developed Panopticon method.
- Highlight ethical issues.

Conclusions

- Interdisciplinary approach towards the solution.
- User/usage profiling leads to classifying users into predefined categories.
- **Ethical** and **legal issues** arise (personality and privacy rights of affected persons).
- Intrusive nature dictates confined application to CI and key, decision-making personnel.
- This topic combines well with similar experience and publications of our Lab [8-12].

References

1. Theoharidou M., Kokolakis S., Karyda M., Kiountouzis E., "The insider threat to Information Systems and the effectiveness of ISO 17799" , Computers & Security, vol. 24, no. 6, pp. 472-484, 2005.
2. Coles-Kemp L., Theoharidou M., "Insider Threat and Information Security Management", Insider Threats in Cyber Security, vol. 49, pp. 45-72, Springer, 2010.
3. Kandias M., Mylonas A., Virvilis N., Theoharidou M., Gritzalis D., "An Insider Threat Prediction Model", Proc. of the 7th International Conference on Trust, Privacy, and Security in Digital Business, pp. 26-37, Springer (LNCS-6264), 2010.
4. Kandias M., Galbogini K., Mitrou L., Gritzalis D., "Insiders trapped in the mirror reveal themselves in social media", Proc. of the 7th International Conference on Network and System Security, pp. 220-235, Springer (LNCS 7873), 2013.
5. Kandias M., Stavrou V., Bosovic N., Mitrou L., Gritzalis D., "Predicting the insider threat via social media: The YouTube case", Proc. of the 12th Workshop on Privacy in the Electronic Society, ACM Press, 2013 (to appear).
6. Kandias M., Mitrou L., Stavrou V., Gritzalis D., "Which side are you on? A new Panopticon vs. privacy", Proc. of the 10th International Conference on Security and Cryptography, pp. 98-110, 2013.
7. 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.
8. Gritzalis D., "Embedding privacy in IT applications development", Information Management and Computer Security, vol. 12, no. 1, pp. 8-26, MCB University Press, 2004.
9. Mylonas A., Dritsas S., Tsoumas B., Gritzalis D., "On the feasibility of malware attacks in smartphone platforms", Proc. of the 9th International Conference on Security and Cryptography, pp. 217-232, Springer Lecture Notes (CCIS-314), 2012.
10. Theoharidou M., Mylonas A., Gritzalis D., "A risk assessment method for smartphones", Proc. of the 27th IFIP International Information Security and Privacy Conference, pp. 428-440, Springer (AICT 267), 2012.
11. Mallios J., Dritsas S., Tsoumas B., Gritzalis D., "Attack modeling of SIP-oriented SPIT", Proc. of the 2nd International Workshop on Critical Information Infrastructures Security, pp. 299-310, Springer (LNCS 5141), 2008.
12. Theoharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", Proc. of the 7th IEEE International Conference in Global Security, Safety and Sustainability, pp. 171-178, Springer (LNICST 0099), 2012.