AN ONLINE GAME SIMULATION ENVIRONMENT FOR DETECTING POTENTIAL DECEPTIVE INSIDERS

Hongmei Chi[1], Shuyuan Mary Ho[2] and Dominique Hubbard[1]
[1]Florida A&M University
[2]Florida State University
Tallahassee, FL 32307, USA

ABSTRACT

This poster presents an initial attempt to simulate a corporate computing environment that can uncover hidden intent within information exchange and interaction among online social actors. The lawful interception approach is deployed in the lab to capture data and information among social actors in online environments. We designed and simulated insider threat scenarios in a controlled lab environment. Captured data is being analyzed with content analysis, LIWC (Linguistic Inquiry and Word Count) toolkits. Our preliminary results shows that deceptive actors tend of use different patterns of communication behavior that can be identified.

1 INTRODUCTION

Insider threat continues to be of serious concern to government agencies and private companies. An insider threat generally refers to a person who has or had authorized access to an organization's network, system, or data, but intentionally misuses that privilege and access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems [2]. Moreover, the risk of exposure through mobile devices and Internet clouds has increased exponentially simply because mobile devices and the cloud environment extend the boundaries and controls of the corporate network domain. The consequences of insider threat or insider attacks can be devastating, and its impacts range from financial loss, damage of reputation, to loss of intellectual property and reputation [2]. The fact that insiders in many cases are current or former employees, interns, contractors and/or business partners makes it more difficult to track and differentiate routine normal behavior from anomalous conduct. Prior research showed that many deviated insiders appeared to display subtle hints in their social networking communications, such as Twitter, or Facebook [4]. One possible direction is to provide an interactive framework for corporate communication, which allows organizations to make sense computationally of their current and regular employees' communicative intent [3, 4].

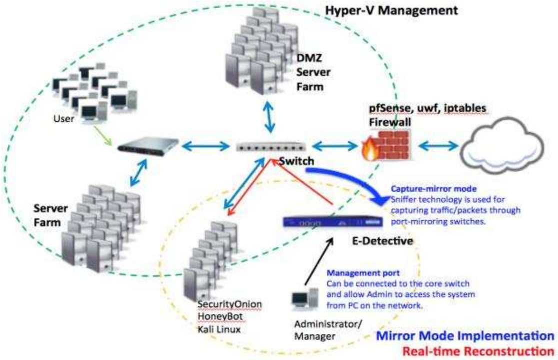
Hyper-V Management
DMZ Server Farm
User
pfSense, uwf, iptables Firewall
Switch
Server Farm
Capture-mirror mode
Sniffer technology is used for capturing traffic/packets through port-mirroring switches.
E-Detective
Management port
Can be connected to the core switch and allow Admin to access the system from PC on the network.
SecurityOnion
HoneyBot
Kali Linux
Administrator/ Manager
Mirror Mode Implementation
Real-time Reconstruction

Figure 1 The virtual lab deployment

This poster describes a study conducted in online simulated incorporate environment based on social networking scenario. The components below demonstrate our initial approach of detecting potential insider threat attacks. We use LIWC (http://liwc.wpengine.com/) toolkit to analyze the language cues from online actors.

2 SIMULATION ENVIRONMENT

The proposed lab was deployed in the virtual lab located at the FSU College of Communication and Information (https://labs.cci.fsu.edu) [1, 2]. To assure the success of the lawful interception program, we identified the data service content in the data capture list for operation. We captured data in its entirety, which included the content of their communication, time-stamps, and the identities of users. Additionally, data such as the protocol types, encryption algorithms, and IP addresses were available but were not subject to this data analysis and reporting. An interactive game interface was developed adopting the chat features of Google+ Hangout. We presented players with interactive scenarios requiring them to write either deceptive or truthful statements. This online game simulates a real-time interactive deception scenario through synchronous communication channels. Each game involves two participants, randomly selected

978-1-4673-9743-8/15/$31.00 ©2015 IEEE

and paired. These players were further randomly assigned with an outer role as either an initiator or a detector in each gaming session. The initiator in each scenario is also randomly assigned with an inner role—either a saint (truthful) or a sinner (deceptive). Our interactive framework captured the ground truth from each initiator player at the beginning of each session. The initiator must answer the question truthfully on a particular topic before the beginning of each scenario. This provides a baseline against which to assess the truthfulness or deceptiveness of his/her subsequent responses to questions posed by the detector, who must decide whether s/he feels the speaker is being truthful or deceptive based on these exchanges [1].

3 EXPERIMENTAL RESULTS

We have provided an initial global view of the data. The graphs below represent the results of LIWC analysis of text files from both “sinners” and “saints.” The data consists of text generated from the 2014 and 2015 “Real or Spiel” game sessions. The files labeled “sinner” contained text from the player characters’ that were labeled sinners within the context of the game, and the sinner files contained text from the player characters’ labeled “saints.” There were a total of 65 text files analyzed, with 32 sinners and 33 saints. Data being analyzed were directly extracted, but not manually cleaned, from the MySQL database of the interactive framework.

There are 19 language-action cues considered as independent variables—being analyzed and portrayed on the scale of normalized word counts [2]. We visualize our data and create a radar chart (see Figure 2). These two spider graphs represent the results of the unfiltered LIWC results of the sinner files and the saint files respectively. The labels on the outside of the circle matches the LIWC scheme codes which were used by LIWC to display the results of the analysis. These results show that Sinners generally used a high level of negation words whereas Saints used a higher amount of social and affect words.

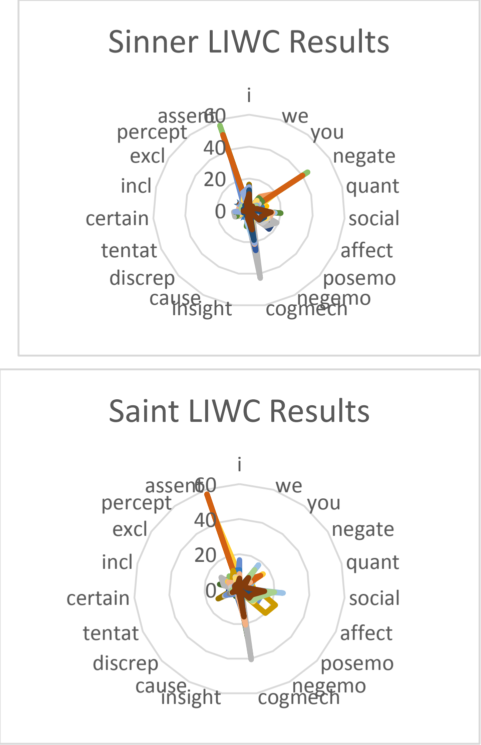

Figure 2 Radar Chart for language-action cues

4 CONCLUSIONS AND FUTURE WORK

This research demonstrates the effectiveness of linguistic analysis as an approach to identify deceptive intent without physical interaction in an organization [1, 2]. Our future work will include collection of a larger dataset, and development of classifiers that learn about online deception in a more in-depth data capture of the insider threat scenarios, and further in real-world social networking sites such as Twitter or Facebook.

REFERENCES

[1] Ho, S.M., Hancock, J.T., et al. (2015) Liar, Liar, IM on Fire: Deceptive language-action cues in spontaneous online communication, IEEE Intelligence and Security Informatics: 157-159. IEEE: Baltimore, MD.

[2] Ho, S.M. et al. (2015) Insider threat: Language-action cues in group dynamics, ACM SIGMIS Computers and People Research: 101-104. ACM: New Beach, CA.

[3] Ho, S.M. and Warkentin, M. (2016) Leader’s dilemma game: An experimental design for cyber insider threat research. Information Systems Frontiers. (To appear).

[4] Brown, C. R., Watkins, A., & Greitzer, F. L. (2013, January). Predicting insider threat risks through linguistic analysis of electronic communication. In System Sciences (HICSS), 2013 46th Hawaii International Conference on (pp. 1849-1858). IEEE.