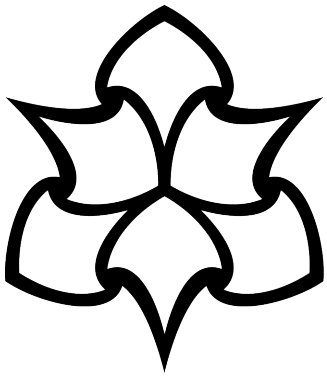


Connected events and malicious insiders: Investigating patterns of insider threat using natural language processing

What is Insider Threat?

Insider threat is a security threat that comes from within an organisation, as apposed to external threats such as hackers. These insiders often have access to systems and information due to their job and understand where there are gaps in security systems. In recent times insider attacks have been widely publicised due to the actions of Edward Snowden and his information theft, however all organisations are at risk of insider attacks, and there are many ways for an insider to damage or attack an organisation or system. These can include malicious insiders, those who purposely and knowingly commit attacks, and inadvertent insiders, those who click on a link in a suspicious email or leave a security door open while going outside to have a cigarette.

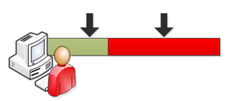
Insiders can be anyone within an organisation

How do we detect insider threats?

Currently insider threats are detected in several ways such as, users accessing files or information that deviates from the expected activity on an IT system or network, behavioural or lifestyle clues such as resentment or gambling. Often insider threats remain unknown and are found by accident or well after the damage has been done. Due to the large amount of privileged access insiders have, as well as their knowledge of security flaws within systems it is no surprise that they are hard to detect. Current state of the art for computer systems involves the tracking and monitoring of computer logs and network traffic, using machine learning to detect anomalies.

Insider Threat activity is often committed at the same time as regular activity

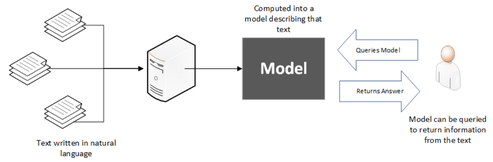
However, if the insider threat activity takes place while a baseline "normal" is being recorded, or if the insider threat activity is so close to the normal baseline with few anomalies it cannot be detected.



If the baseline reading for normal activity is taken when insider activity is being recorded it can be impossible to detect

Why use natural language processing?

Natural language processing (NLP) is the process in which a computer can "understand" natural language, this can be text or speech. There are many different types of NLP tasks, such as translation, summarisation, recognising appointments from emails and finding entities such as places or people's names. Insider threats are witnessed by different people, at different times, and in different ways, after an attack reports can be a valuable source of information on the attack, however this value is often lost and locked behind large amounts of text, using natural language processing details can be extracted which would otherwise be missed. This can be achieved by taking reports written after an insider attack and mapping these relationships, focusing on actors, actions, causality and events that took place. This will then allow an investigator to explore an attack, and develop mitigation and defence strategies from their understanding of the attack. In addition to this new detection systems can be developed and created based on the evolving nature of the attack



An example NLP system

Goal of this Research

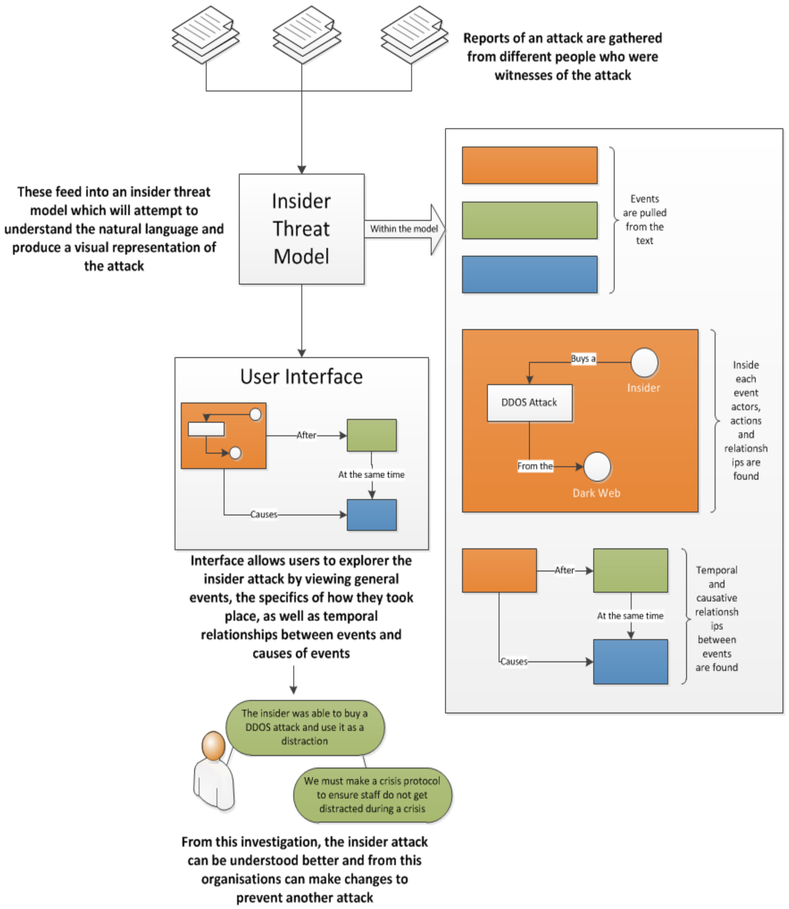
To present a new methodology for the investigation and understanding of insider threat events. Using natural language processing and visualisations to investigate written reports, revealing links between actions, actors, events and causes of insider attack.

References

Cappelli, D., Moore, A. and Trzeciak, R. (2015) *The Cert Guide to Insider Threats: How to prevent, detect, and respond to Information Technology crimes (Theft, Sabotage, Fraud)*. Addison-Wesley. Available at: 10.1017/CBO9781107415324.004 (Accessed: 21 February 2018).

Sanzgiri, A. (2016) 'Classification of Insider Threat Detection Techniques', *CISRC '16 Proceedings of the 11th Annual Cyber and Information Security Research Conference*, New York, New York, USA: ACM Press, pp. 5–8. Available at: 10.1145/2897795.2897799 (Accessed: 21 February 2018).

Proposed natural language processing and visualisation techniques for insider threat



Katie Paxton-Fear K.Paxton-Fear@cranfield.ac.uk †, Dr Duncan Hodges d.hodges@cranfield.ac.uk †,

Dr Oliver Buckley o.buckley@uea.ac.uk‡

† Cranfield University ‡ University of East Anglia

Centre for Electronic Warfare and Cyber, Cranfield Defence and Security, Defence Academy of the United Kingdom

www.cranfield.ac.uk