

Semantic Hacking and Intelligence and Security Informatics

Paul Thompson

Institute for Security Technology Studies
Dartmouth College
Hanover, NH 03755
Paul.Thompson@dartmouth.edu

Extended Abstract

In the context of information warfare Libicki first characterized attacks on computer systems as being physical, syntactic, and semantic, where software agents were misled by an adversary's misinformation [1]. Recently cognitive hacking was defined as an attack directed at the mind of the user of a computer system [2]. Countermeasures against cognitive and semantic attacks are expected to play an important role in a new science of intelligence and security informatics. Information retrieval, or document retrieval, developed historically to serve the needs of scientists and legal researchers, among others. In these domains, documents are expected to be honest representations of attempts to discover scientific truths, or to make sound legal arguments. This assumption does not hold for intelligence and security informatics.

Intelligence and security informatics will be supported by data mining, visualization, and link analysis technology, but intelligence and security analysts should also be provided with an analysis environment supporting mixed-initiative, utility-theoretic interaction with both raw and aggregated data. This environment should include toolkits of semantic hacking countermeasures. For example, faced with a potentially deceptive news item, an automated countermeasure might provide an alert using adaptive fraud detection algorithms [3], or through a retrieval mechanism allow the analyst to quickly assemble and analyze related documents bearing on the potential misinformation. The author is currently developing such countermeasures.

References

1. Libicki, M.: The mesh and the net: Speculations on armed conflict in an age of free silicon National Defense University McNair Paper 28 (1994)
2. Cybenko, G., Giani, A., Thompson, P.: Cognitive Hacking: A Battle for the Mind IEEE Computer. Vol. 35, No. 8. (2002) 50-56
3. Fawcett, T., Provost, F.: Fraud Detection. In: Kloesgen, W., Zytkow, J. (eds.) Handbook of Data Mining and Knowledge Discovery, Oxford University Press (2002)