

Utility-Theoretic Information Retrieval, Cognitive Hacking, and Intelligence and Security Informatics

Paul Thompson
Dartmouth College

Introduction

Libicki first characterized attacks on computer systems in the context of information warfare as being physical, syntactic, and semantic, where software agents were misled by misinformation deliberately fed by an adversary [1]. Recently Cybenko et al. [2] defined cognitive hacking as an attack on a computer system directed at the mind of the user of the system, which, in order to succeed, had to influence the user's perceptions and behavior. This paper generalizes the concept of cognitive hacking, placing it in Libicki's framework of semantic attack. The concept of semantic attacks and their countermeasures are expected to be an important component of a new science of intelligence and security informatics. In particular cognitive attacks influence the utility of information accessed from a computer system. Furthermore, since the cognitive attacker can be a trusted insider of an organization, it is important for that organization's computer system to have a cost model of its information assets as well as a model of each insider's use of the computer system.

Background

In 1981, Landwehr provided a discussion of computer system security which has framed subsequent discussion of computer security [3]. His model arose from a consideration of the requirements of military security. He postulated that:

Information contained in an automated system must be protected from three kinds of threats: (1) the *unauthorized disclosure* of information, (2) the *unauthorized modification* of information, and (3) the *unauthorized withholding* of

information (usually called *denial of service*)

Libicki described semantic attacks in the context of information warfare, where software agents were misled by misinformation which they were being deliberately fed by an adversary [1]. Schneier, by contrast, defined semantic attacks as “. . . attacks that target the way we, as humans, assign meaning to content. . . . Semantic attacks directly target the human/computer interface, the most insecure interface on the Internet” [4].

Denning also developed a similar notion to semantic attacks, which she referred to as information warfare [5], described as a struggle over an information resource by an offensive and a defensive player. The resource has an exchange and an operational value. The value of the resource to each player can differ depending on factors related to each player's circumstances. The outcomes of offensive information warfare are: increased availability of the resource to the offense, decreased availability to the defense, and decreased integrity of the resource. Although not receiving as much attention as syntactic or external attacks, the majority of attacks on a computer system come from insiders.

Cognitive and Semantic Hacking

In Cybenko et al. [2] the focus of semantic attacks was on manipulation of consumers on the Internet, e.g., through pump-and-dump schemes. This paper considers two types of extensions to this model. First, the notion of cognitive attacks is extended to a consideration of deception and denial in open source intelligence, where again the attack is against the mind of the user, i.e., the intelligence analyst. Second the notion of semantic attacks is extended to cover attacks against the semantics of

the computer system in a computer-theoretic sense, as described by Wing [6]. As an example, consider the semantics of an intelligence textual database. Intelligence analysts access this database in the course of their work. If an analyst engages in espionage through this access, this is a violation of the semantics of the database. The database system needs to have a cost model of the documents it contains and it needs to model the transactions of the analyst.

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 interaction with both raw and aggregated data sets [7]. Since analysts will need to defend against semantic attacks, this environment should include a toolkit of semantic hacking countermeasures. For example, if faced with a potentially deceptive news item from FBIS, an automated countermeasure might provide an alert using adaptive fraud detection algorithms [8] or through a retrieval mechanism allow the analyst to quickly assemble and interactively analyze related documents bearing on the potential misinformation. The author is currently developing both of these countermeasures.

Information retrieval, or document retrieval, developed historically to serve the needs of scientists and legal researchers, among others. Despite occasional hoaxes and falsifications of data in these domains, the overwhelming expectation is that documents retrieved are honest representations of attempts to discover scientific truths, or to make a sound legal argument. This assumption does not hold for intelligence and security informatics. Most information retrieval systems are based either on: a) an exact match Boolean logic by which the system divides the document collection into those documents matching the logic of the request and those that do not, or b) ranked retrieval. With ranked retrieval a score is derived for each document in the collection based on a measure of similarity between the query and the document's representation, as in the vector space model [9], or based on a probability of relevance [10, 11]

Although not implemented in existing systems, a utility theoretic approach to information retrieval

[12] shows promise for a theory of intelligence and security informatics. In information retrieval predicting relevance is hard enough. Predicting utility, although harder, would be more useful. When information contained in, say, a FBIS document, may be misinformation, then the notion of utility theoretic retrieval, becomes more important. The provider of the content may have believed the information to be true or false, aside from whether it was true or false in some objective sense. The content may be of great value to the intelligence analyst, whether it is true or false, but, in general, it would be important to know not only whether it was true or false, but also whether the provider believed it to be true or false. Current information retrieval algorithms would not take any of these complexities into account in calculating a probability of relevance.

Predictive Modeling in Intelligence and Security Informatics

Predictive modeling using the concepts of cognitive hacking and utility-theoretic information retrieval can be applied in two intelligence and security informatics settings which are mirror images of each other, i.e., the user's model of the system's document content and the system's model of the user as a potential malicious insider. Consider an environment where an intelligence analyst accesses sensitive and classified information from intelligence databases. The accessed information itself may represent cognitive attacks coming from the sources from which it has been gathered, e.g., FBIS documents. As discussed above, each of these documents will have a certain utility for the analyst, based on the analyst's situation, based on whether or not the documents contain misinformation, and, if the documents do contain misinformation, whether, or not, the analyst can determine that the misinformation is present. On the other hand, the analyst might be a malicious insider engaged in espionage. The document system will need to have a cost model for each of its documents and will need to build a model of each user, based on the user's transactions with the document system and other external actions. This model could be expressed as a Hidden Markov Model.

Denning's theory of information warfare [5] and an information theoretic approach to the value of information [13, 14] can be used to rank potential risks given the value of each document held by the

system. Particular attention should be paid to deception on the part of the trusted insider to evade detection, using cognitive hacking countermeasures [2]. Modeling the value of information to adversaries will enable prediction of which documents are likely espionage targets and will enable development of hypotheses for opportunistic periods and scenarios for compromise. These models will be able to detect unauthorized activity and to predict the course of a multi-stage attack so as to inform appropriate defensive actions.

Conclusions

Misinformation, or semantic hacking, plays a much more prominent role in intelligence and security informatics than it has played in traditional scientific informatics. The status of content as information, or misinformation, in turn, influences its utility for users. This paper suggests the need for tools to detect and defend against semantic hacking and outlines the role for utility theoretic retrieval, along side data mining, as an important foundational technology for intelligence and security informatics.

References

1. Libicki, Martin. The mesh and the Net: Speculations on armed conflict in an age of free silicon National Defense University McNair Paper 28, 1994.
<http://www.ndu.edu/ndu/inss/macnair/mcnair28/m028cont.html>
2. Cybenko, George; Giani, Annarita; and Thompson, Paul. Cognitive Hacking: A Battle for the Mind *IEEE Computer* vol. 35, no. 8, August 2002, p. 50-56.
3. Landwehr, Carl E. Formal models of computer security *Computing Surveys*, vol. 13, no. 3, 1981.
4. Schneier, Bruce. 2000. "Semantic attacks: The third wave of network attacks" *Crypto-gram Newsletter* October 15, 2000.
<http://www.counterpane.com/crypto-gram-0010.html>
5. Denning, Dorothy. *Information warfare and security* Reading, Mass.: Addison Wesley, 1999.
6. Wing, Jeannette M. A Symbiotic Relationship Between Formal Methods and Security *Proceedings from Workshops on Computer Security, Fault Tolerance, and Software Assurance*, 1998.
7. Thompson, Paul. Semantic Hacking and Intelligence and Security Informatics" *NSF / NIJ Symposium on Intelligence and Security Informatics, Lecture Notes in Computer Science*, Berlin: Springer-Verlag, June 1-3, 2003, Tucson, Arizona, 2003.
8. Fawcett, Tom and Provost, Foster in W. Kloesgen and J. Zytow (eds.) *Handbook of Data Mining and Knowledge Discovery*, Oxford University Press, 2002.
9. Salton, Gerard and McGill, Michael. *Introduction to Modern Information Retrieval* New York: McGraw-Hill, 1983.
10. Maron, M.E. and Kuhns, J.L. On relevance, probabilistic indexing and information retrieval *Journal of the ACM* vol. 7 no. 3, 1960, p. 216-244.
11. van Rijsbergen, C.J. *Information Retrieval* 2d. edition, London: Butterworth, 1979.
12. Cooper, William S. and Maron, M.E. Foundations of Probabilistic and Utility-Theoretic Indexing *Journal of the Association for Computing Machinery* vol. 25, no. 1, 1978, p. 67-80.
13. Cover, Thomas A. and Thomas, Joy A. *Elements of Information Theory* New York: Wiley, 1991.
14. Cybenko, George; Giani, Annarita; and Thompson, Paul. Cognitive Hacking and the Value of Information *Workshop on Economics and Information Security*, May 16-17, 2002, Berkeley, California.