

Search and Misinformation in Intelligence and Security Informatics

Paul Thompson

25 April 2006

Outline

- Intelligence and Security Informatics
- Semantic Hacking Project
- Detecting Deception in Language
- Infrastructural Solutions

Intelligence and Security Informatics

- Symposium on Intelligence and Security Informatics,
 - First held in 2003
 - Now held annually
 - Sponsored by National Science Foundation and National Institute of Justice
- Towards a new science along the lines of bioinformatics

Intelligence and Security Informatics (cont.)

- Traditional Information Retrieval
 - Developed to serve needs of scientific researchers and attorneys
 - Misinformation usually not seen as an issue
- Increasing fraud in science: Rossner [Managing Editor, Journal of Cell Biology] estimates that roughly 20% of accepted manuscripts contain at least one figure that has to be remade because of inappropriate image manipulation. 1% of figures are fraudulent.

Intelligence and Security Informatics (cont.)

- Utility-Theoretic Retrieval taking into account misinformation
 - Cognitive hacking, e.g., Internet stock trading pump-and-dump schemes
 - Deception and denial in open source intelligence
 - Semantic attacks on software agents in warfare

Semantic Hacking Project

- Institute for Security Technology Studies, Dartmouth College, 2001-2003
- Funded by National Institute of Justice
- Computer Security Focus

Types of Attacks on Computer Systems

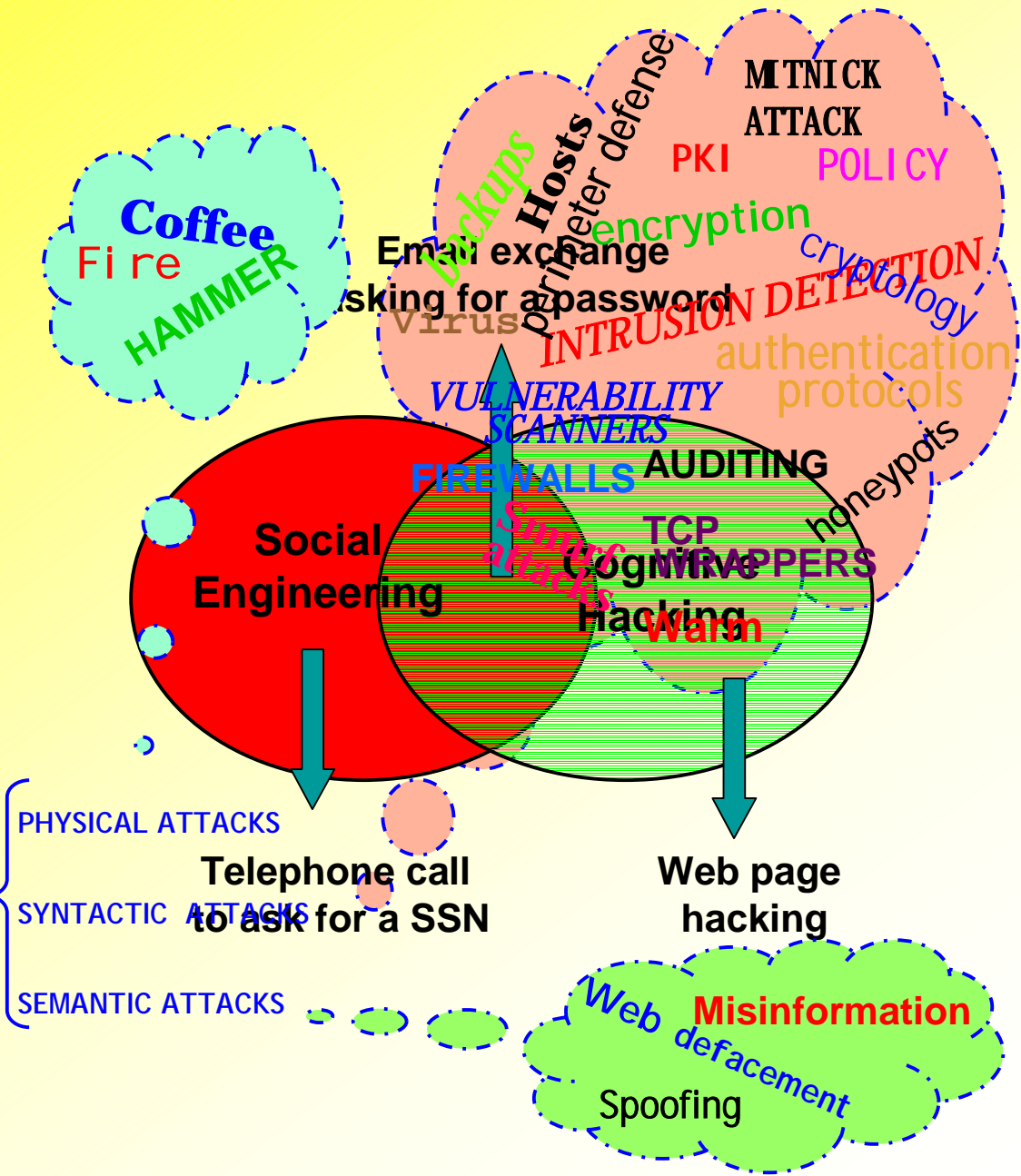
- Physical
 - Syntactic
 - Semantic (Cognitive)
- Martin Libicki: The mesh and the net: Speculations on armed conflict in an age of free silicon. 1994.

Perception Management

- “. . . Information operations that aim to affect the perceptions of others in order to influence their emotions, reasoning, decisions, and ultimately actions.”
 - Denning, p. 101
- Continuum
 - Propaganda -> Psychological Operations ->
-> Advertising -> Education
- Has existed long before computers

Related concepts

- Propaganda
- Advertising
- Social Engineering
- Semantic Hacking
- Computer Security
- Information Warfare



Definition

COGNITIVE HACKING

A networked information system attack that relies on changing human users' perceptions and corresponding behaviors in order to be successful.

Key elements:

- ❑ Requires the use of an information system - not true for all social engineering
- ❑ Requires a user to change some behavior- not true for all hacking

Exploits our growing reliance on networked information sources

NEI Webworld pump-and-dump

- November 1999 – two UCLA graduate students and one associate purchase nearly all shares of bankrupt NEI Webworld
- Open many Internet message board accounts and post over 500 false messages to pump value of stock
- In less than one day stock value increased from \$0.13 to \$15 per share - made about \$364,000 by selling shares

Countermeasures for Misinforming News

- End user finds possibly misinforming news item
- User wants to act quickly to make huge profit, but does not want to be victim of pump-and-dump scheme
- Query automatically generated and submitted to Google News to create collection of related news items

News Countermeasure 1: News Verifier

- Stories optimally re-ranked and presented to user
- User scans top two or three stories and decides whether or not original news item is reliable
- Countermeasure fails if user cannot determine reliability based on top two or three ranked stories
- News Verifier – prototype implementation

News Countermeasure 2

- Collection assembled by search of Google News is analyzed automatically, e.g., via information trajectory modeling
- Countermeasure system extracts monetary amounts or price movement references from text and compares to database of stock prices
- If movement is out of range, user is alerted
- Can process 2 work better than 1?

Denial and Deception

- Foreign Broadcast Information Service
 - Collects news from around the world to support open source intelligence analysis
 - Misinformation could be planted in stories to mislead analysts
 - FBIS going beyond traditional sources of information to collect more information from the Web
 - More chance for denial and deception

Detecting Deception in Language

- First of seven National Science Foundation and Office of Science and Technology Policy Workshops on Security Evaluations – summer 2005
- Most participants psychologists
- Funding expected in FY 2007

Infrastructural Changes

- Lynch, Clifford “When Documents Deceive: Trust and Provenance as New Factors for Information Retrieval in a Tangled Web, JASIS&T 52(1), 2001
- Pedigree Management and Assessment Framework – Air Force SBIR, ATC-NY
- Internet Search Environment Number (ISEN)

Conclusions

- Semantic Hacking countermeasures will play an important role in cyber security and in intelligence and security informatics
- Infrastructural development will also play an important role