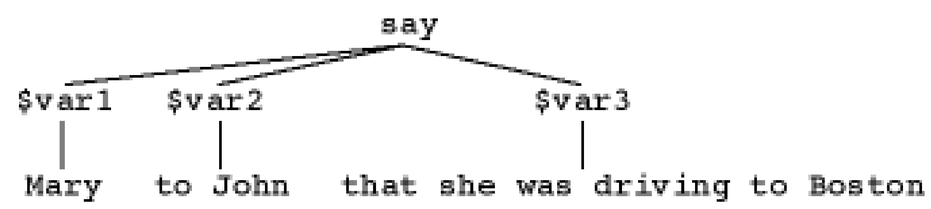
CERIAS

Natural Language Information Assurance and Security

Introduction: Ontological Semantics

- Inclusion of **natural language (NL) data** sources as an integral part of the overall data sources in InfoSec applications
- Analysis of NL at the level of meaning with the knowledge-based methods **ontological semantics**
- already used for MT, IR, IE, QA, planning and summarization,data mining, information security, intelligence analysis, etc.

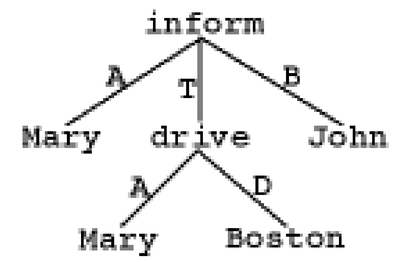
- syntactic analysis



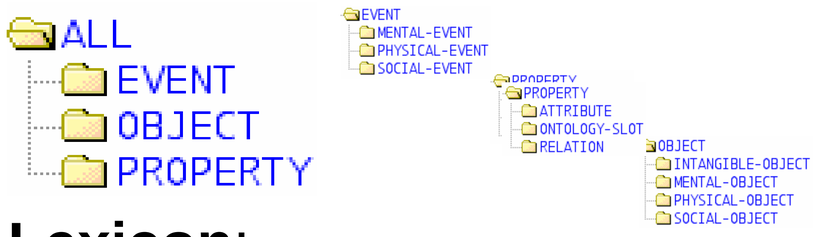
- semantic analysis

```
(inform
   (agent Mary)
   (theme drive
       (agent Mary)
       (destination Boston))
   (beneficiary John))
```

TMR tree

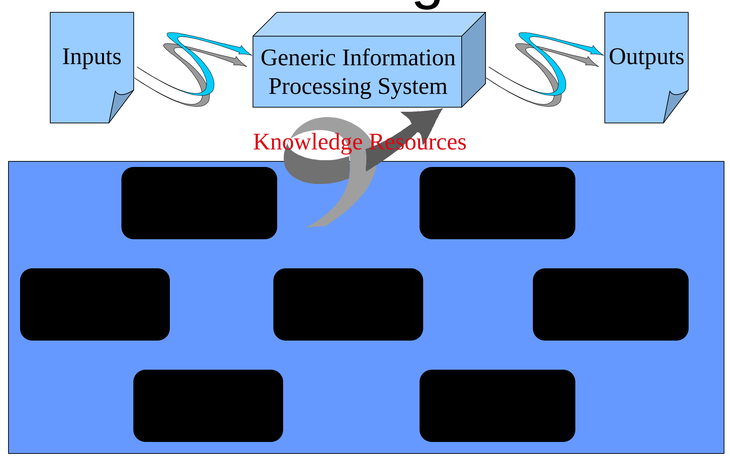


- **Ontology**:
  hierarchy of conceptual nodes



- **Lexicon**:
  entries explained in terms of nodes
- Necessary modules:
  Analyzer, Generator
- Basis for analysis into **Text-meaning-representation** (TMR)

- Resources of ontological semantics



- References

Atallah, M. J., C. J. McDonough, V. Raskin, and S. Nirenburg 2001. Natural Language Processing for Information Assurance and Security: An Overview and Implementations. In: M. Schaefer (ed.), Proceedings. New Security Paradigm Workshop. September 18th-22nd, 2000, Ballycotton, County Cork Ireland. New York: ACM Press, pp. 51-65.

Atallah, M. J., V. Raskin, M. Crogan, C. F. Hempelmann, F. Kerschbaum, D. Mohamed, and S. Naik 2001. "Natural Language Watermarking: Design, Analysis, and a Proof-of-Concept Implementation." In: I. S. Moskowitz (ed.), *Information Hiding: 4th International Workshop, IH 2001, Pittsburgh, PA, USA, April 2001 Proceedings.* Berlin: Springer, 185-199.

Atallah, M. J., V. Raskin, C. F. Hempelmann, M. Karahan, R. Sion, U. Topkara, and K. E. Triezenberg 2002. "Natural Language Watermarking and Tamperproofing." In: F. A. P. Peticolas (ed.), *Information Hiding: 5th International Workshop, IH 2002, Proceedings.* Berlin: Springer, (forthcoming).

McDonough, J. 2000. Mnemonic String Generator: Software to aid memory of random passwords. CERIAS TR.

Mohamed, D. 2001. *Ontological Semantics Methods for Automatic Downgrading.* Unpublished Masters Thesis, Program in Linguistics and CERIAS, Purdue University, CERIAS TR.

Nirenburg, S. and V. Raskin 2003. *Ontological Semantics.* Cambridge, MA: MIT Press (forthcoming).

Raskin, V., M. J. Atallah, C. F. Hempelmann, and Dina Mohamed 2001. *Hybrid Data and Text System for Downgrading Sensitive Documents.* CERIAS TR.

Raskin, V., S. Nirenburg, M. J. Atallah, C. F. Hempelmann, and K. E. Triezenberg 2002. "Why NLP should move into IAS." In: Steven Krauwer (ed.), *Proceedings of the Workshop on a Roadmap for Computational Linguistics*, Taipei, Taiwan: Academia Sinica, 2002, pp. 1-7.

Raskin, V., C. F. Hempelmann, K. E. Triezenberg, and S. Nirenburg 2002. "Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool." In: V. Raskin and C. F. Hempelmann (eds.), *Proceedings. New Security Paradigms Workshop 2001. September 10th-13th, Cloudcroft, NM, USA*, New York: ACM Press, pp. 53-59.

PURDUE UNIVERSITY

CERIAS®

e-Enterprise Center

CERIAS

Natural Language Information Assurance and Security

Applications (1)

Mnemonic String Generator (MSG): Memorization of Random Passwords

- *problem*: weak passwords that are easy to remember
  - poorly chosen: existing words, names, possibly augmented by leetspeak substitution
  - rarely changed
- *solution*: random passwords that are easy to remember
  - turned into memorable humorous sentences or jingles
- *requirements:*
  - handle alphabetic and alphanumeric passwords
  - handle all possible permutations of the *n*-character x *i*-symbol password (e.g., an 8-character password limited to characters a-z yields 2x1011 possible passwords)
  - generate a mnemonic from which the password is easily recoverable because it is more memorable than the password
- *method*:
  - if the password character is (a-z) or (A-Z), then the mnemonic word will begin with that character; for example, “a” -> “apple” and “B” -> “Banished”
  - if the password character is (0-9), then the mnemonic word will begin with the letter corresponding to the word for the digit in all caps; for example, “8” -> “EGGS” resulting jingle has meter (rhythm) and two clauses humorously opposed
- *examples*:

  WDhpuD53: Walesa Desired heston's pole, while ulster Doubted FISCHER's TEST.
  g2RTwEhUz: gramm THANKED Reagan's Toes, while Ehud hindered Ursula's zipper.

Natural Language Sanitizer/Downgrader

- *purpose:*
  automatically and seamlessly removes classified or proprietary information from documents that have to be shared with unauthorized parties
- *customers*:
  - governmental agencies under presidential de-/reclassification order
  - private industries, who need to closely monitor traffic between separate
    - open/public/unclassified
    - closed/private/classified

    circuits in their network
- *problem*:
  too costly and slow to do manually
- *solution*:
  meaning-based NLP methods of ontological semantics remove sensitive content or replace it with inoccuous text

Terminology Standardization

- In IAS, terminology evolves rapidly and is not standard between groups
- “Dialectal” differences waste time and can easily cause errors
- An ontological processor can recognize a concept by its properties rather than its name(s), allowing users to have their own “dialects” and also avoid confusion

Semantic Mimicking

- Steganography damages a text
- Stylistic analyzers can easily pick out phrases that have been damaged, pinpointing the location of information
- An ontological processor can cause semantically and syntactically correct damage throughout a text to camouflage information-containing phrases

PURDUE UNIVERSITY

CERIAS®

e-Enterprise Center

CERIAS

Natural Language Information Assurance and Security

Applications (2): Watermarking and Tamper-proofing

Properties of Proposed Schemes

- Abides by the common principles of watermarking, such as undetectability, holding up in court, public algorithm etc.
- Hides in digital NL text itself, not image of it.

Watermarking Algorithm:

- Split text into sentences $s_1,...,s_n$
- Find tree representation $T_1,...,T_n$ of each sentence
- Map each tree into a bit string $B_1,...,B_n$ according to secret key
- Choose subset $t_1,...,t_\alpha$ of sentences according to secret key
- Transform subset, such that β bits of each $B_{t1},...,B_{t\alpha}$ correspond to the watermark W

Probabilities of damage

- Meaning-modifying transformation: $<=3\alpha/n$
- Insertion of a sentence: $<=2\alpha/n$
- Moving a block of sentences:$<=3\alpha/n$
- Meaning-preserving transformation on semantic wm: 0

All of the above are upper bounds

Info-Hiding based on Syntactic Analysis

Syntactic tree representation is modified by:

"The dog chased the cat."

- Passivization: the cat was chased by the dog
- Adjunct movement: (often) the dog (often) chased the cat (often)
- Clefting: it was the dog that chased the cat
- Adjunct insertion: it seems that the dog chased

Info-Hiding based on Semantic Analysis

higher bandwidth than syntactic-based

"*The Pentagon ordered two new spy planes to the region to start flying over Afghanistan*"

TMRs are modified by:

- Grafting: The Pentagon ordered two new spy planes to the region to start flying over Afghanistan,which has been under attack since October.
- Pruning: Afganistan has been under attack since October, and the Pentagon ordered two new spy planes to the region to start flying over there.
- Substitution: The Pentagon ordered two new spy planes to the region to start flying over the Taliban-ruled country.

Tamper-proofing based on Syntactic and Semantic Analysis

- Formatting modifications do not constitute tampering (else problem is trivial)
- Brittle watermark as witness to integrity
- Two way "chaining" of sentences according to secret ordering
  - First pass modification via semantic transformations, second pass in reverse order via syntactic transformations
  - *It was the* Pentagon ordered two new spy planes to the region to start flying over the Taliban-ruled country.
- Probability of escaping detection of tampering on a sentence:

$2^{-b*(1+\text{total length of chain})}$

PURDUE UNIVERSITY

CERIAS

e-Enterprise Center

CERIAS

Natural Language Information Assurance and Security

Applications (3)

Surveillance

Automatic detection of protected content at the perimeter when content-modification (sanitization and/or downgrading) is not practical or allowable

- Two-pass system:
  - Content is passed through lightweight semantic analysis at the perimeter
  - Content meeting the alert criteria is passed to the ***full offline semantic analysis*.**
- Full semantic analysis mirrors analysis used in downgrading
- Flagged content and results of analysis are passed to human analyst for *approval*, *negotiation*, and *action*.

Attack Detection and Prevention - Crawling the Web

Web crawling is used as an offline search tool in combination with semantic analysis to highlight content which may indicate an exploit or potential attack.

- Semantic analysis is necessary to differentiate idle chatter from serious threats; keyword extraction is not enough.
- Hybrid texts (exploit code and natural language text) present a special challenge for lexical and ontological acquisition
- Results of semantic analysis may be used in the future to generate automated, standardized exploit reports

Intrusion Detection

- Current **Intrusion Detection Systems (IDS)** are not being fully utilized
- Heterogeneous data formats and languages in IDS's make correlation impossible
- Inclusion of NLP in IDS's (or a broker) can allow for more effective use of correlation engines by:
  - Transforming inputs to a language understood by the destination
  - Categorizing inputs and relaying them to an appropriate destination

Steganalysis

- Analyzing streaming information is a very new in information retrieval.
- Crucial for auditing information flow to and from secure areas.
- Cannot store the information; need to have a compact representation of the past.
- TMRs have the ultimate summarizing capability for natural language; capturing content, and style.
- Unaudited information flow is possible using covert channels.
- Threat to security if measures for detection of stego are not taken.
- Steganalysis exists for images.
- Steganogaphy uses generation techniques to create or modify cover.
- TMRs are a robust representation of the information in text.
- Anomalies in TMR for an author flag steganography.