Detecting the Misappropriation of Sensitive Information through Bottleneck Monitoring

SKM 2004

TJ Goan
Stottler Henke Associates Inc.

1107 NE 45th St., Suite 310, Seattle, WA 98105
206-545-1478 FAX: 206-545-7227
goan@stottlerhenke.com

ARDA

Stottler Henke
Smarter Software Solutions

ARDA

The Insider Threat

- Much bigger risk to corporations and government organizations than outsider penetration
- Insiders can go low and slow and exploit the trust of others
- Physical Access
- Difficulty in specifying attack signatures
- Insufficiency of statistical anomaly detection
- Many attacks paths undetectable by sensors

Stottler Henke
Smarter Software Solutions

Our Focus

Unauthorized Information Access / Distribution

- Protect intellectual property from theft
- Protect sensitive intelligence
  - Special Access Programs (SAP) & Spillage
- Attack method independent
  - Cooperative, distributed, multi-stage attacks
  - Human channels
- **Information** rather than document control

Stottler Henke
Smarter Software Solutions

ARDA

Assumptions

- Some collection of documents has been identified as “access restricted” and that we know who has legitimate privileges to access that information
- The insider will transport, view, or (at least temporarily) store the *access restricted* information within the monitored environment during the attempt to exploit it
- We can decode the information

Stottler Henke
Smarter Software Solutions

Obvious Approaches

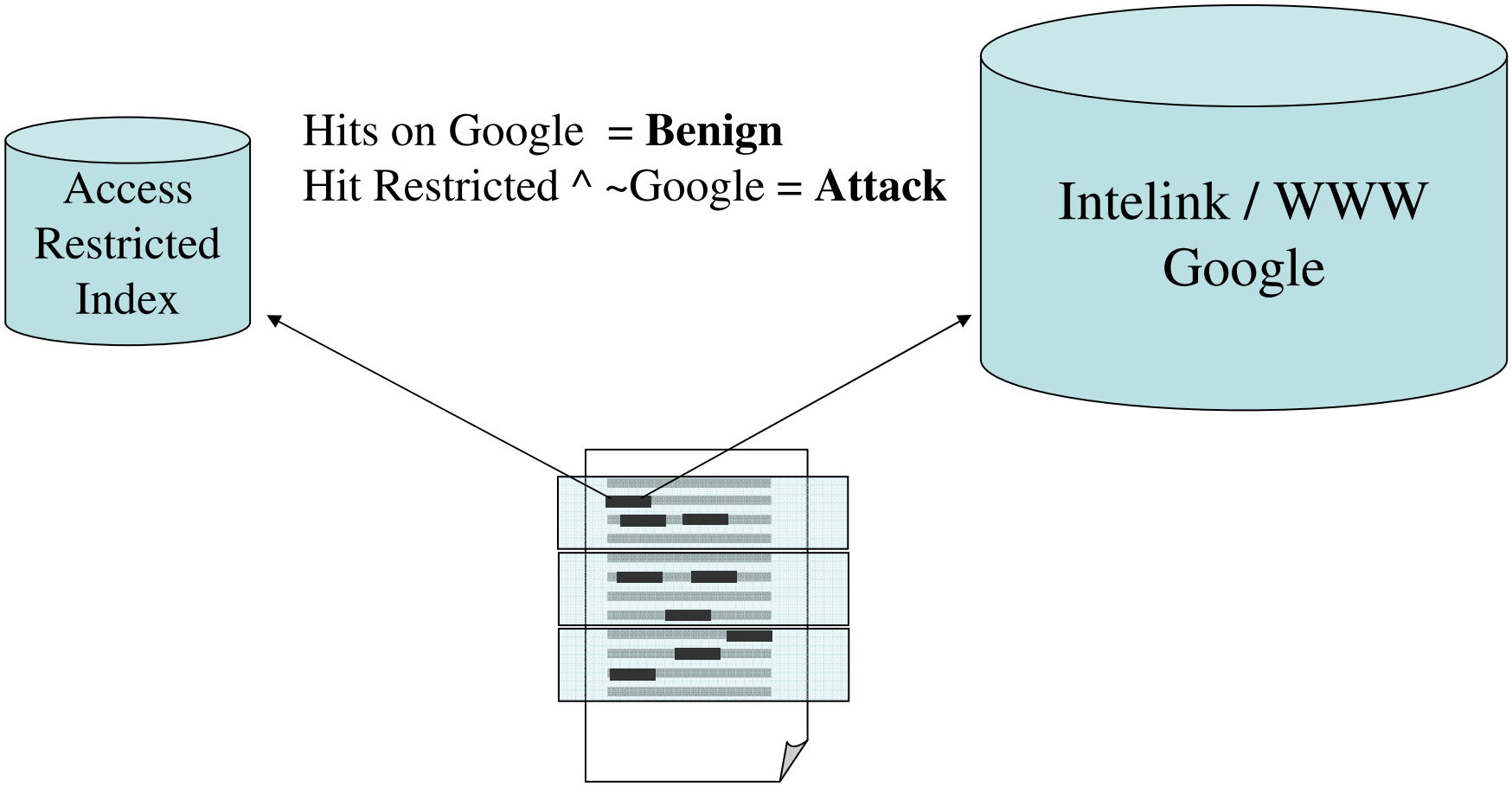
- Document identifiers, checksums, & forensic file access analysis based methods
  - Assume too much
- Simple string matching
  - High false alarm rates
- Document similarity (key terms, named entities, or concepts)
  - Higher false positive rates – not interested in topically related, only derivative documents
  - Pairwise comparisons are costly

Our Solution

- Protect content by monitoring bottlenecks
  - Compliments strong access controls
- SL-SAFE: **S**tochastic **L**ong-**S**tring **A**nalysis with **FE**edback
  - Monitors sample strings and search for them in indices of (1) *public* and (2) *access restricted* content
  - Feedback direct from the content creator quickly minimizes false alarms

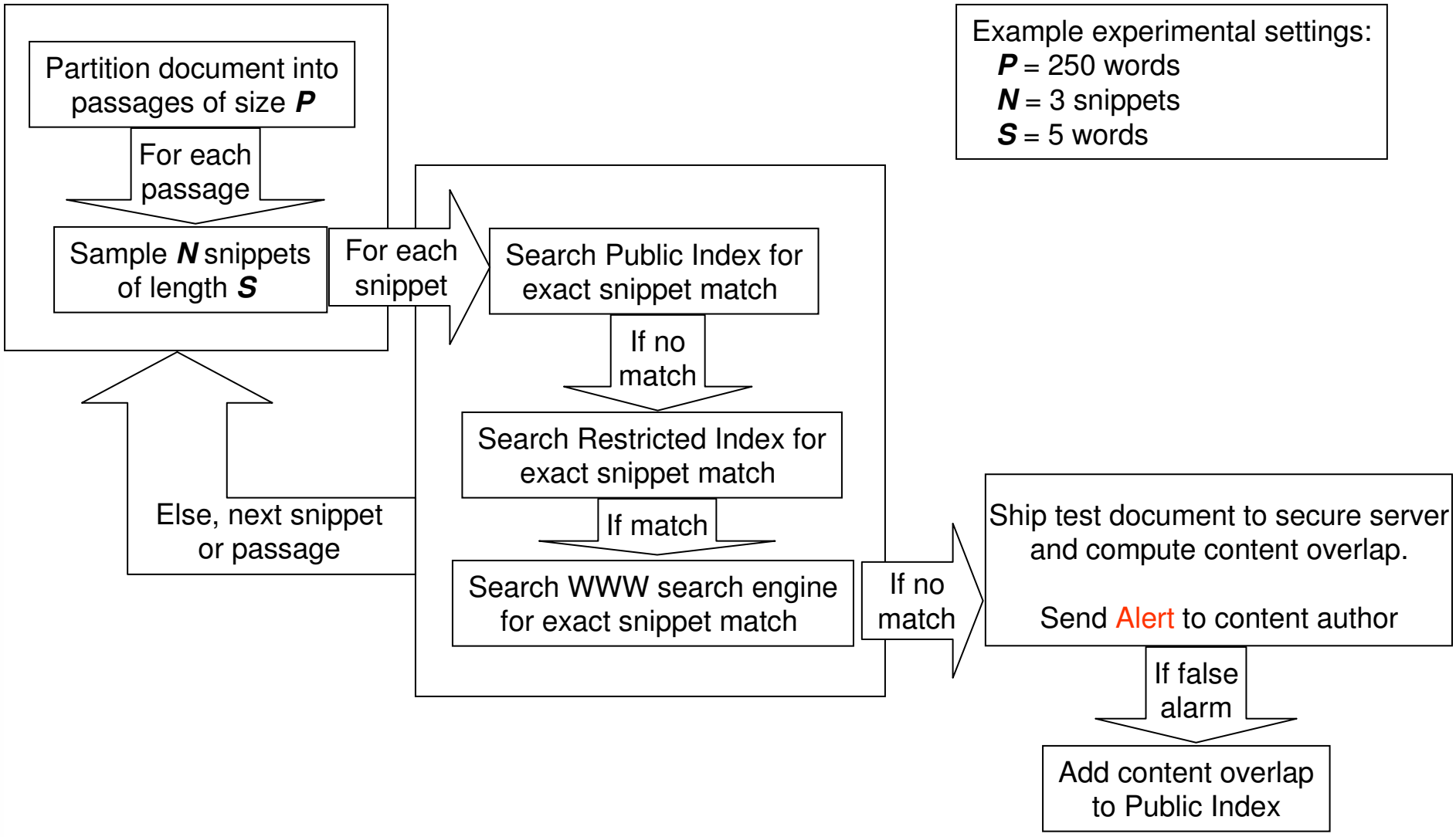
Stottler Henke
Smarter Software Solutions

SL-SAFE Overview



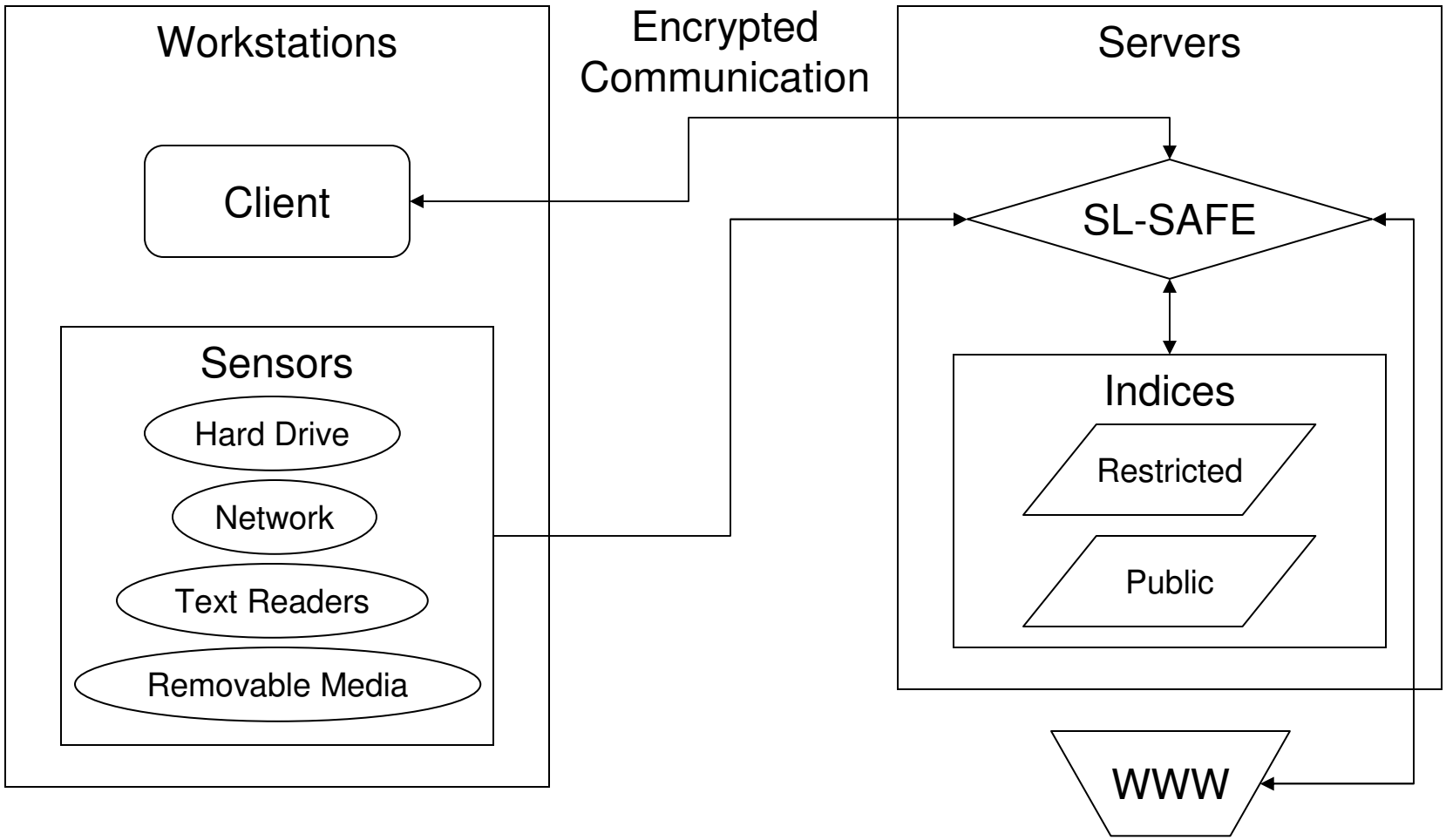
Stottler Henke
Smarter Software Solutions

SL-SAFE Algorithm



Stottler Henke
Smarter Software Solutions

Deployment Overview



Stottler Henke
Smarter Software Solutions

ARDA

Hypotheses

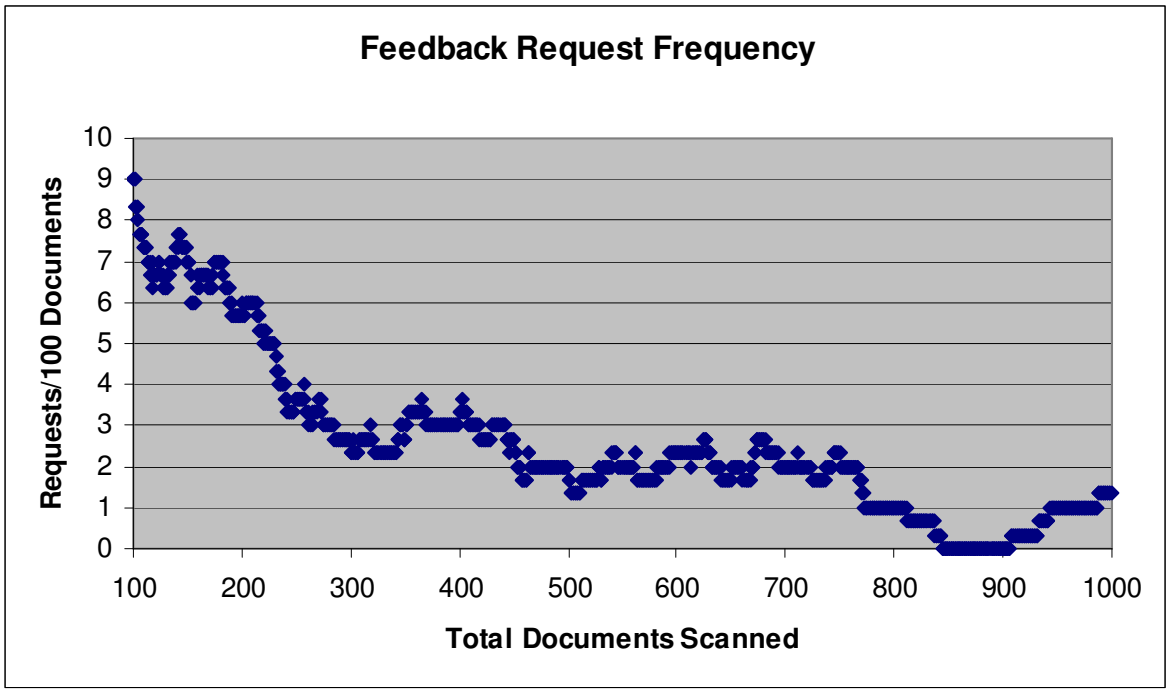
- High hit rate (~80%) on baseline task
- Low/decreasing false alarm rate (approach 0%)
- Can involve information authors (or authoring organizations) directly in detection
- Scales to realistic information environments
- Can detect non-cyber methods of unauthorized access

Baseline Experimental Setup

- Intellectual Property protection example
  - Restricted documents: 11 “Aware” proposals from 2002 & 2003
  - The Public documents: 15 proposals unrelated to Aware
  - Test documents:
    - 1 proposal taken from the Restricted Set
    - 3 Aware-related proposals from 2004
    - 1 non-Aware-related proposal from 2004 written by the researchers involved in Aware’s development
    - 39 proposals from 2002-2004 written by Stottler Henke researchers uninvolved with Aware
  - 3 runs of 1000 random samples from Test set

Experimental Results

- Experiment showed:
  - Good sensitivity (85.7% hit rate)
  - False positives (average 2.6, median of 1.67) decline as expected:



Stottler Henke
Smarter Software Solutions

Example Overlap Report

Aware, will be able to not only identify topically relevant material but also :::

to be consumed by time consuming :::

to guide the automated acquisition and filtering of mission critical :::

search the infosphere for relevant reports :::

establishing the utility of the retrieved reports to current I&W analyses :::

failures of query terms and phrases and term :::

analysis practical through text mining driven data acquisition and filtering :::

ARDA

Varying Experimental Settings

- Same data sets as experiment 1
- Swept variables 1 degree each way from experiment 1:
  - ***P*** = 125, 250, 375
  - ***N*** = 2, 3, 4
  - ***S*** = 4, 5, 6
- 3 runs of 1000 random samples per setting combination (for a total of 81 separate runs)

Stottler Henke
Smarter Software Solutions

Experimental Results 2

- More sampling improved hit rate and steepness of decline in false positives
- Longer strings lead to more hits, but benefits seem to taper off above length 5 (later tests cover length up to 8)
- Longer snippets decrease the rate at which we encounter false positives
- Hit rate peaked at 95%

Paraphrasing Experiment

- Gave 4 people 30 minutes to review and take notes on a restricted document (proposal)
- Subjects then wrote emails including key details
- Added the 4 paraphrase documents to the Test Set
- Ran 3 sets of 1000 samples for the settings:
  - ***P*** = 125, ***N*** = 4, ***S*** = 4, 5, 6

Paraphrasing Results

- Hit rates were lower for paraphrased documents, and varied from 18% to 78% across users
- Shorter snippet sizes were no better than longer
- Alignment of the beginning of a snippet is much more important in paraphrasing

ARDA

Future Work

- Testing new features
  - Content bearing long strings
  - Improbable collocations of short strings
- Tackling the intelligence “spillage” problem
- Testing paraphrasing of verbal presentations
- Developing sensors and infrastructure

Stottler Henke
Smarter Software Solutions

Summary

- SL-SAFE represents a scalable partial solution to the insider threat
- Simple mechanism – controlled by information owner
- Low and decreasing false alarm rates
- Supports “ad hoc” protection of documents
- Addresses (to a degree) human channels, flawed protection schemes…