Les Approximations Dangereuse: The Sorcerer's Apprentice and other Dangerous Approximations

Thursday, March 21, 2002

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 (718) 463 1079
gezelter@rlgsc.com
http://www.rlgsc.com

- What has four legs and fur?
- Please write down your answers

Statement

- “I do not leave people behind.”
- What does this mean? Write down your answer

What do your answers say?

- The statements are very incomplete
- Now let’s take a look at your answers

What has four legs and fur?

- child's perspective
- adult's perspective
- regional variations

“I do not leave people behind”

- Are you a military officer?
- Are you a drug lord?
- Who is listening to your answer?

Often, sayings and facts are incomplete, yielding a mental Rorshach test, which reveals more about prejudices and underlying beliefs than anything else.

Problem Summary

$$A \Rightarrow B \neq B \Rightarrow A$$

Misfiring Heuristics

- AOL – Harvard Early Action
- Packet Floods
- Relaying Email
- Personnel Information

AOL – Harvard Early Action

- “Early Action” letters
- identical text
- “.edu” domain
- mass recipients
- “obviously” SPAM

Discriminatory Effects

- email newsletters
- unpublished criteria
- SPAMMER labeling

Survellance and Data Gathering

- Admissibility
- Profiling
- difference between “meets pattern” and guilt
- presumptive scenarios

Presumptive Guilt

- “The Shopping Secretary”
- “The Business Traveler”

“The Shopping Secretary”

- large purchases
- unexplained cash deposits
- access to sensitive information
- Obviously Guilty — Right? Wrong!!

“The Business Traveler”

- Out of Town
- The Hotel
- The telephone call
- Woman 20 years younger
- Physical affection
- A compromising situation — Right? Wrong!!

Dangers –

- outside organizations
- gossip
- notification
- prosecution

Outside Organizations

- loss of control
- outside agendas and issues
- containment failure

Gossip – Information Distribution

- Gossip can be as damaging as prosecution
- Breach of confidentiality
- Job discrimination

Notification

- Collateral damage
- loss of control
- 2 + 2 = 17

Prosecution

- legal costs – all sides
- stopping is difficult
- may prejudice future cases

Failures of Planning

- Distributed Malaise
- Floods
- Loss of connectivity
- Cascades

Distributed Malaise

- AOL router update
- Email servers
- clogged senders
- no contingency plan
- no outside MX
- “A client SHOULD keep a list of hosts it cannot reach and corresponding connection timeouts, rather than just retrying queued mail items.” – RFC 2821 4.5.4.1

Floods

- Can be hostile
- Can be configuration errors
- Can be software/firmware bugs
- How do you tell the difference

Loss of Connectivity

- Email is delivered immediately – Right?
- Cell phones always work
- Email never disappears in transit

Cascades

- The AOL (America Offline) Incident
- Multiple errors are pervasive
- Many analyses are cursory at best
- Prepare to contain damage

How can we deal with this?

- Pride goeth before the fall.
  Understand your limits
- Rigorously check presumptions
- Think carefully!
- Measure twice – Cut once

Questions?

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America
+1 (718) 463 1079
gezelter@rlgsc.com
http://www.rlgsc.com

Session Notes & Materials:

http://www.rlgsc.com/e-protectit/2002/index.html