Network Radar: Update

Todd Heberlein

Net Squared, Inc.

18 July 2000

todd@NetSQ.com

Overview

- Repeating Content
  - Objectives
  - Practices
  - Technical approach
  - Status
- Network Radar Database
  - Objectives
  - Practices
  - Technical approach
  - Status
- Risks
- Technology Transition

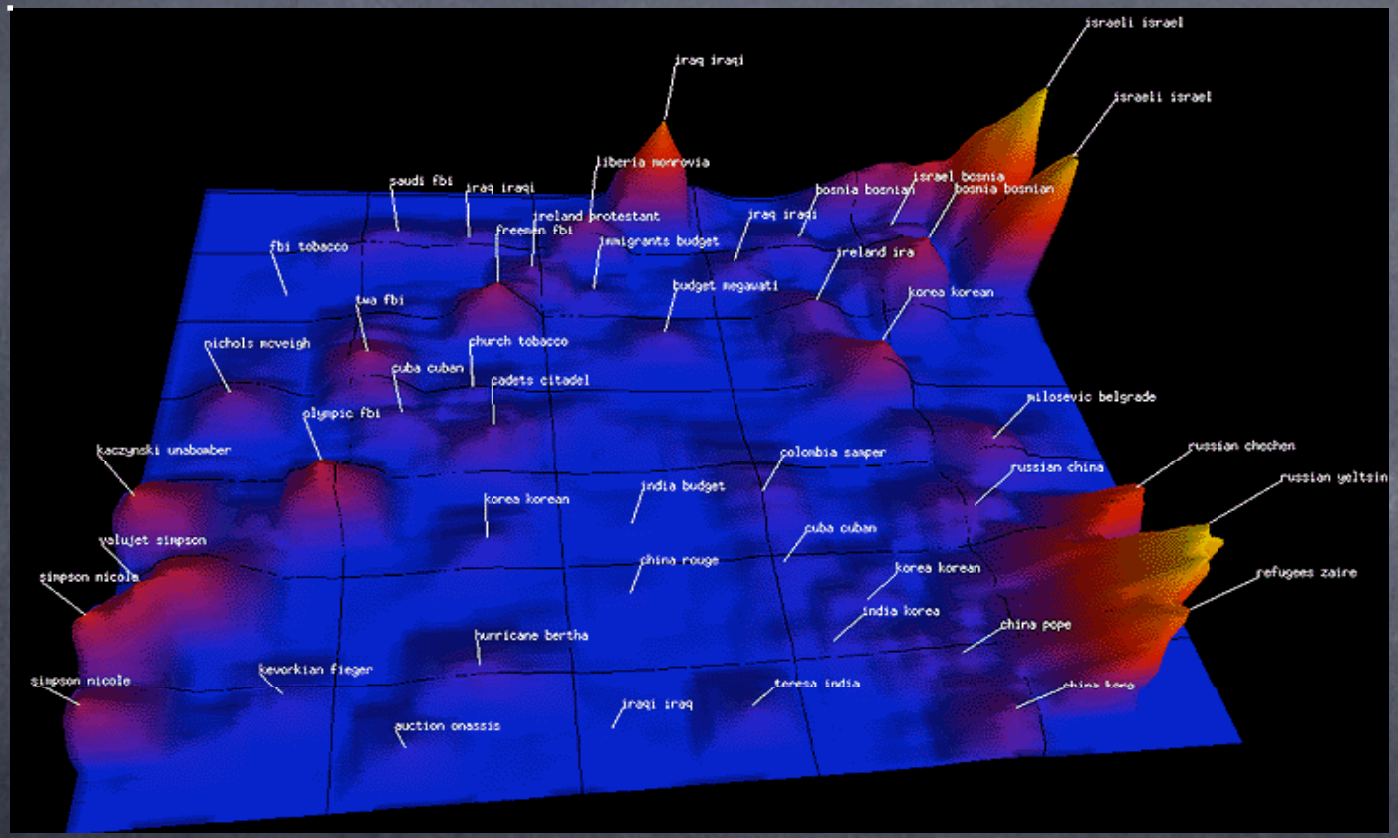
Repeating Content: Objective

- Identify repeating content.
  - Attackers "script" an attack and try it multiple times. The same content going to several web servers might indicate a new attack.
  - Worm carry essentially the same code from infection to infection.
  - Automatic signature (forwards and backwards in time).
- Detection needs to be robust against minor perturbations in content.

Existing Practice

- Largely not addressed in this problem space.
- Thumbprinting applied the technique for tracing hackers.
- Addressed in other information spaces, SPIRE, Themescape, Webscape.
- Large body of multivariate statistical analysis; principal component analysis.

PNNL's SPIRE


israeli israel
iraq iraqi
israeli israel
liberia monrovia
saudi fbi
iraq iraqi
israel bosnia
bosnia bosnian
bosnia bosnian
ireland protestant
iraq iraqi
freeman fbi
immigrants budget
fbi tobacco
ireland ira
budget megawati
korea korean
twa fbi
nichols mcveigh
church tobacco
cuba cuban
cadets citadel
olympic fbi
milosevic belgrade
kaczynski unabomber
colombia sanper
russian chechen
russian china
india budget
korea korean
russian yeltsin
valujet simpson
cuba cuban
china rouge
korea korean
simpson nicole
refugees zaire
india korea
china pope
hurricane bertha
kevorkian fieger
simpson nicole
teresa india
iraqi iraq
auction onassis

Cartia's Commercial Version

Technical Approach

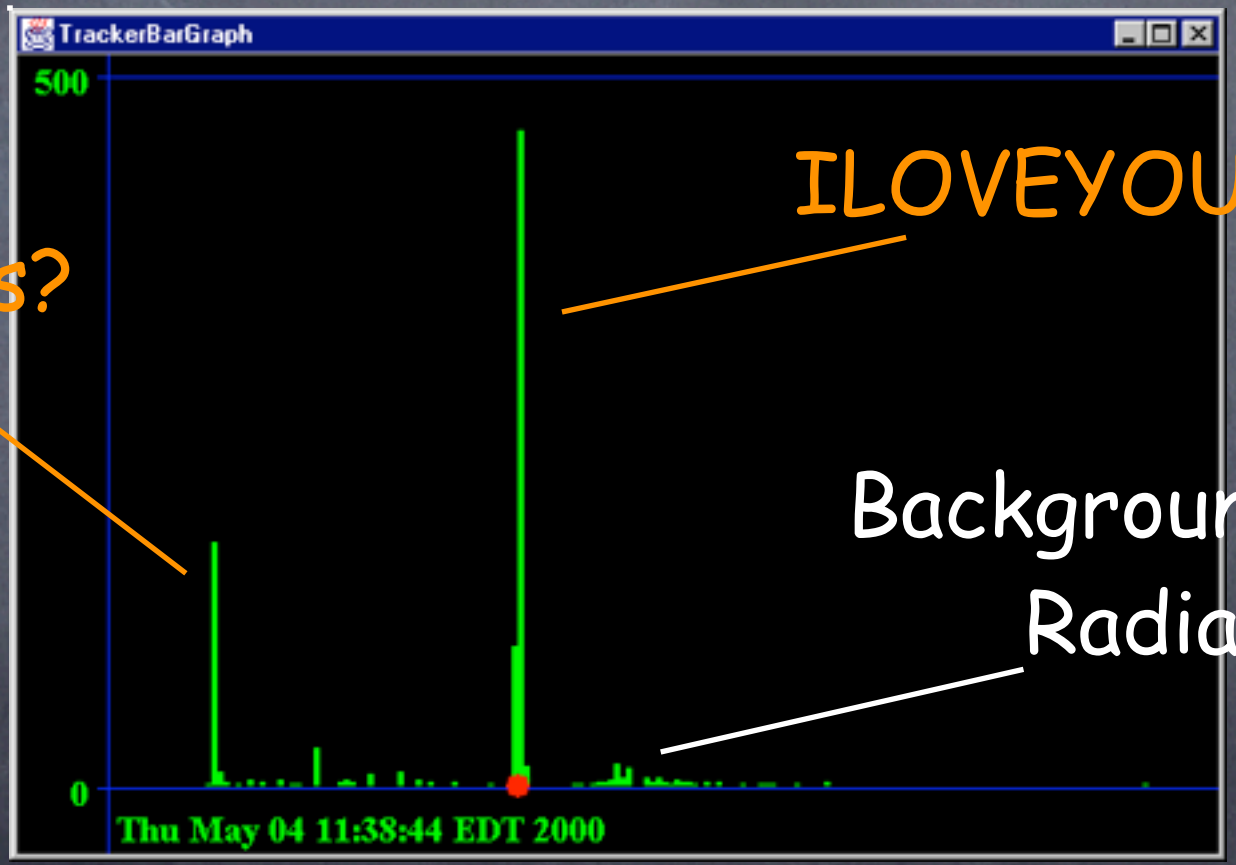
- Build mini-sensors for Network Radar.
- Reduce content to a single number or small set of numbers. Conceptually similar to checksums.
  - Rapidly compare numbers
  - Identify clusters of activity
- Apply principal component analysis (PCA) to optimize "robust checksum" generation keys.

Status

- Initial mini-sensors implemented in Network Radar.
  - Generic PcaStream.
  - WebPcaStream (optimized for web requests).
  - Generate numbers only; post mortem analysis tools needed to generate clusters or perform comparisons.
- Analyzed ILOVEYOU hitting Rome Labs.
- Needs more tuning.
- Need to address junk mail and mailing lists.

Rome: Morning E-Mails

Rome: ILOVEYOU Strikes



ILOVEYOU

What is this?

Different Mail encoding?

Background Worm Radiation