Network Discovery, Characterization, and Prediction: A Grand Challenge LDRD

Because our real adversaries are networks

LDRD
LABORATORY DIRECTED RESEARCH & DEVELOPMENT

Sandia National Laboratories
Bruce Hendrickson

The Network Threat

- Loose, dynamic groupings of often-unknown players
- Engaged in
  - terrorism, weapons proliferation, physical attacks, cyber-intrusions, IEDs and more
- Enabled by networks for
  - financing, supply, recruiting, shipment, communication, computing, etc.
- Information about these networks is buried in the terabytes of raw data that come in, every day, to multiple intelligence agencies

President Bush looks over a chart created with i2 software depicting Osama bin Laden's financial network during a tour of the Department of Treasury's Financial Crimes Enforcement Network in Vienna, Virginia, Wednesday, Nov. 7, 2001. (AP Photo/Doug Mills)

Discovery, Characterization, & Prediction

- **Vision: Defeat the network**
  - Enable analysts to discover, characterize, and understand adversarial networks buried in massive amounts of data.
  - Deliver orders of magnitude improvement in analysis capability.
  - Transform the way analysts and decision-makers address threats to national security
    - Use all the massive, diverse data that has been collected
    - Gain insight in time to do something about it
    - Make knowable, the unknown unknowns
- **Approach and Scope**
  - The analyst is pivotal — human creativity, insight, perspective and judgment are critical for the analysis process
  - Develop enabling, graph-based technologies, recognizing from the start, that we are dealing with graphs of unmanageable size
  - Leverage a close partnership between an analyst community with needs and a research community with significant capability
  - Focus on two domains
    - Proliferation analysis
    - Cyber-intrusion analysis
  - Research & develop a coordinated, iterative series of prototypes

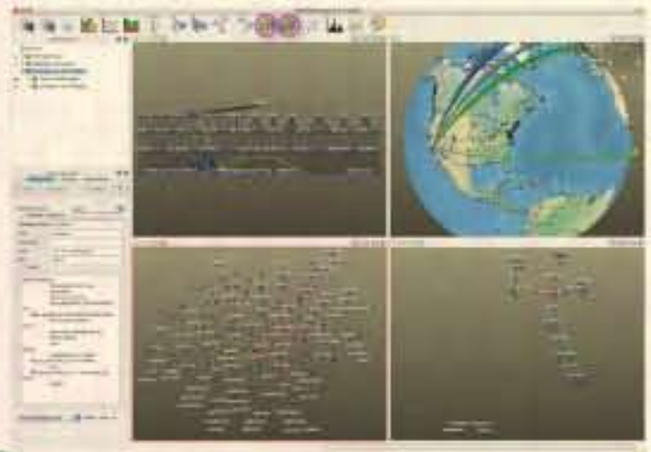
Sandia Has Unique Capabilities

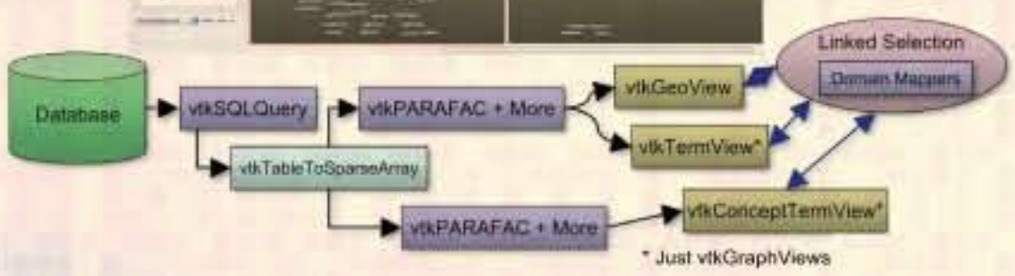
- **Specialized technology**
  - Information visualization
  - High-performance graph queries & algorithms
  - Advanced algebraic analysis algorithms
  - Network prediction & analysis
- **Organizational expertise**
  - High-performance computing
  - Technical intelligence analysis
  - Only DOE discrete math research department
  - Human factors
  - Data management
- **Strategic commitment to partnering**

Merge Advanced Sandia Capabilities

- Fast graph algorithms
  - Find subsets, patterns, trends in large data sets
- Algebraic methods
  - Rank importance, find missing relationships, dimensionality reduction, temporal analysis, trends
- Statistics and uncertainty
  - Characterize datasets, quantify anomalies, model and communicate uncertainty
- Advanced visualization
  - Communicate with user, facilitate exploration and serendipitous discovery
- Predictive modeling
  - Support interpretation, suggest likely evolution
- Integration
  - Titan framework, enable usability, interactivity at scale

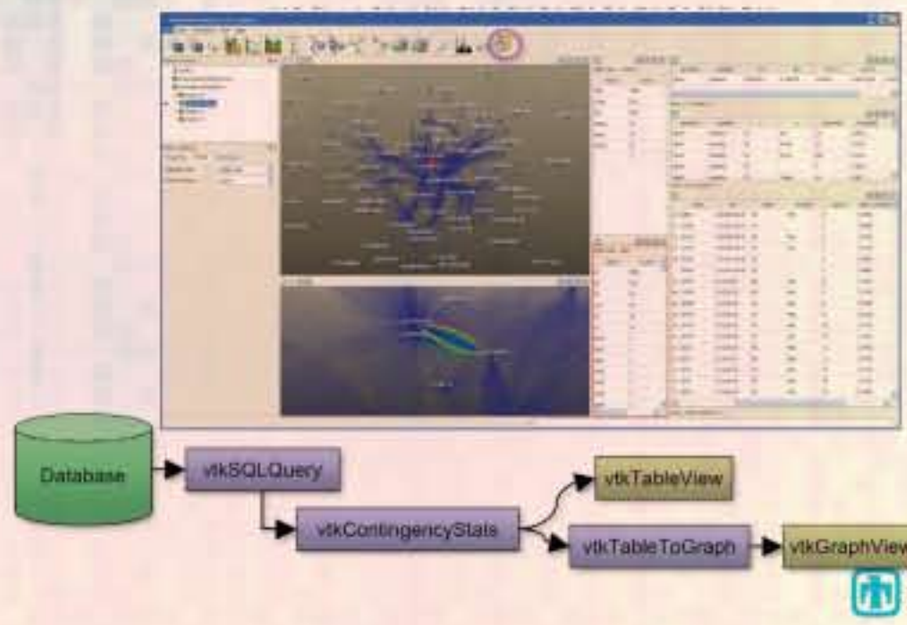
Cyber Analysis Prototype, Use Case: What "payloads" were exfiltrated?





Cyber Analysis Prototype: Use Case 4:

Analyst needs suspicious (out of the "norm") behaviors "flagged" for further exploration



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
SAND 2008-5471P CreativeArts 98429.LW3.08

National Nuclear Security Administration

Sandia National Laboratories