Insider Threat Mitigation Project

A Dynamic Network Approach

CMU-CS (and CASOS):
– Dr. Kathleen Carley
– Neal Altman
– Geoff Morgan
– Matt Benigni

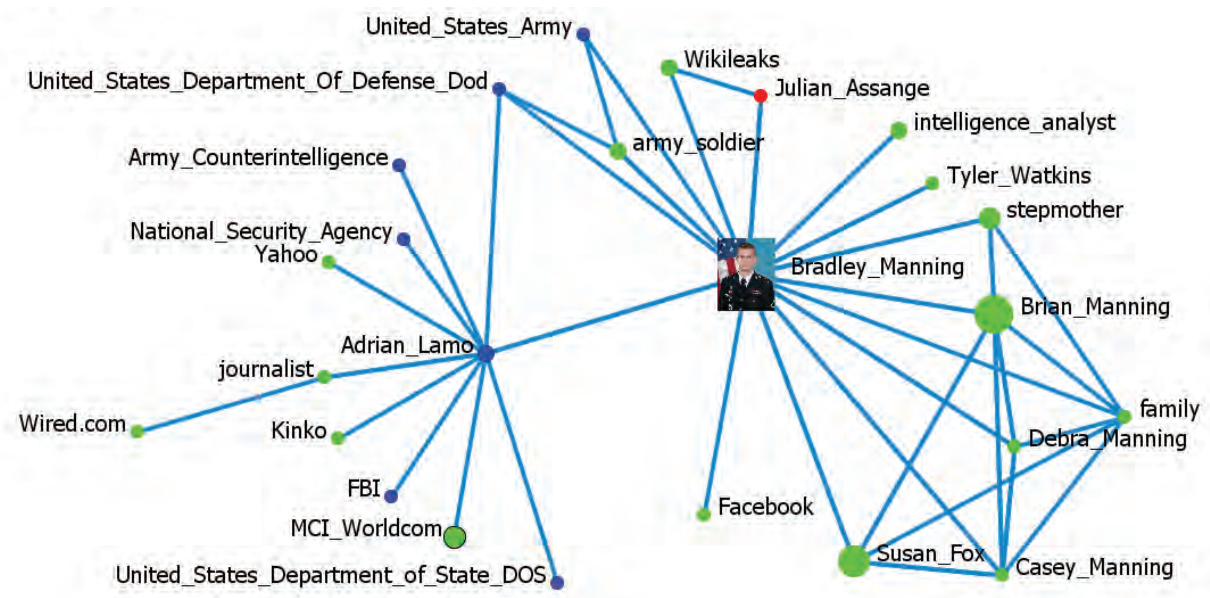
SEI:
– Matthew Collins
– Andrew Moore
– Dr. William Claycomb

Emergence of Threat – Ego centered analysis of specific cases

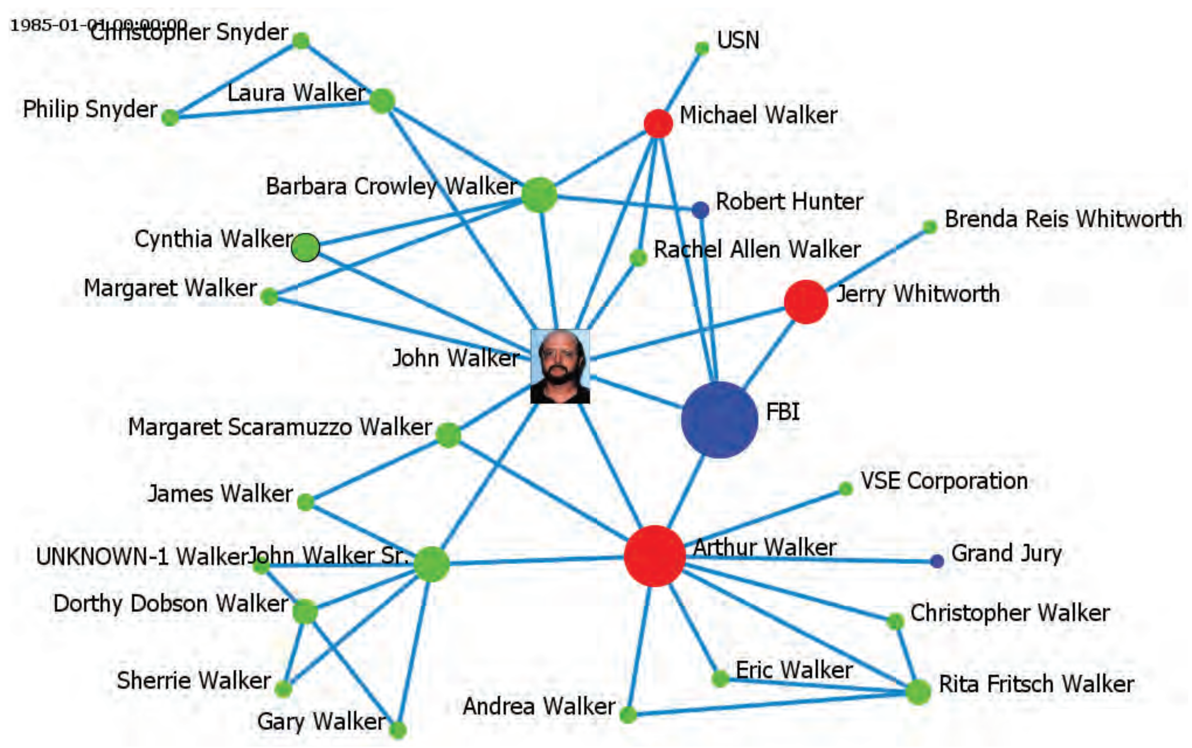
Approach:

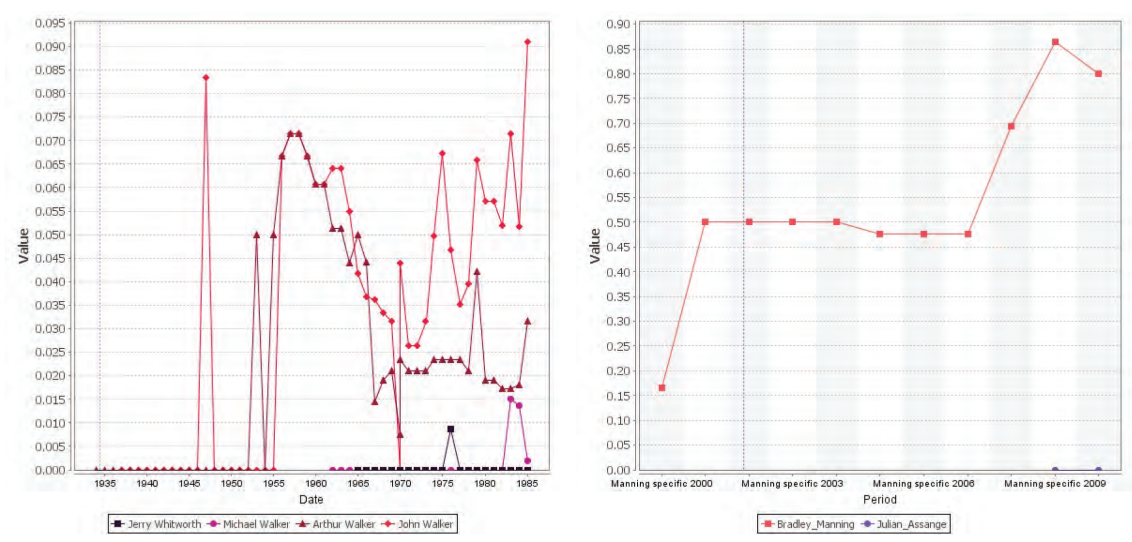
- Semi-automated coding with fine-tuning to add dates
- Extract meta-networks one per year
- Comparison at "role" level
- Apply network analytics and visualization

Manning – Lone Wolf
example open-source

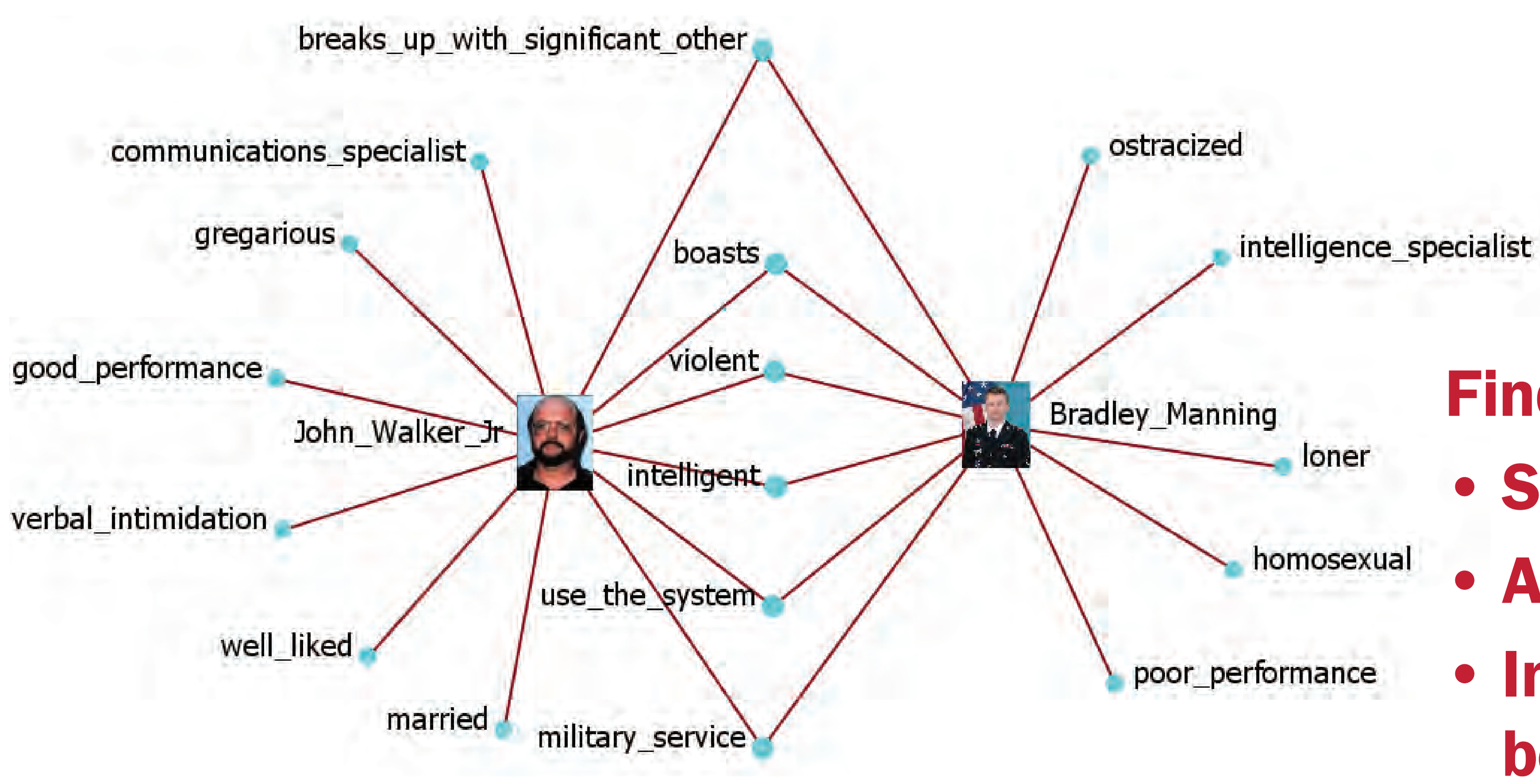


Walker – Gang example
Case records/searches
(open-source)





Increasing betweenness during spy activities



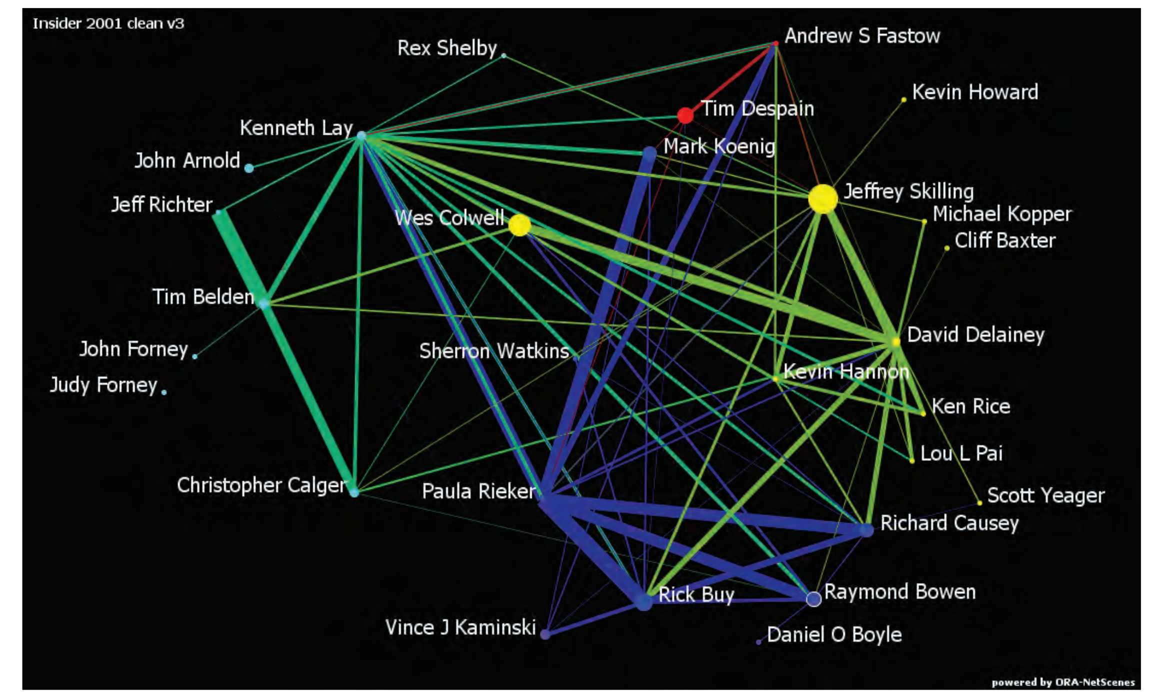
Findings on Insiders:

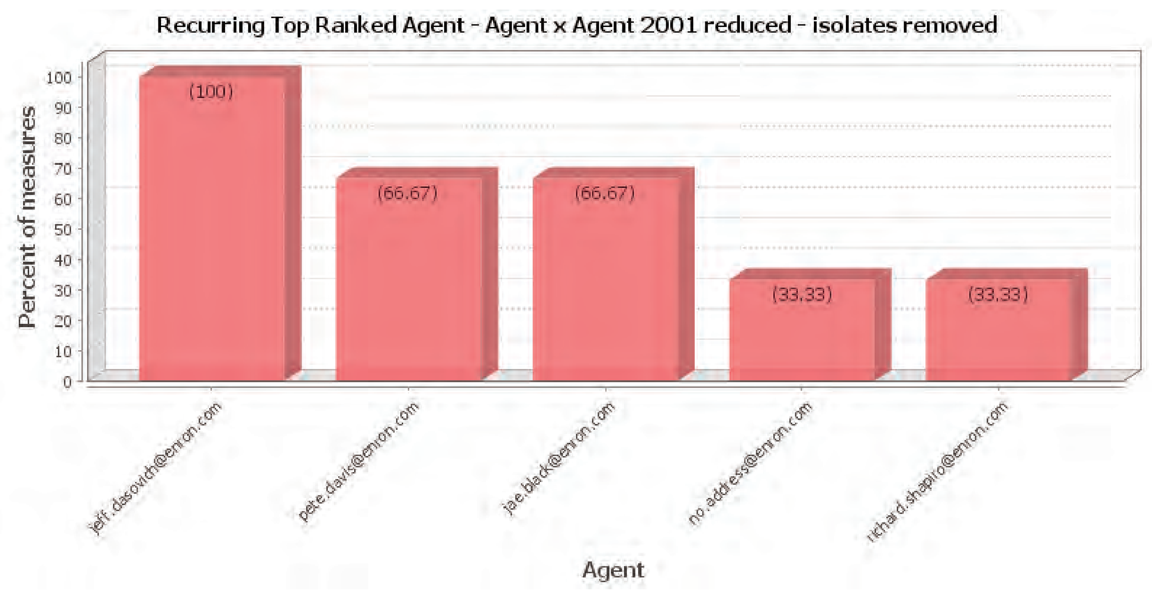
- **Special characteristics**
- **Access**
- **Increasing betweenness**
- **Disrupted family network**

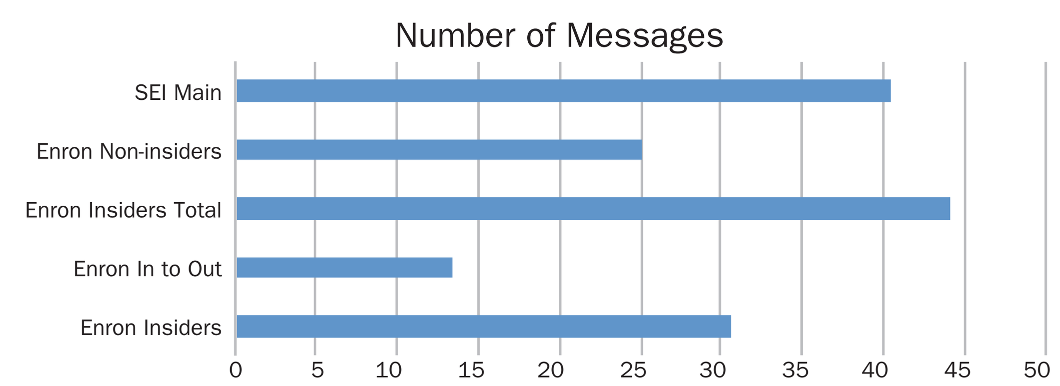
Emergence of Threat – Email centered analysis of possible anomalies

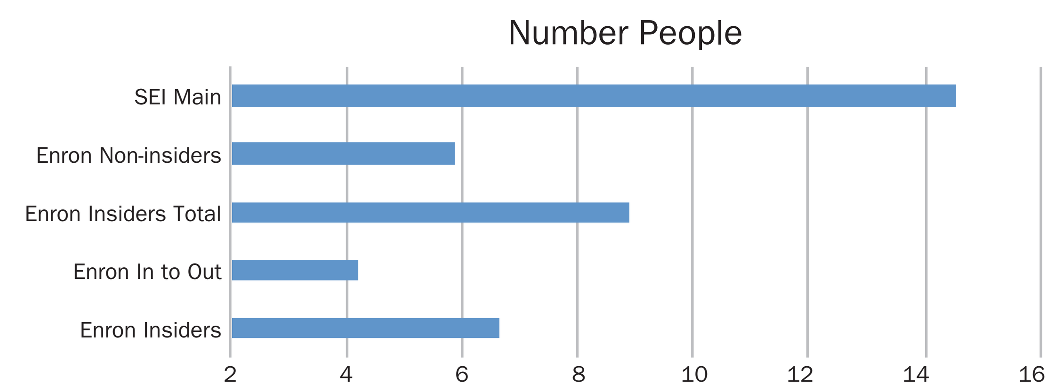
Approach:

- Networks formed from meta-data
- One network per year
- Segment internal from internal-to-external communication
- Remove suspected distribution lists
- Identify "normal behavior" using Enron
- Develop pattern for "insiders" in contrast to "normal" using Enron
- Apply to anonymized SEI email

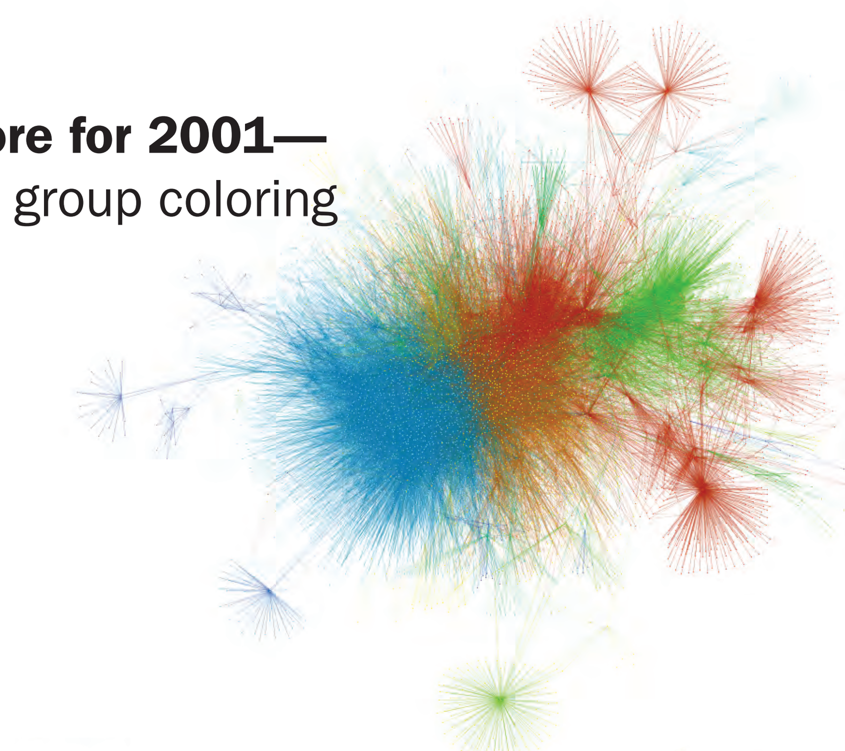








Enron core for 2001—
Newman group coloring



SEI core for 2013—
Newman group coloring

Findings on SEI -v- Enron:

- **SEI—more email, proportions similar**
- **Both—dominant dense core with numerous stars**

Findings on "Insiders"—those accused:

- **Are not "top" network actors**
- **Form a densely connected sub-group**
- **High level of in-group communication**
- **Low out-group communication**

Software Engineering Institute | Carnegie Mellon University

Center for Computational Analysis of Social and Organizational Systems

Contact: Andrew P. Moore apm@cert.org
Kathleen Carley kathleen.carley@cs.cmu.edu