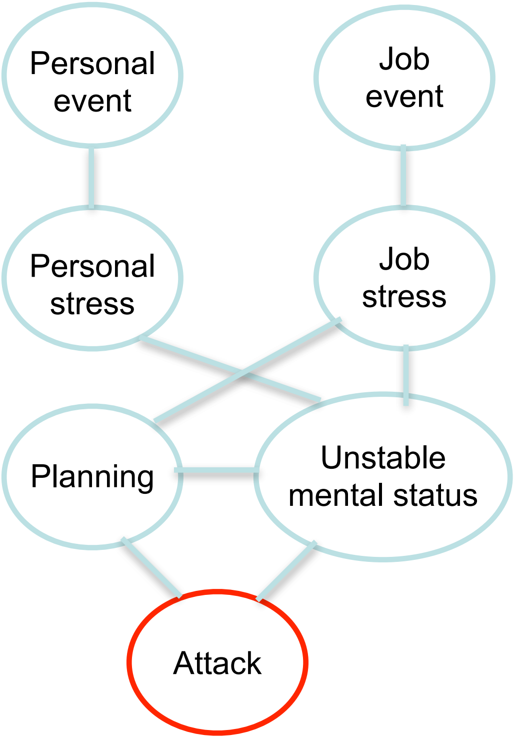
- Offerer Information
  - IBM T.J. Watson Research Lab
  - Ching-Yung Lin
  - Anni Coden, Sabrina Lin, Keith Houck
- Research Area of Interest
  - Social analysis
  - Multi-modality fusion
  - Behavior reasoning
  - Anomaly detection
  - Natural language processing

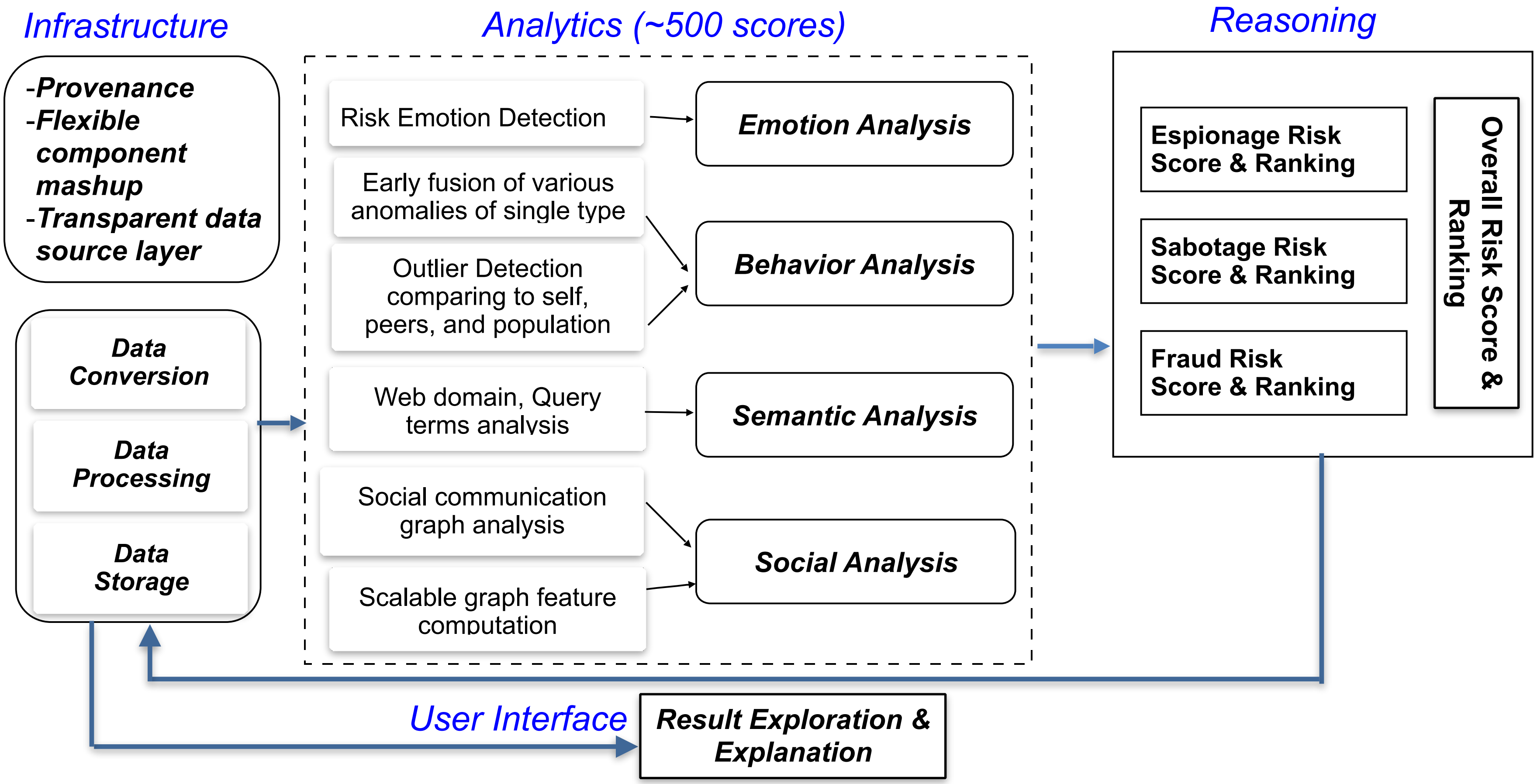
Qualifications and Capabilities

- Insider threat comes with a sequence of weak signals:
  - Example: Manning leaking classified information



- Personal stress
  - Gender identity confusion; termination of a stable relationship
- Job stress
  - Dissatisfaction with job roles, location, and work hours
- Unstable mental status
  - Fight with colleagues, emotional collapse in workspace, and large number of unhappy posts on social media
- Planning
  - Online chat with a hacker confiding his attempt of information leakage
- Attack
  - Download classified military documents and send to Wikileaks

Overview of Current Solution



Infrastructure

- ***Provenance***
- ***Flexible component mashup***
- ***Transparent data source layer***

Data Conversion

Data Processing

Data Storage

Analytics (~500 scores)

Risk Emotion Detection

Early fusion of various anomalies of single type

Outlier Detection comparing to self, peers, and population

Web domain, Query terms analysis

Social communication graph analysis

Scalable graph feature computation

Emotion Analysis

Behavior Analysis

Semantic Analysis

Social Analysis

Reasoning

Espionage Risk Score & Ranking

Sabotage Risk Score & Ranking

Fraud Risk Score & Ranking

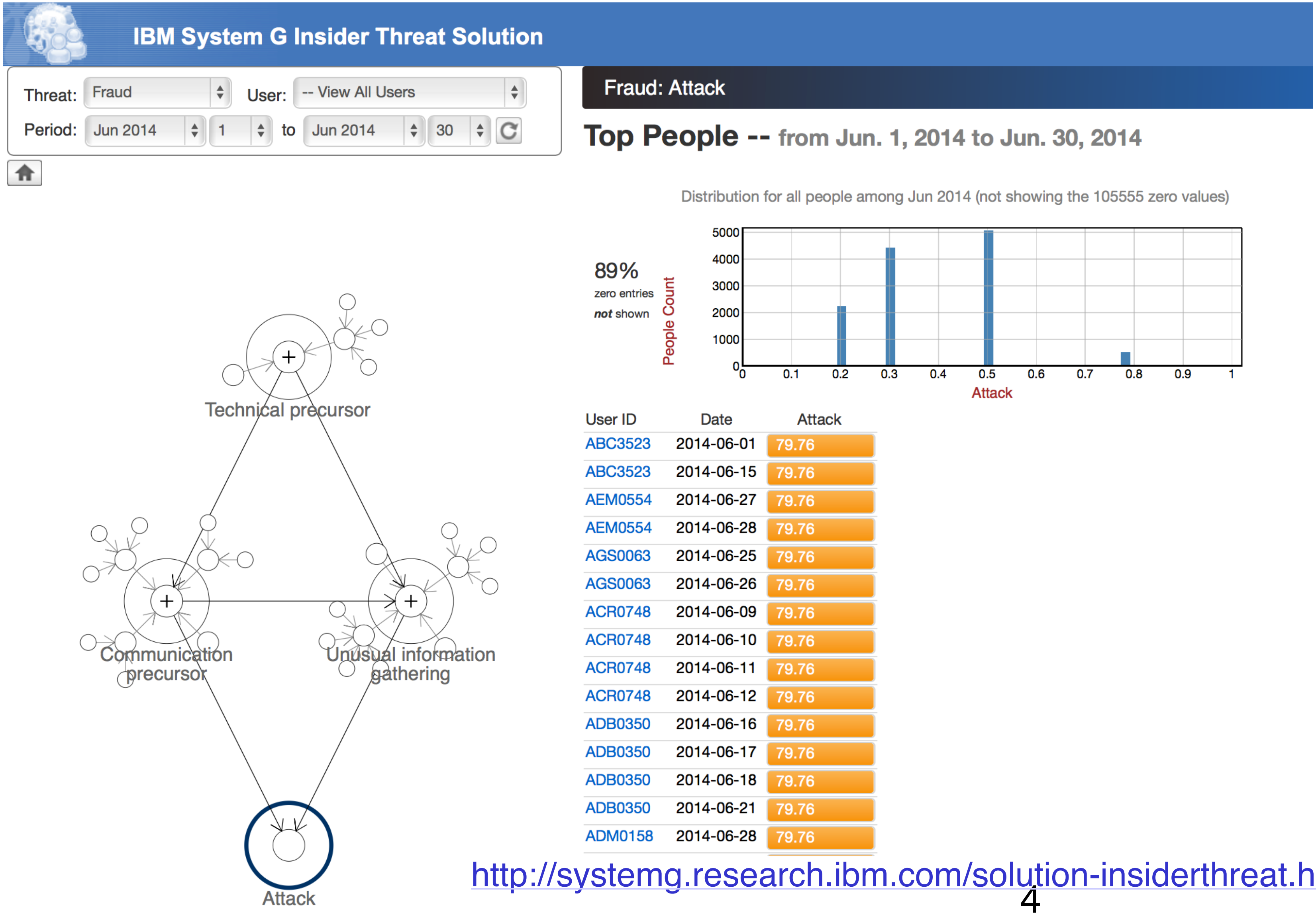
Overall Risk Score & Ranking

User Interface

Result Exploration & Explanation

- Performance of our solution
  - Evaluation data: anomalous activity data inserted by a third party into activity streams of 5500 people on their PCs
  - Results: out of 52 inserted activity scenarios (Apr. 13 to Oct. 14), 46 (88%) in top 1% of people, 6 (12%) in top 4% of people

User Interface



IBM System G Insider Threat Solution

Threat: Fraud User: -- View All Users

Period: Jun 2014 1 to Jun 2014 30

Fraud: Attack

Top People -- from Jun. 1, 2014 to Jun. 30, 2014

Distribution for all people among Jun 2014 (not showing the 105555 zero values)

User ID	Date	Attack
ABC3523	2014-06-01	79.76
ABC3523	2014-06-15	79.76
AEM0554	2014-06-27	79.76
AEM0554	2014-06-28	79.76
AGS0063	2014-06-25	79.76
AGS0063	2014-06-26	79.76
ACR0748	2014-06-09	79.76
ACR0748	2014-06-10	79.76
ACR0748	2014-06-11	79.76
ACR0748	2014-06-12	79.76
ADB0350	2014-06-16	79.76
ADB0350	2014-06-17	79.76
ADB0350	2014-06-18	79.76
ADB0350	2014-06-21	79.76
ADM0158	2014-06-28	79.76

http://systemg.research.ibm.com/solution-insiderthreat.html

- Capabilities We Seek
    - Data collection and curation
    - Collaboration on testing procedures
    - Collaboration on inference enterprise models
- Contact Information
    - Ching-Yung Lin
    - IBM Distinguished Researcher & Chief Scientist, Graph Computing Research
    - IBM T.J. Watson Research Center
    - chingyung@us.ibm.com
    - 914-945-1987
    - http://systemg.research.ibm.com