

Detecting Insider Threat Behavior

Gregory D. Stephens

703-983-3242 • stephens@mitre.org

MITRE Sponsored Research

The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow, orange, and blue to the left of the text.

MITRE
Technology
Program

The MITRE logo, consisting of the word "MITRE" in a bold, black, sans-serif font.

MITRE

Problem

- **Trusted insiders committing espionage have caused tremendous damage to U.S. national security.**
- **Sensitive U.S. information is vulnerable to insider misuse.**
 - **More information to protect than ever**
 - **Need to know impossible to enforce**
 - **Post 9/11 drive to share across boundaries**
- **Effective mechanisms to detect information misuse do not exist.**

Background

■ Observation #1

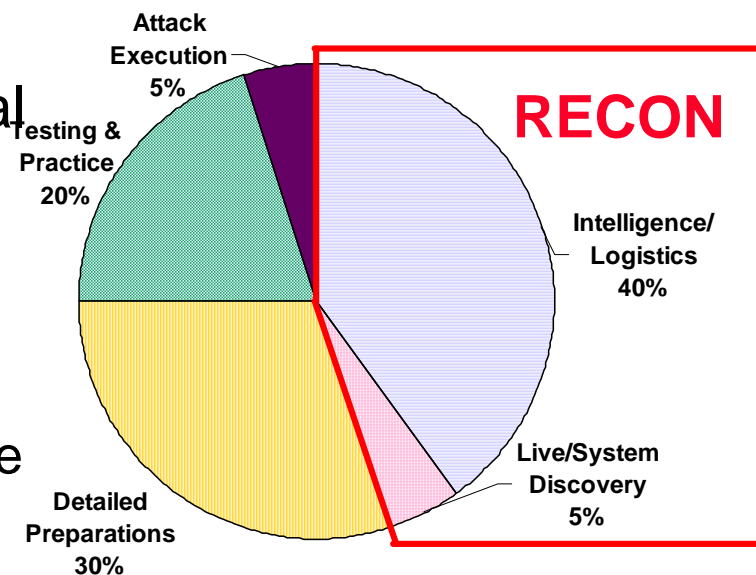
Reconnaissance is an essential step for the malicious insider.

- National Intelligence Council Cyber Threat Estimate
- Red team activity analysis
- MITRE operational experience

■ Observation #2

Need context to differentiate reconnaissance from legitimate information use

- Organizational (formal, relatively static)
 - e.g., organizational structure, user directory information
- Behavioral (informal, relatively dynamic)
 - e.g., communities of interest



2000 Insider Threat Workshop Proceedings

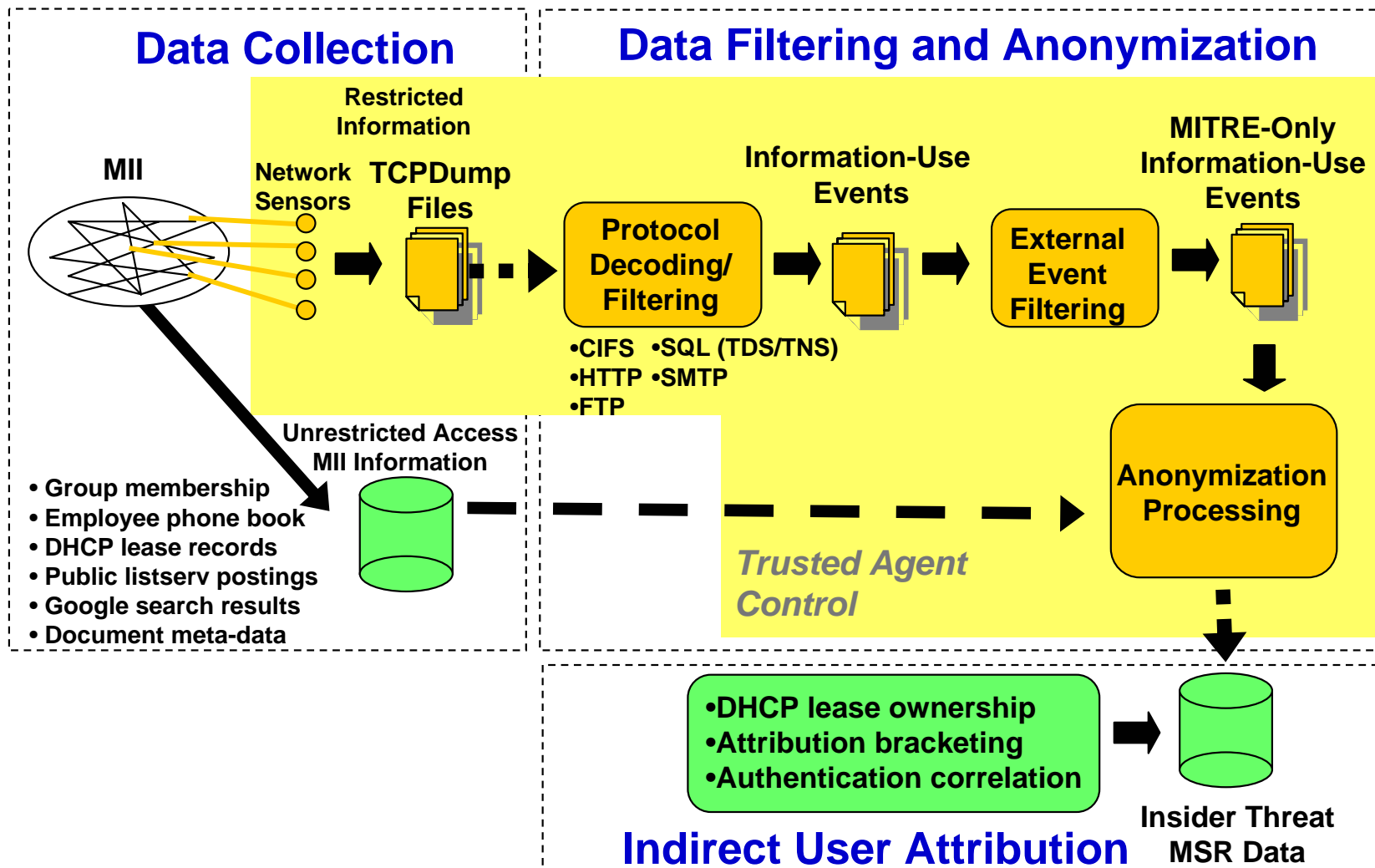
Objective

- **Develop sensors to collect data streams closely tied to information use; attribute to users**
- **Build information context from available sources**
- **Develop context-sensitive rules that identify insider reconnaissance**
 - **FY04: Heuristic-based**
 - **FY05/FY06: Learned**

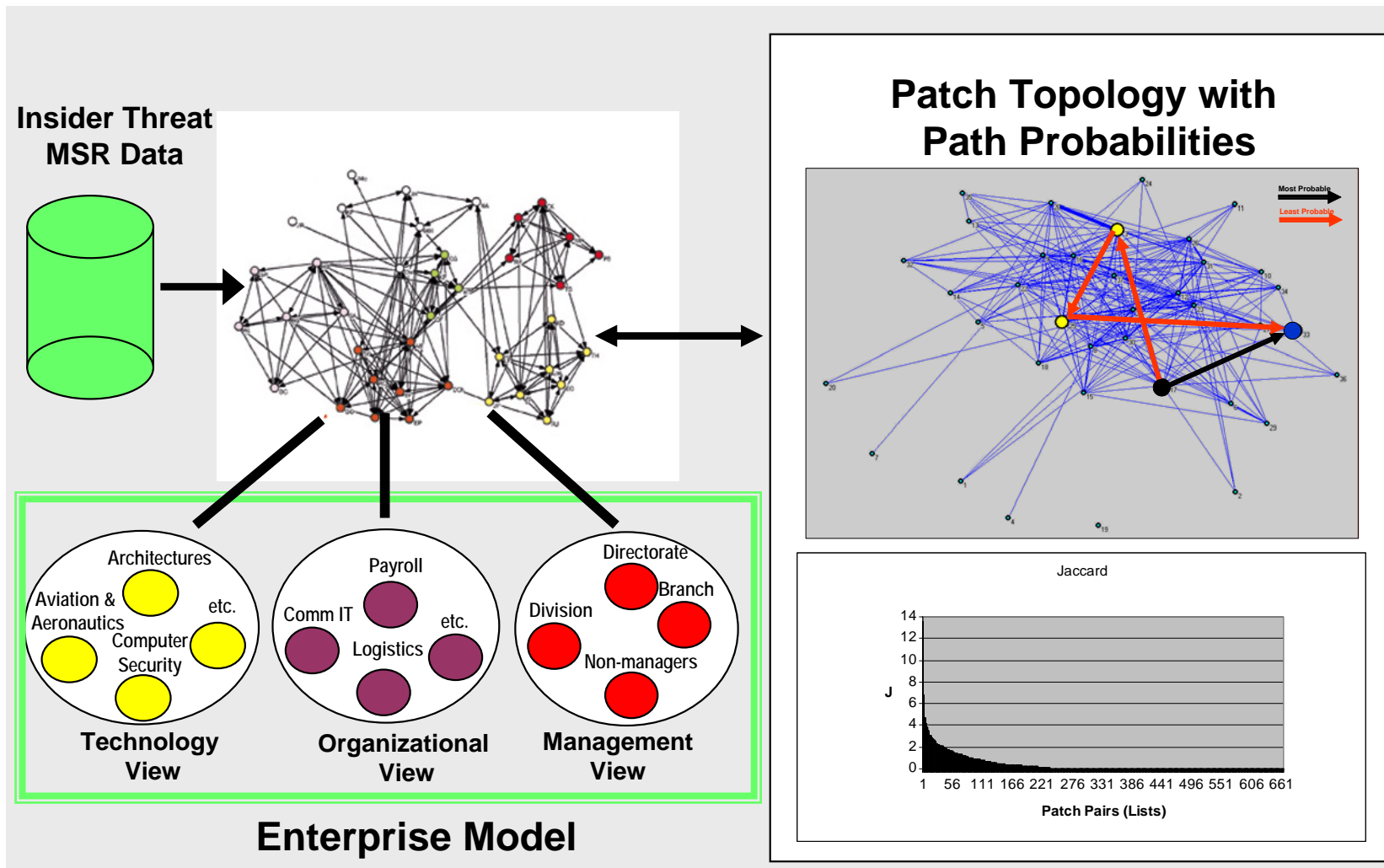
Activities

- **Data collection architecture development**
 - **Information use/context sources**
 - **User attribution**
 - **User privacy protection**
 - **Data protection CONOPS**
 - **Data scrubber architecture**
- **Context space (patch) modeling**
 - **Subject and object attributes**
 - **Patch membership**
 - **Patch similarity (landscape)**
 - **Information access → patch traversal**

Highlight



Highlight

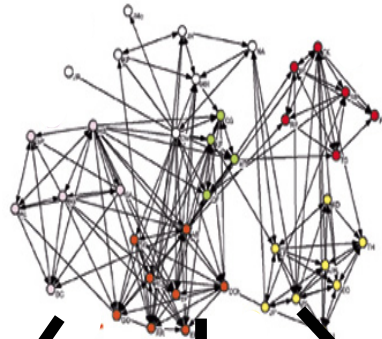
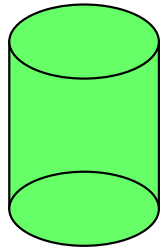


Impacts

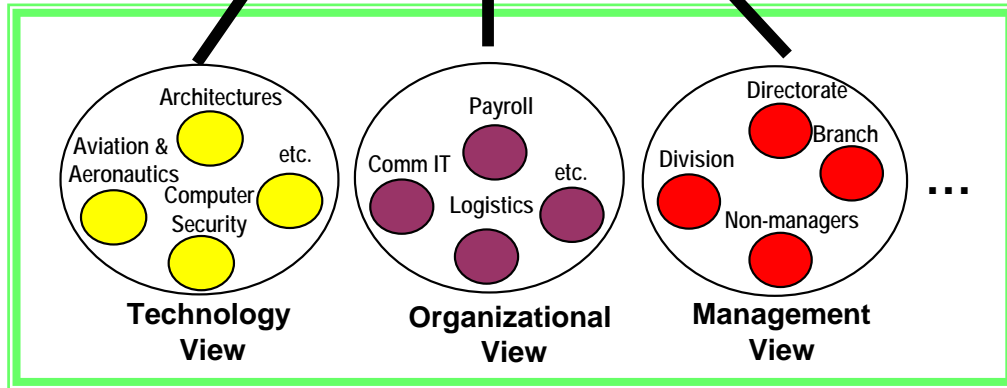
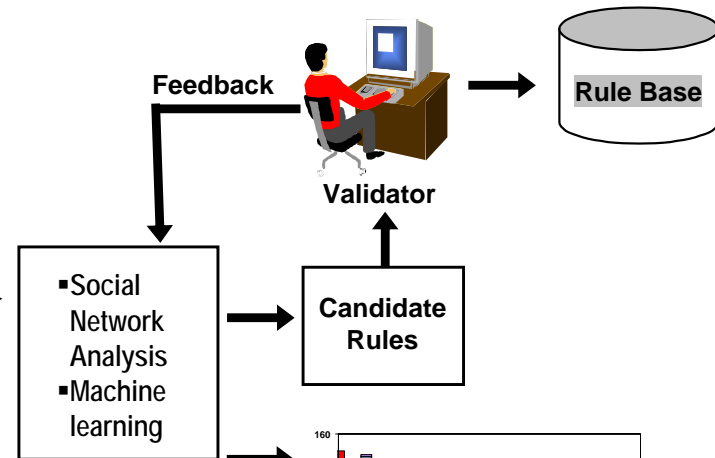
- **Demonstrate that insiders can be detected BEFORE they damage U.S. national security**
- **Transition technology to MITRE sponsor base**
- **Enable increased information sharing**
 - **Share but monitor for abuse**

Future Plans

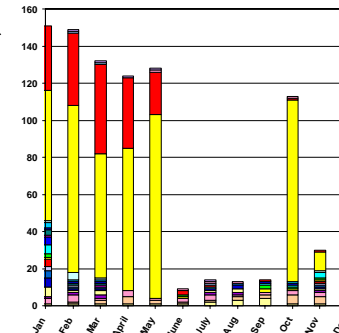
Insider Threat
MSR Data



Learned Rule Development



Enterprise Model



Information Use Profiling