

Detecting Insider Threat Behavior

Greg Stephens

703.983.3242 •
gstephens@mitre.org

MSR

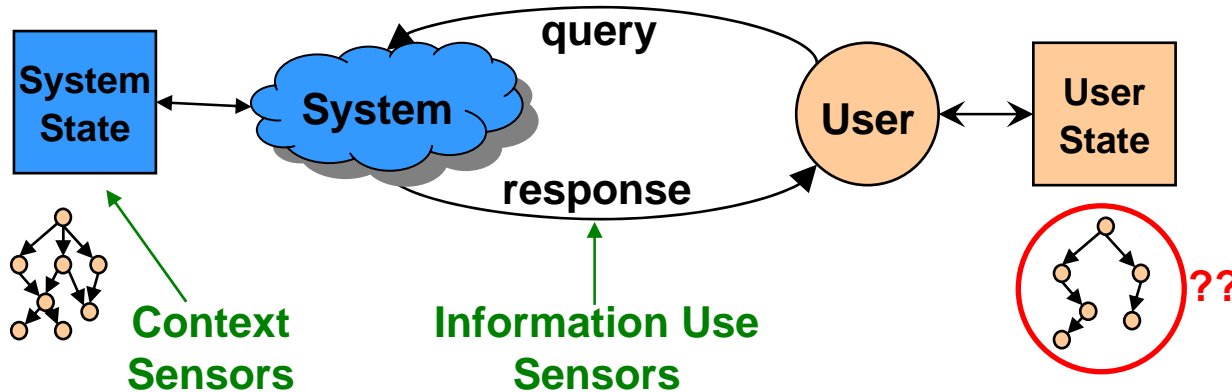
 MITRE
Technology
Program

Problem

- **Trusted insiders committing espionage have caused tremendous damage to U.S. national security**
- **Sensitive U.S. information is vulnerable to misuse**
 - **More information to protect than ever**
 - **Need to know difficult to enforce**
 - **Post 9/11 drive to share across boundaries**
- **Effective information misuse detection mechanisms do not exist**
 - **Focused on detecting rule-breaking**
 - **Malicious insiders can engage in espionage without tripping current sensors**

Background

Information gathering is an essential step for the malicious insider



Need context to differentiate legitimate from malicious information use

Objective

Detect when trusted insiders misuse information in a manner consistent with espionage

- Develop passive, network-based sensors that monitor how users interact with information
- Attribute observed activity to users
- Collect context on users and information
- Develop a broad set of context-sensitive rules that highlight potentially abusive behavior
- Fuse individual indicators into overall threat scores

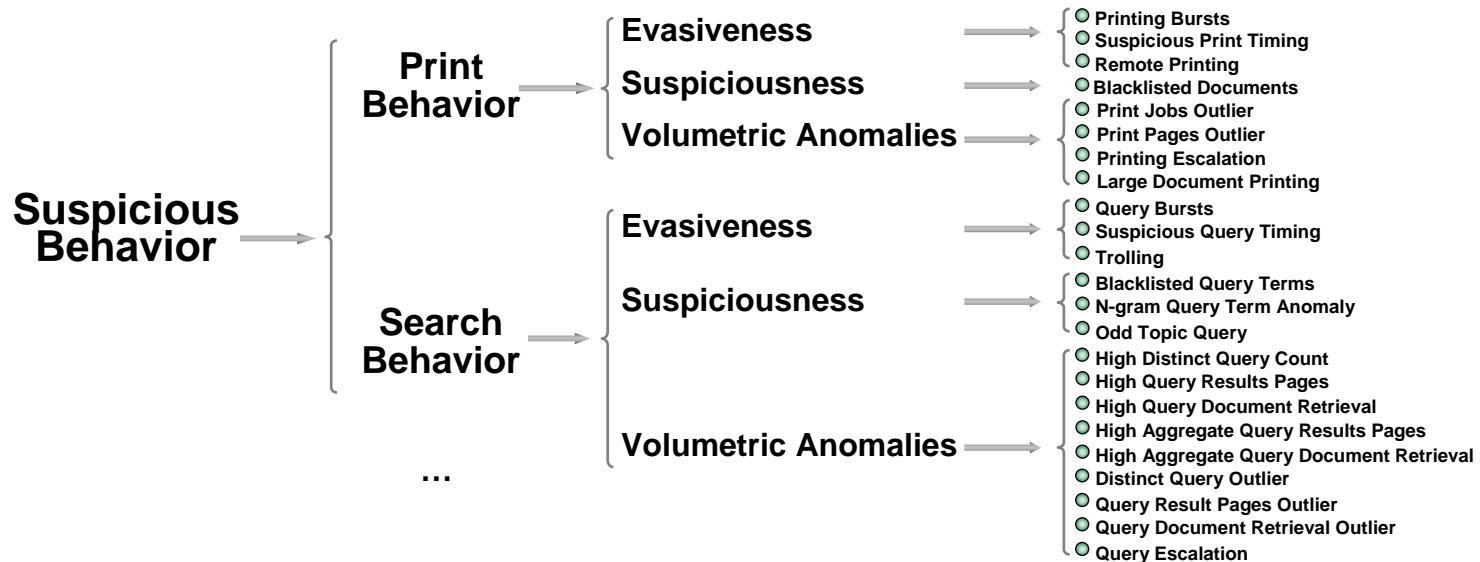
Activities

- **Built information use sensors and user attribution algorithms**
- **Collected, processed, and anonymized large real-world data set**
- **Executed many malicious insider scenarios**
- **Developed broad set of information misuse detectors**
- **Developed indicator fusion framework**
- **Built information misuse detection prototype**
- **Tested prototype against data sets**

Highlight

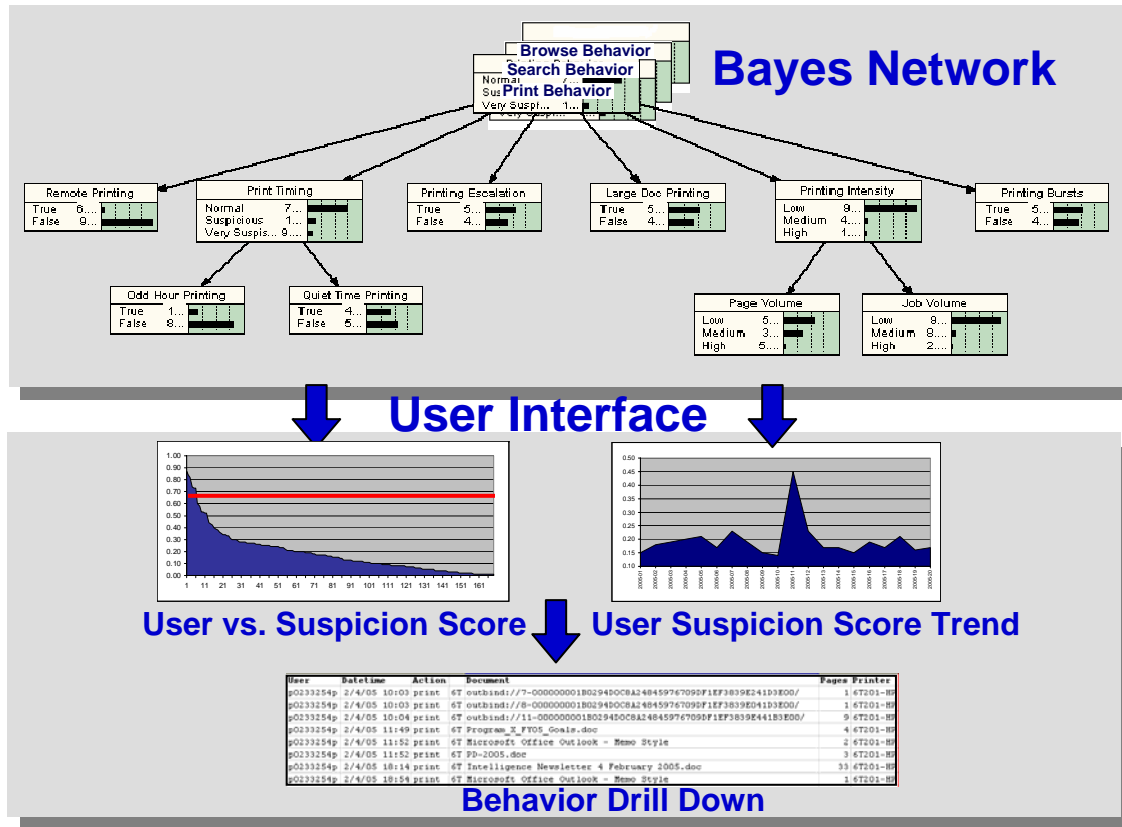
Detector Hierarchy

- Focuses on aspects that maximize discrimination between innocuous and malicious users
- Detects diversity of behaviors so that malicious insiders cannot achieve objective without detection



Demonstration

Malicious Insider Detection Using Research Prototype, Exploit Latent Information To Counter Insider Threats (ELICIT)



Impacts

- **Demonstrate that insiders can be detected BEFORE they damage U.S. national security**
- **Transition technology to MITRE sponsor base**
- **Develop sharable reference data set for insider threat research community**
- **Enable increased information sharing**
 - **Share but monitor for abuse**

Future Plans

Refine ELICIT prototype and investigate other applications

