Monitoring Database Management System (DBMS) Activity for Detecting Data Exfiltration by Insiders

Northrop Grumman Information Systems
Donald Steiner, PhD

17 September 2013
Team Profile

- **Northrop Grumman**: (Virginia) 68,000 employees, 50 States
  - Information Systems Sector → Cyber Solutions Division → Civil Systems Business Unit
    - Focus on Cyber Security, Emergency Management
  - **Dr. Donald Steiner**, Principal Technologist and Technical Fellow
    - PhD Mathematics, Iowa State University
    - Data Management & Analytics, Cybersecurity, Cloud Computing
    - Manager Northrop Grumman Cybersecurity Research Consortium
    - 20 years applied research & development in Artificial Intelligence, Multi-Agent Systems

- **Purdue University**: (Indiana) 3,000 staff, 39,000 Students
  - Center for Education and Research in Information Assurance and Security (CERIAS): 81 faculty led by Dr. Eugene Spafford
  - **Prof. Elisa Bertino**, Director of Research at CERIAS
    - Fellow of the IEEE and Fellow of ACM
    - Distinguished awards for contributions to database systems, database security, advanced data management systems, and secure distributed systems.
    - Relevant publications
Customer Need

• DBMS = ?
  – Database Management System OR …
  – Detect Behavior by Manning and Snowden

• Data Exfiltration = Unauthorized removal of data from the enterprise
  – Lots of ways this can happen (humans and software)

• Goal: Detect and alert on data exfiltration attempts as early as possible
  – Before the horse leaves the barn
Approach

• Monitor user interaction with database systems for anomalous behavior
  – Most data on databases, file systems, etc.
  – Equally applicable to other data storage systems (Hadoop, …) and applications accessing such systems
  – Not local applications (Excel, Access, …)

• Project Flow (over 3 years)
  – Core research at Purdue University → Proof of Concepts
  – Transition at Northrop Grumman → Prototypes, Evaluation
    • Evaluation & Testing through Red-Team/Blue-Team
  – Operational Pilot at TBD
Benefits

• Detection and alerting in **real-time**
  – Immediate intervention if necessary
• **Low-cost** integration with existing infrastructure
Competition (optional)

• Improvement to:
  – Existing database monitoring systems
  – User monitoring systems
  – Network monitoring systems
  – Computer monitoring systems
Current Status

• Just started (5 business days ago)
  – Getting project up and running
Next Steps

- Requirements
  - Conceptual / Research
  - Development / Deployment
  - Testing
- Research
  - Assumption: Exfiltration causes an anomalous state that can be distinguished from the legitimate actions executed in a DBMS system.
  - Identify the events that represent signs of cyber-insider actions:
    - “How do we define and identify user queries that are anomalous?”
    - “Which data sources does an insider target?”
    - “What information should be collected to detect such actions?”
  - Build accurate DBMS access profiles
    - Use Role Based Access Control (RBAC) model
  - Detect Anomalous User Behavior
  - Detect Anomalous Events
    - Build repository of relevant DBMS log & SQL events
    - Analyze the events and detect anomalous events that raise alarm flags
Contact Information

- Donald Steiner, PhD
  Principal Technologist and Technical Fellow
  Northrop Grumman Information Systems
  7575 Colshire Dr., McLean, VA 22102
  donald.steiner@ngc.com ; (703)556-2115

- Professor Elisa Bertino
  Purdue University
  305 N. University Street, West Lafayette, IN 47907
  bertino@cs.purdue.edu ; (765)496-2399