PURDUE UNIVERSITY

Cybersecurity for Product Lifecycle Management
A Research Roadmap

Elisa Bertino

CS Department, Cyber Center, and CERIAS

Purdue University

PLM Fellow

CERIAS®

PURDUE UNIVERSITY

Why is Security Challenging in PLM?

- PLM is a complex environment
- PLM involves many different users, with different roles, possibly located in different countries
- PLM is knowledge-intensive, collaboration-intensive, and competitive

PURDUE UNIVERSITY

Research Agenda for PLM Security

Critical requirements: need to address all problems you have in most enterprises +

- Protection from Insider Threat
- Compliance with Export Regulations
- Secure Supply Chain
- Secure Remote 3D Printing
- Security for Industrial Control Systems
- Secure Collaboration Techniques
- Security for Legacy Equipment

Research directions:

- Anomaly Detection Systems and Advanced Access Control Systems
- Security Techniques for Embedded Systems, Firmware, and IoT
- Security for Industrial Cyber-Physical Systems and Industrial Processes
- Secure Collaboration Platforms
- Tools for Compliance Support

E. Bertino, N. Hartman, “Cybersecurity for PLM – A Research Roadmap”, IEEE Intelligence and Security Informatics (ISI), May 2015, Baltimore May 2015.

PURDUE UNIVERSITY

Insider Threat in Manufacturing

PURDUE UNIVERSITY

Definitions

The President's National Infrastructure Advisory Council defines the insider threat as follows:

> "The insider threat to critical infrastructure is one or more individuals with the access or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm."
>
> "A person who takes advantage of access or inside knowledge in such a manner commonly is referred to as a "malicious insider.""

Definitions from FEMA – Emergency Management Institute
http://www.training.fema.gov/emi.aspx

PURDUE UNIVERSITY

The Scope of Insider Threats

Insider threats can be accomplished through either physical or cyber means and may involve any of the following:

Threat	Involves
Physical or information-technology sabotage	Modification or damage to an organization's facilities, property, assets, inventory, or systems with the purpose of harming or threatening harm to an individual, the organization, or the organization's operations
Theft of intellectual property	Removal or transfer of an organization's intellectual property outside the organization through physical or electronic means (also known as economic espionage)
Theft or economic fraud	Acquisition of an organization's financial or other assets through theft or fraud
National security espionage	Obtaining information or assets with a potential impact on national security through clandestine activities

PURDUE UNIVERSITY

Examples of Actual Incidents

Sector	Incidents
Chemical	**Theft of intellectual property.** A senior research and development associate at a chemical manufacturer conspired with multiple outsiders to steal proprietary product information and chemical formulas using a USB drive to download information from a secure server for the benefit of a foreign organization. The conspirator received $170,000 over a period of 7 years from the foreign organization.
Critical Manufacturing	**Physical sabotage.** A disgruntled employee entered a manufacturing warehouse after duty hours and destroyed more than a million dollars of equipment and inventory.
Defense Industrial Base	**National security threats.** Two individuals, working as defense contractors and holding U.S. Government security clearances, were convicted of spying for a foreign government. For over 20 years, they stole trade and military secrets, including information on advanced military technologies. **Information-technology sabotage.** A system administrator served as a subcontractor for a defense contract company. After being terminated, the system administrator accessed the system and important system files, causing the system to crash and denying access to over 700 employees.

PURDUE UNIVERSITY

Organizational Factors that Embolden Malicious Insiders

Access and Availability	• **Ease of access to materials and information** • **Ability to exit the facility or network with materials or information**
Policies and Procedures	• **Undefined or inadequate policies and procedures** • **Inadequate labeling** • **Lack of Training**
Time Pressure and Consequences	• **Rushed employees** • **Perception of lack of consequences**

PURDUE UNIVERSITY

DBSafe
An Anomaly Detection System for Relational Databases

PURDUE UNIVERSITY

The Insider Threat – Why it is so Dangerous

- Insiders know where the data is and probably know how to access it.
- Outsiders probably don't know as much about what is stored in which systems. This creates a window of opportunity to detect the intrusion while the outsider is feeling his way around
  - "Feeling your way around" is actually a pattern we can search for
- Insiders may be able to disguise their activities within normal day to day activities
- Requirement
  - We cannot make life difficult for users who are just doing their jobs.

PURDUE UNIVERSITY

Guiding Recommendation

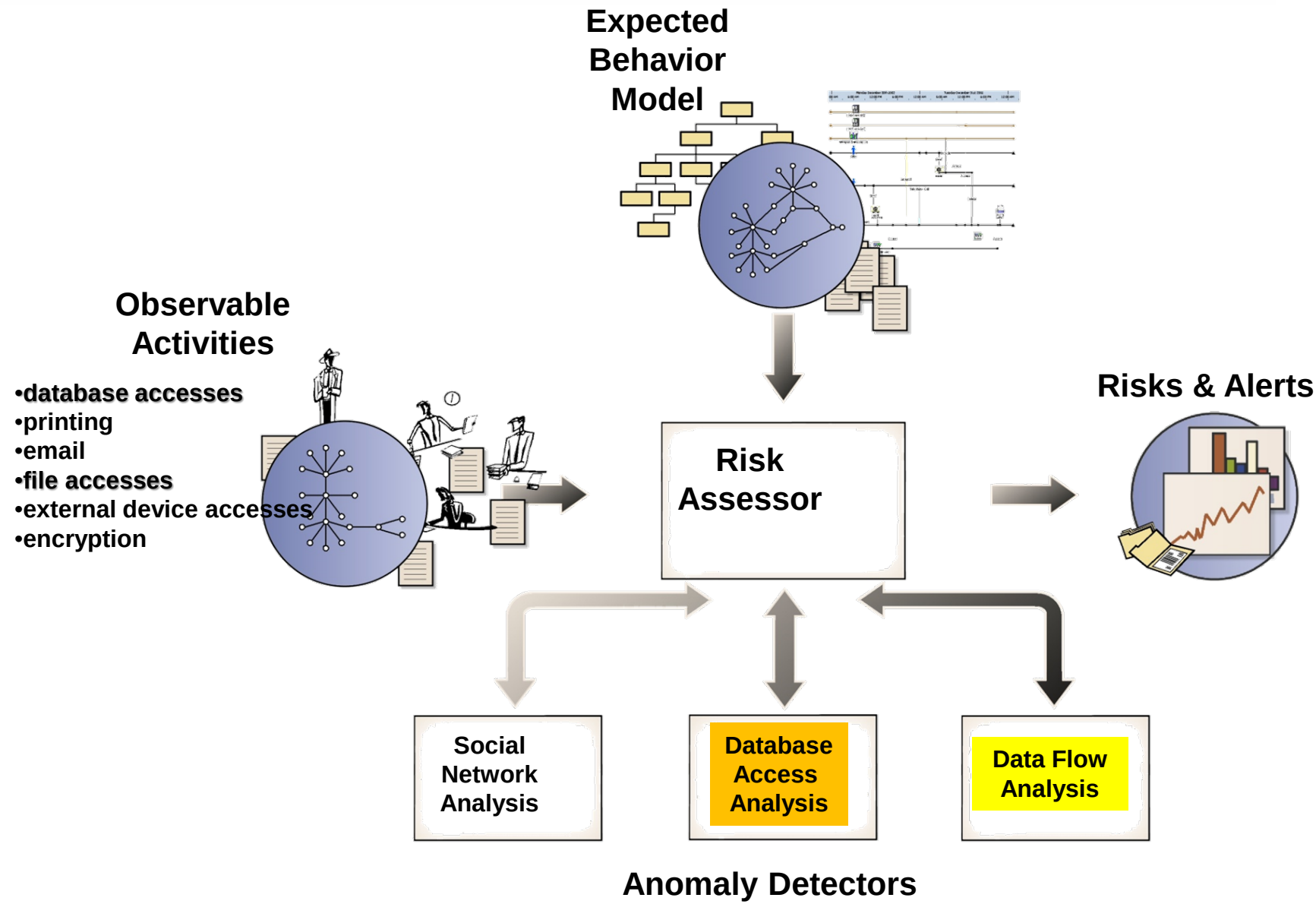
From "*Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments or Organizations*", CMU/SEI, May 2013

- **Recommdendation3:**

Monitor Intellectual Property Leaving the Network

- **Identify critical information and track its location, access, modification, and transfers**
- **Implement technical controls that log the access and movement of critical information that employees**
  - **Download from company servers**
  - **Email from the organization's network to personal accounts**
  - **Download to removable media**
- **Many cases involved downloading source code, executables, or excessive amount of data before leaving the organization**

Our Guiding Idea



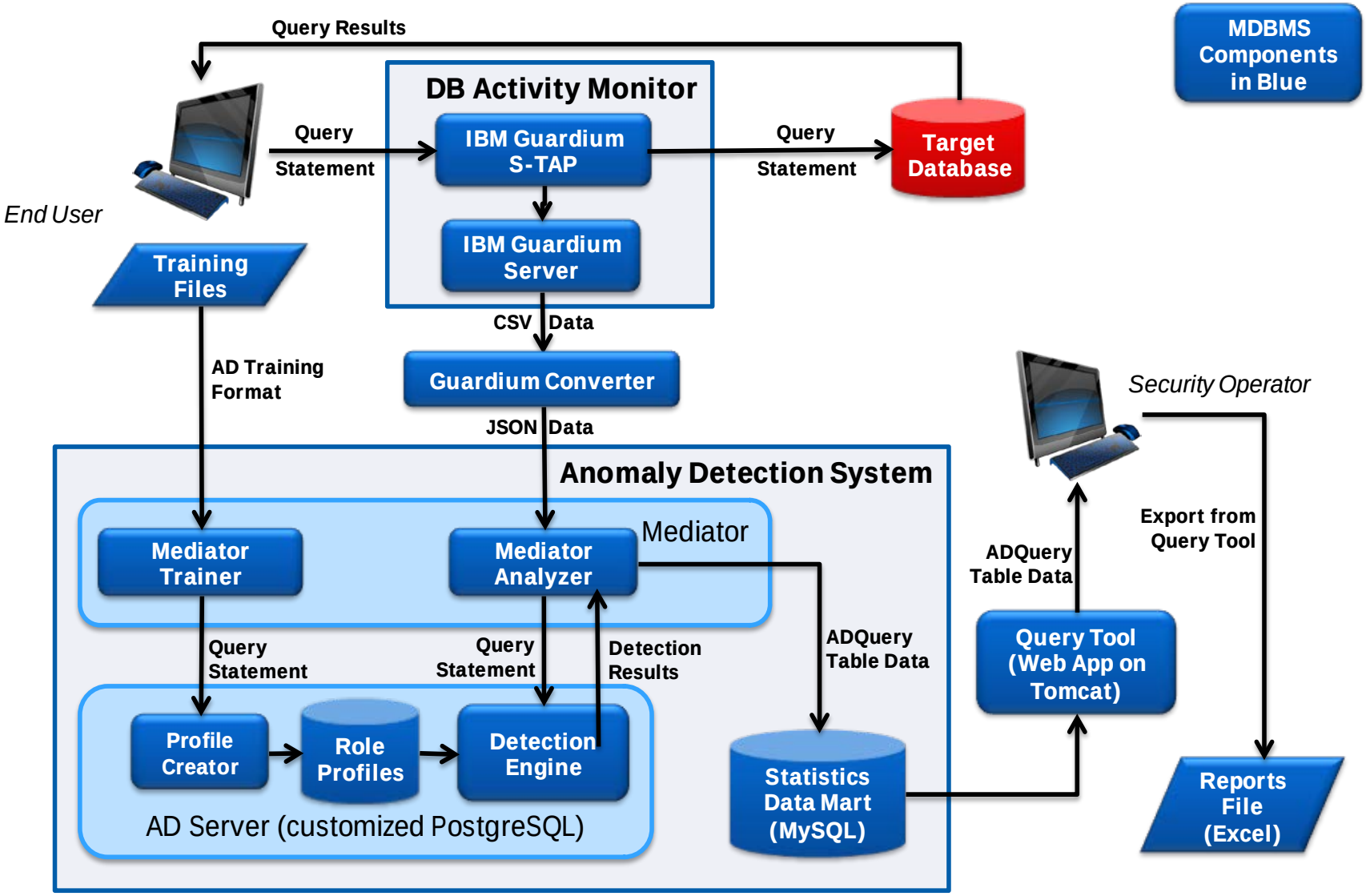
PURDUE UNIVERSITY

Approach

- RBAC-administered databases
  - ❑ Access permissions are associated with roles
  - ❑ Users are assigned to roles
- Goal: Detect anomalous database accesses by roles
- Strategy:
  - ❑ Build profiles of normal role behavior
    - o Mine database traces stored in log files
    - o Extract access pattern from queries acquired during a "Training Phase"
    - o Create profiles of roles from queries submitted by users
  - ❑ Use these profiles to detect anomalous behavior (Detection Phase)

PURDUE UNIVERSITY

System Architecture



The Classifier

- Creating Profiles ≡ Training the classifier
- "Classification is the problem of identifying to which of a set of categories a new observation belongs, on the basis of a training set of data containing observations"
- We use the NBC (Naïve Bayes Classifier) with the MAP (Max-Aposteriori Probability) decision rule
- Given an input query →

  Identify which role (most probably) this query came from →

  Compare it with the actual role of the user submitting the query
- *Recent progresses*
  - Developed and integrated into the system multi-label classification techniques
  - Developed and integrated into the system clustering techniques in order to support the case in which roles are not used

PURDUE UNIVERSITY

Further Research Challenges In Anomaly Detection for PLM

- How to represent the typical accesses to data managed by non-relational data management system (e.g. file systems)
- How to track, represent, and monitor data flow in a PLM system
- How to capture, represent, and monitor use of data by PLM users
- How to reduce false positives

PURDUE UNIVERSITY

IoT Security

PURDUE UNIVERSITY

IoT - Risks

IoT dramatically expands the attack surface

- **IoT systems do not have well defined perimeters**
- **IoT systems are highly dynamic and continuously evolve because of mobility**
- **IoT are highly heterogeneous with respect to:**
  - ❑ **Communication**
  - ❑ **Platform**
  - ❑ **Devices**
- **IoT systems may include physically unprotected portions**
- **IoT systems may include “objects” not designed to be connected to the Internet**

PURDUE UNIVERSITY

IoT - Risks

The OWASP Internet of Things Top 10 - 2014

1. **Insecure Web Interface**
2. **Insufficient Authentication/Authorization**
3. **Insecure Network Services**
4. **Lack of Transport Encryption**
5. **Privacy Concerns**
6. **Insecure Cloud Interfaces**
7. **Insecure Mobile Interfaces**
8. **Insufficient Security Configurability**
9. **Insecure Software/Firmware**
10. **Poor Physical Security**

Summary of Projects

- **Encryption Protocols**
  - **Key management schemes for small devices**
    - *Team members:* Anes Seo (Korea U.), Jongho Won, Elisa Bertino
  - **Hardware Accelerated Authentication for Vehicular Networks**
    - *Team members:* Anand Mudgerikar, Ankush Singla, Attila Yavuz, Ioannis Papapanagiotu, Elisa Bertino
- **Software Security**
  - **Techniques for static and dynamic analysis for nesC memory safety for embedded systems**
    - *Team members:* Daniele Midi, Mathias Payer, Elisa Bertino
  - **Techniques to prevent RoP and code injection attacks on Raspberry Pi devices**
    - *Team members*: Javid Habibi, Ajay Panicker, Aditi Gupta, Elisa Bertino
- **Network Security**
  - **Denial of service attacks on IoT routers and defense techniques**
    - *Team members:* Javid Habibi, Daniele Midi, Elisa Bertino
  - **Fine-grained diagnosis for data packet losses in sensor networks**
    - *Team members:* Daniele Midi, Elisa Bertino

PURDUE UNIVERSITY

Further Research

- Development of case studies data security in smart manufacturing

PURDUE UNIVERSITY

Thank You!

- *Questions?*
- Elisa Bertino bertino@purdue.edu