Developing and Validating Statistical Cyber Defenses

IEEE Software Technology Conference
April 10 2013

Michael Jay Mayhew (AFRL)
Michael Atighetchi (BBN)
Rachel Greenstadt (Drexel University)
Aaron Adler (BBN)

Raytheon BBN Technologies

Drexel UNIVERSITY

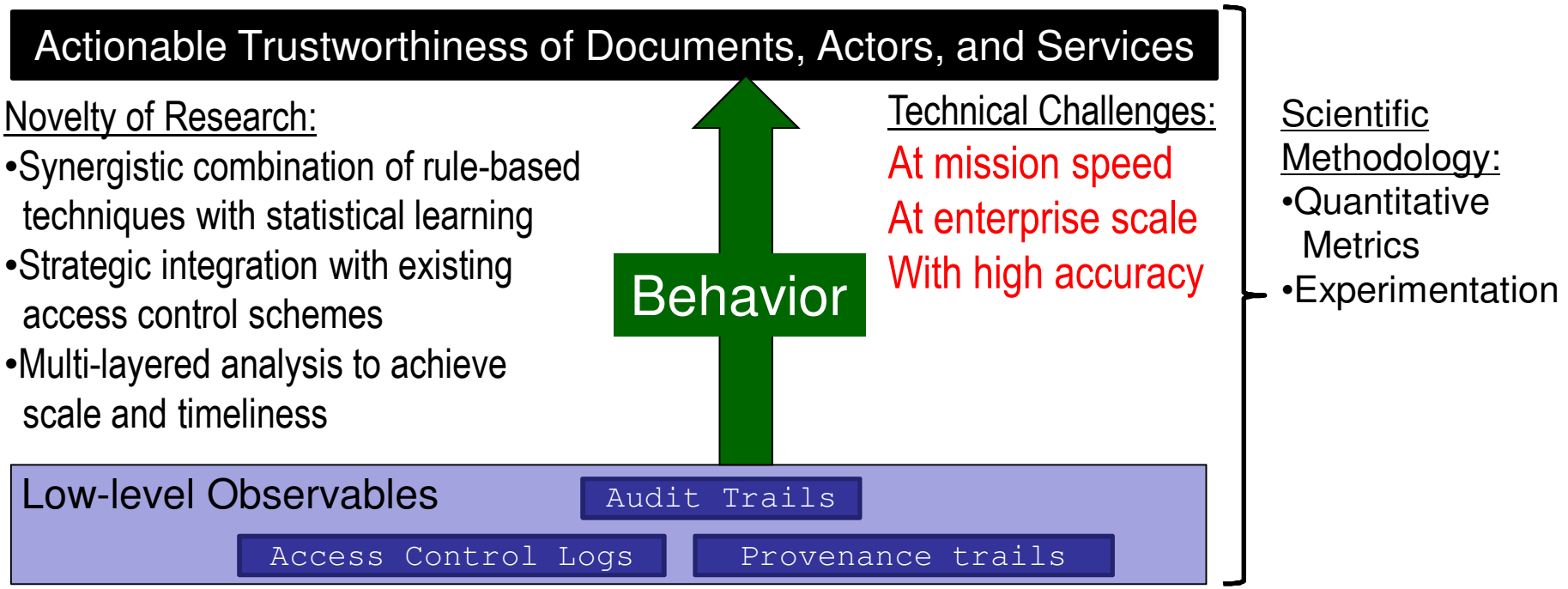
Outline for TIM September 2012

- **Behavior-Based Access Control (BBAC)**
  - Need for Statistical Cyber Defenses
  - Objectives & Scope
  - Technical Approach
- **Validating BBAC**
  - Challenges
  - Mitigation Approaches for Dealing with Lack of Data
- **Next Steps & Conclusion**
  - Immediate & Longer Term Tasks

Behavior Based Access Control (BBAC)

Urgent Need in the DoD Enterprise:

- **Day to day operation in the DoD enterprise incurs undue risk.**
  - –No systematic way to determine how recent and unfolding security events impact the trustworthiness of information, its sources, and consumers.



Impact:

Diminishes the risk of misplaced trust, increases mission reliability and assurance, and deters abuse of authorized privileges

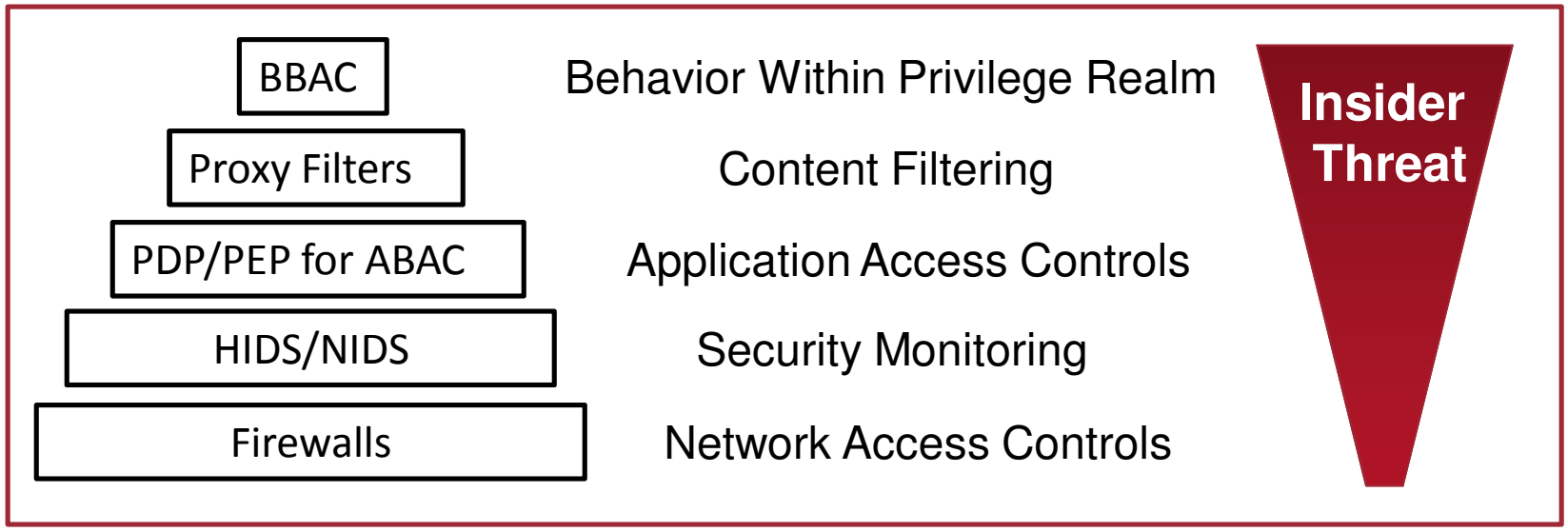
Context: Cyber Attacks

- **<u>Advanced Persistent Threats:</u> An extremely proficient, patient, determined, and capable adversary, including two or more of such adversaries working together.***
  - **Centralized Botnets**
    - Flashback Trojan Mac OS X Botnet infected 600k Mac OS X hosts (April 2012)
    - Continuously connects to one of its command-and-control (C&C) servers
    - DNS names generated programmatically & encodes "id" as part of User-Agent
  - **Decentralized Botnets**
    - Zeus turns victims into peer-to-peer-like C&C servers
- **<u>Insider Threat</u>: A person, known or suspected, who *uses their authorized access* to DoD facilities, systems, equipment, information or infrastructure to damage, disrupt, operations, commit espionage on behalf of a foreign intelligence entity or support international terrorist organizations.***
  - **Data Leaks: Stratfor Hack (starting December 6 2011)**
    - Data was being exfiltrated under the watching eye of the FBI after two weeks of the FBI knowing about the penetration
    - 200GB of data, with an additional 30GB of documents stored on an e-mail attachment or intranet server named "Clearspace"
  - **Massive unauthorized disclosure of documents: Wikileaks incident**
- **<u>Mitigation through BBAC:</u> Analysis of behaviors at multiple layers**
  - **TCP and HTTP classifiers detect change in behavior of desktop machines that all of a sudden start serving out HTTP traffic**
  - **Wikipedia edit sequence classifier detecting suspicious changes in documents**

* TERMS & DEFINITIONS OF INTEREST FOR DoD COUNTERINTELLIGENCE PROFESSIONALS,
OFFICE OF COUNTERINTELLIGENCE (DXC) DEFENSE CI & HUMINT CENTER DEFENSE INTELLIGENCE AGENCY, 2 May 2011

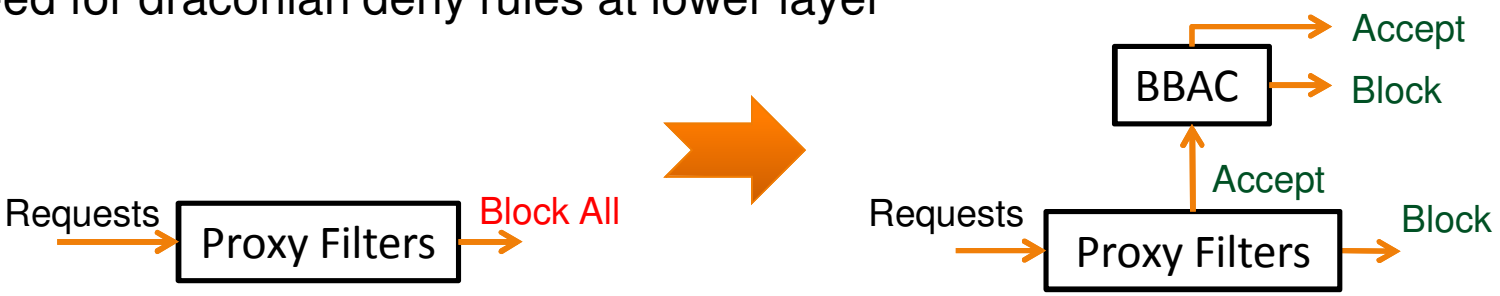
BBAC in Context

Layered Defense-in-Depth: BBAC works in conjunction with existing capabilities



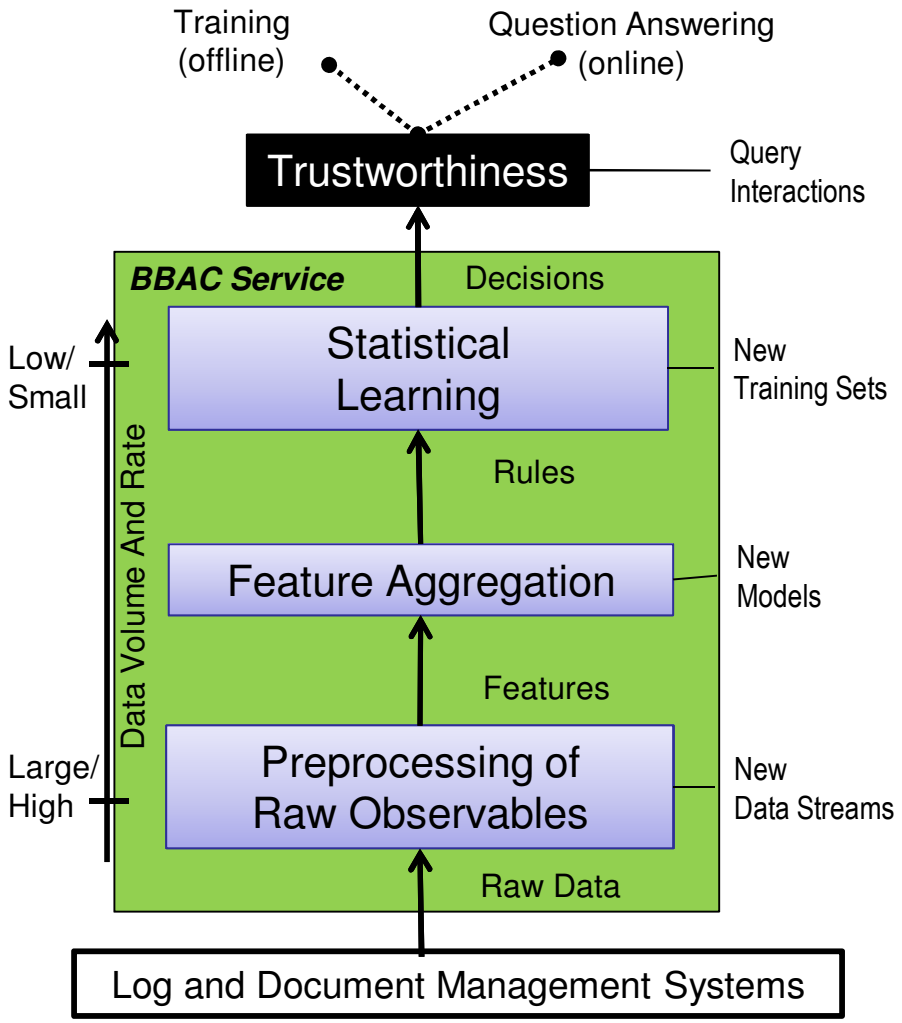
Cyber Security Monitoring and Enforcement

Compensation Controls: Sophisticated analysis at higher layers avoids the need for draconian deny rules at lower layer



BBAC Processing Pipeline

- **Combine explicit rule-based analysis of behaviors with statistical learning**
  - **Capture Subject Matter Expert knowledge through rules**
  - **Learn threshold values and combination functions over rules using Support Vector Machines (SVMs)**
- **Perform analysis at multiple layers**
  - **TCP Connections**
  - **HTTP Requests**
  - **Document Edit Sequences**

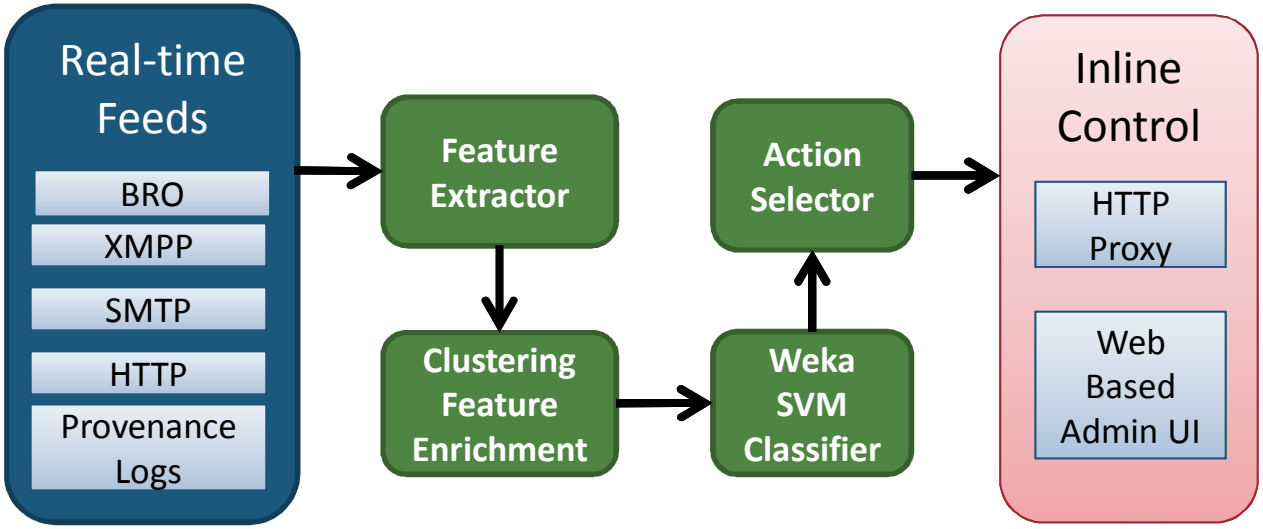


BBAC Multi-stage processing pipeline

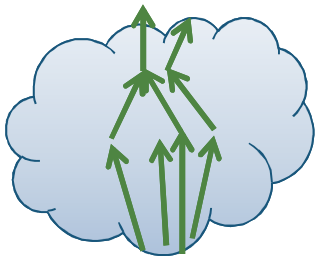
BBAC Scope

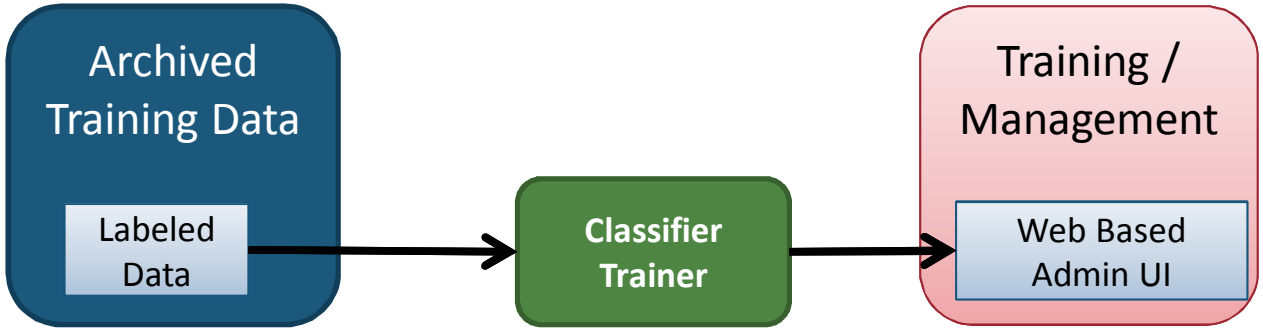
- **Network Connection Behaviors**
  - **Adversaries will use any available channel to exfiltrate information**
  - **Observable network behaviors (TCP, UDP) form a lowest level of observables**
  - **Data Set: BBN + simulated attacks**
- **HTTP Request Behaviors**
  - **HTTP is widely used and applicable for authorized and unauthorized use (web browsing, botnets)**
  - **Data Set: BBN + blacklists**
- **Information Provenance**
  - **Interactions of actors with with servers and data**
  - **Data Set: Simple English Wikipedia**
- **Email / Chat**
  - **Widely used but content is very sensitive and difficult to sanitize**
  - **Data Set: Enron**

BBAC Cloud Architecture

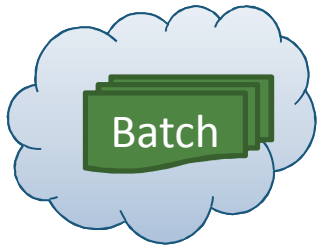


Storm: Low-Latency Scalable Stream Processing in the Cloud





Hadoop MapReduce: CPU intensive Classifier Training



Technical Challenges

- **SVM robustness**
  - **Mixed results on accuracy based on construction of training set**
    - Training times grow nonlinear with the number of observed hosts
  - **Many parameters to tune**
- **Dealing with environmental dynamics**
  - **Unanticipated users**
  - **Legitimately changing identities (DHCP)**
  - **Legitimately changing behaviors (difference in mission assignments)**
- **Managing historical information**
  - **Keeping extensive historical information about individual actors may be impractical for storage and privacy considerations.**
- **Training data**
  - **Ground truth unknown for most data**
  - **Attack simulation fidelity (TCP Connections)**
    - Cost of creating diversified attacks
    - Sensitivity of approach to assumptions introduced through simulation
  - **Processing of very large data sets (Wikipedia)**
  - **Lack of the right kind of observables (HBSS)**

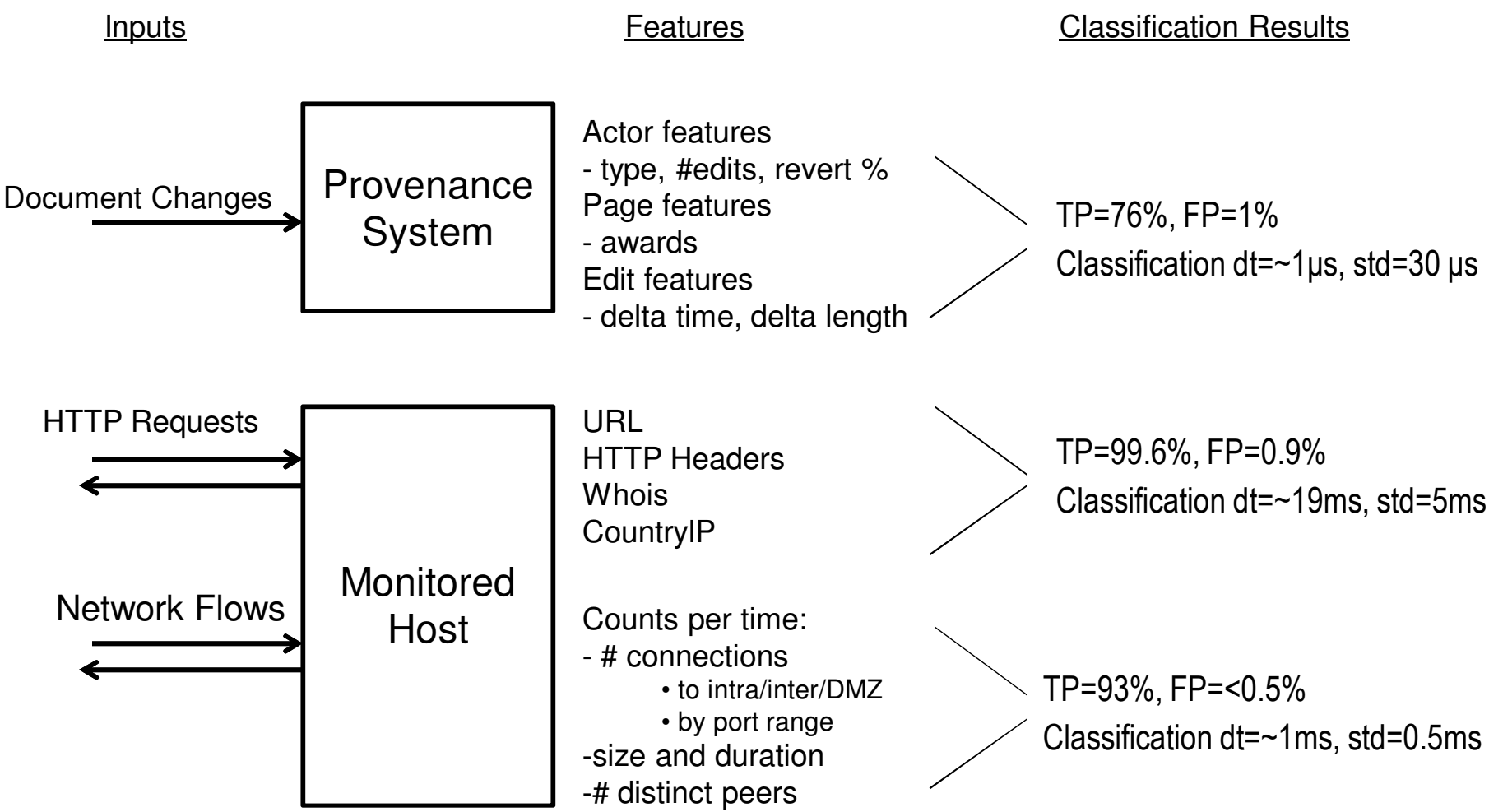
Problems with Cyber Security Data Sets

- **Value Proposition Bootstrap**
  - **Reluctance to share data before value of analysis is clear**
- **Granularity Mismatch**
  - **Processing of raw data eliminates observable behaviors**
- **Lack of Ground Truth**
  - **Specifically on APTs and Insider Attacks**
- **Accidental Complexities**
  - **Processing mechanics quickly become the main focus, e.g., by dealing with the massive amount of Wikipedia data**
- **Lack of Correlated Data Sets**
  - **Across layers, domains, and time**
- **Relevance**
  - **Specificity of available data leads to features that are difficult to reuse in other contexts**
  - **Example: Distributed trust in Wikipedia vs. hierarchical trust in DoD**

Mitigation Strategies for Validation

- **Simulated Ground Truth**
  - **Similar to Fault Injection used successfully in the past during Red Team evaluations**
  - **Coverage over interesting expected scenarios**
    - Significant Spike: Significant consistent increase in outbound connections.
    - Unexpected Connection: These attacks show outbound activity where there never was any, e.g., a server that has never made outbound requests suddenly making outbound requests.
    - Pattern Interruption: Many hosts follow a regular pattern (e.g., servers fetching updates at regular intervals). The attacks cause interruptions in those patterns.
    - Slow and Steady: Slight increase over normal values, should still be detectable, though with lower accuracy.
    - Hide within Noise: These attacks form a control case, as BBAC should not be able to detect them (Control Case).
- **Focus on Realistically Observable Information**
  - **Utilize most granular sensors available on DoD networks**
- **Find Reduced Size Data Sets**
  - **Simple English Wikipedia instead of Wikipedia**
- **Establish Correlation Through Attack Splicing**
  - **Merge known bad URLs into TCP streams**

Current Validation Results



Conclusion

- The DoD collects large amounts of audit data but lacks capabilities for performing real-time analysis to enable decision makers to respond to evolving cyber events
- BBAC aims to continuously assess trustworthiness of actors, documents, and services by virtue of classifying behaviors at multiple layers
  - TCP Connection Analysis
  - HTTP Request Analysis
  - Wikipedia Edit Sequence Analysis
- The current proof-of-concept prototype demonstrates feasibility of the approach at a Technology Readiness Level of 3
  - Accuracy of ~99% and false positive rate of ~1 %
- Validating BBAC is difficult due to availability of cyber security data sets
  - Relevant data sets anyone, please!?
- Next steps
  - Focus on engineering to increase TRL of prototype from 3 to 5
  - Focus on Stylometric features for insider detection
  - Conduct extended experimentation, e.g., in the DoD IA Range

Contacts

Michael J. Mayhew, AFRL/RIEBA
BBAC Program Manager
Michael.Mayhew@rl.af.mil
315-330-2898 (DSN = 587)

Michael Atighetchi, BBN
BBAC Principal Investigator
matighet@bbn.com
617-873-1679

Dr. Rachel Greenstadt
Statistical Machine Learning Expert
greenie@cs.drexel. edu

Acronyms

Acronym	Description
ABAC	Attribute Based Access Control
BBAC	Behavior Based Access Control
DoD	Department of Defense
FP	False Positive
HIDS	Host Intrusion Detection System
HTTP	Hyper Text Transfer Protocol
IA	Information Assurance
NIDS	Network Intrusion Detection System
PDP	Policy Decision Point
PEP	Policy Enforcement Point
TCP	Transmission Control Protocol
TP	True Positive
TRL	Technology Readiness Level
SVM	Support Vector Machine
URL	Uniform Resource Locator