**Introduction and Research Goals**

- **Problem:** Data for detecting cyber attacks may not be available at both the training and deployment phases:
  - Data from a source may be "missing" and therefore unavailable for processing.
  - Data from a source may be ignored if it is suspected to be compromised.
  - Data from a source may be restricted due to privacy issues.
  - Data from a source may be too expensive or impractical to obtain at deployment time, such as expert information produced by human analysts.

Terminology: We call features that are available for training but are not available at deployment "privileged features," and we call feature that are available both at training and deployment time "standard features."

PrivSense: A novel system that aims to make use of privileged features only for training in order to improve the accuracy of cyber attack detection.

**Technical Approach**

**State of the Art:**
- Current machine learning techniques cannot make use of observables for training if the same observables are not available at test time.
- Drawback: Degraded accuracy of detection due to loss of information.

**PrivSense Design:**
- $x(\text{train})$ is the dataset available during training, $x(\text{test})$ is the test dataset which is in the same space as $x(\text{train})$, and $x'(\text{test})$ is the test dataset without privileged features.
- $M$ is the model used as a learning algorithm, and $f$ is the hypothesis it learns from the $x(\text{train})$.

PrivSense makes continuous evaluation of $f(x)$ on $x'(\text{eval})$ by predicting the privileged features from standard ones.

**Underlying Theory: Learning Using Privileged Information (LUPI) [1]**

1. Where does "Privileged" Information come from? Some possible sources include:
   - Features that are too expensive to collect on a deployed system, such as detailed system performance data.
   - Features that are not available at deployment time, such as expert analysis.
   - Features that are missing, e.g., from malfunctioning sensors.
   - Features that may be compromised due to infection of the source system.

2. How to use privileged features:
   - Transferring knowledge from standard features to derive privileged features (Knowledge Transfer).
   - Use privileged features during training to learn a more accurate unified model (SVM+).

**Results**

**Case Study:**

- **Standard Features**
  - Intra Flow Stats
  - Inter Flow Stats
  - DNS Stats

- **Privileged Features**
  - App Information

- Investigating applicability of PrivSense to detection of botnet clients that use DGA (Domain Generation Algorithm) for botnet C&C
  - Differentiate between "legitimate" DNS queries resulting in NXDOMAIN responses (e.g., generated through genuine user/app typos/errors) and those generated by a DGA.

**Preliminary Results:**

- Knowledge Transfer accuracy for privileged features

**Research Plan/Next Steps**

- Complete PrivSense evaluation on DGA case study using CyberVAN testbed.
- Use new evaluation metrics to measure PrivSense performance gain.

**Primary Researchers**

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z. Berkay Celik</td>
<td>PSU</td>
<td><a href="mailto:zbc102@cse.psu.edu">zbc102@cse.psu.edu</a></td>
</tr>
<tr>
<td>Patrick McDaniel</td>
<td>PSU</td>
<td><a href="mailto:mcmichael@cse.psu.edu">mcmichael@cse.psu.edu</a></td>
</tr>
<tr>
<td>Rauf Izmailov</td>
<td>ACS</td>
<td><a href="mailto:rizmailov@appcomsci.com">rizmailov@appcomsci.com</a></td>
</tr>
<tr>
<td>Ritu Chadha</td>
<td>ACS</td>
<td><a href="mailto:rchadha@appcomsci.com">rchadha@appcomsci.com</a></td>
</tr>
<tr>
<td>Constantin Serban</td>
<td>ACS</td>
<td><a href="mailto:cserban@appcomsci.com">cserban@appcomsci.com</a></td>
</tr>
<tr>
<td>Roberto Pagliari</td>
<td>ACS</td>
<td><a href="mailto:rpagliari@appcomsci.com">rpagliari@appcomsci.com</a></td>
</tr>
</tbody>
</table>

**Task Rotations (listed by PI)**

| Dr. Ritu Chadha, PI (ACS) | ARL | 10 days, ARL |
| Z. Berkay Celik, PhD. Student (PSU) | ACS | 3 months, ACS |

**Collaborations**

| PSU | Penn State University |
| ACS | Applied Communication Sciences |