CS259D: Data Mining for Cybersecurity
One-class classification

- Most samples from target class
- Rejection rate
  - % of training data points classified as outliers
  - Allows for presence of noise
  - Tolerable false positive rate
One-class SVM

- Hyperplane separating training samples from the feature space origin
  - May not always exist in original feature space
  - Feature space mapped to a Kernel space
  - With Gaussian kernel, hyperplane always exists

\[ K(x, y) = \Phi(x) \cdot \Phi(y) = \exp\left(-\frac{\|x - y\|^2}{2s}\right) \]

\[
\min_{w, \xi, \rho} \left( \frac{1}{2} \|w\|^2 - \rho + \frac{1}{hC} \sum_{i=1}^{h} \xi_i \right)
\]

\[ w \cdot \Phi(x_i) \geq \rho - \xi_i \quad (1 \leq i \leq h) \]

\[ f_{svc}(z) = I(\sum_{i} \alpha_i K(x_i, z) \geq \rho); \quad \sum_{i=1}^{h} \alpha_i = 1 \]
Class-conditional probability formulation

- Conditional probability representation:

\[ p(x \mid w_t) = \frac{1}{(2\pi s)^{d/2}} \sum_{i=1}^{n} \alpha_i K(x, x_i) \]

- This is actually a distribution
- Classify as normal if:

\[ p(x \mid w_t) \geq \rho'; \quad \rho' = \rho/(2\pi s)^{d/2} \]
Fusion rules

- Min, Max, Mean, Product
- Applied to a-posteriori class probabilities under different models: $P_i(w_j | x)$
- Assuming uniform distribution for outliers can turn these rules into class-conditional probabilities
Combining one-class SVM classifiers

- **Average:**
  \[
  y_{\text{avg}}(x) = \frac{1}{L} \sum_{i=1}^{L} p_i(x \mid w_t)
  \]
  \[
  y_{\text{avg}}(x) < \theta \Rightarrow \text{outlier}
  \]

- **Product:**
  \[
  y_{\text{prod}}(x) = \prod_{i=1}^{L} p_i(x \mid w_t)
  \]

- **Min and Max rules similarly defined**
- **Majority voting rule:** Class voted for by majority of classifiers
McPAD: Multiple Classifier System for Accurate Payload-based Anomaly Detection

- Features (2\(v\)-grams): frequencies of bytes that are \(v\) bytes apart
- \(256^2\) features irrespective of \(v\)
- Computed using a sliding window of size \(v + 2\)
  - Marginalized distribution
- \(v=0\) is the 2-gram model of PAYL
- Combination to reconstruct sequence information
- Feature clustering to reduce dimension
McPAD architecture

Diagram:
- PAYLOAD
- Feature Extraction and Reduction
- Model 1
- Model 2
- Model m
- Summation (Σ)
- Label
# Experiments: Parameters

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\gamma$</td>
<td>0.5</td>
<td></td>
</tr>
<tr>
<td>$\nu$</td>
<td>0-10</td>
<td></td>
</tr>
<tr>
<td>Feature Clusters ($k$)</td>
<td>10, 20, 40, 80, 160</td>
<td></td>
</tr>
<tr>
<td>Desired $FP$ Rate</td>
<td>10%, 5%, 2%, 1%, 0.5%, 0.2%</td>
<td>0.1%, 0.05%, 0.02%, 0.01%, 0.001%</td>
</tr>
</tbody>
</table>
Attacks

- Generic attacks
- Shell-code attacks
- CLET attacks
- PBA attacks
## Results

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Generic Attacks</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>k=10</td>
<td>0.83501</td>
<td>0.86331</td>
<td>0.8633</td>
<td>0.87187</td>
<td>0.75765</td>
</tr>
<tr>
<td>k=20</td>
<td>0.8366</td>
<td>0.8613</td>
<td>0.86135</td>
<td>0.86882</td>
<td>0.7492</td>
</tr>
<tr>
<td>k=40</td>
<td>0.8366</td>
<td>0.86312</td>
<td>0.86407</td>
<td>0.87783</td>
<td>0.77834</td>
</tr>
<tr>
<td>k=80</td>
<td>0.84778</td>
<td>0.85948</td>
<td>0.8595</td>
<td>0.88594</td>
<td>0.80212</td>
</tr>
<tr>
<td>k=160</td>
<td>0.87016</td>
<td>0.8884</td>
<td>0.8828</td>
<td>0.87131</td>
<td>0.69164</td>
</tr>
</tbody>
</table>

| **Shell-code Attacks** |
| k=10   | 0.98632   | 0.99544    | 0.99543     | 0.99323    | 0.94105    |
| k=20   | 0.98758   | 0.99689    | 0.9969      | 0.99361    | 0.94685    |
| k=40   | 0.98903   | 0.99827    | 0.99826     | 0.99417    | 0.97585    |
| k=80   | 0.99613   | 0.99874    | 0.99875     | 0.9965     | 0.98666    |
| k=160  | 0.98723   | 0.99785    | 0.99775     | 0.99709    | 0.76661    |

| **CLET Attacks** |
| k=10   | 0.99776   | 0.99854    | 0.99854     | 0.99866    | 0.9589     |
| k=20   | 0.99778   | 0.99839    | 0.99839     | 0.99925    | 0.969      |
| k=40   | 0.99757   | 0.99815    | 0.99815     | 0.99908    | 0.98624    |
| k=80   | 0.99773   | 0.99785    | 0.9979      | 0.99925    | 0.99669    |
| k=160  | 0.99737   | 0.9985     | 0.99844     | 0.99913    | 0.83275    |
Results
Results
References

“McPAD: A Multiple Classifier System for Accurate Payload-Based Anomaly Detection”, Perdisci et al, 2009