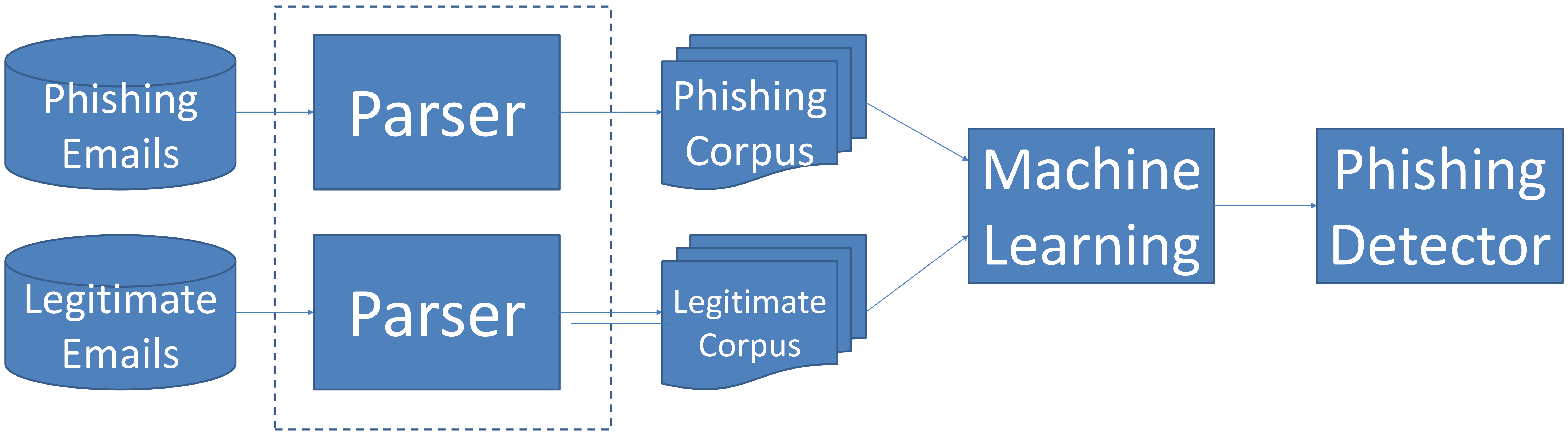
CERIAS
The Center for Education and Research in Information Assurance and Security

Semantic Phishing Detection

Courtney Falk

Our goal is to improve the detection of phishing attack emails by using natural language processing (NLP) technology that models the semantic meaning behind the email text.


(Same software, different data flows)

Phishing Emails

Legitimate Emails

Parser

Parser

Phishing Corpus

Legitimate Corpus

Machine Learning

Phishing Detector

This is a specific application that belongs to the meaning-based machine learning (MBML) program which claims that machine learning on meaningful data will produce superior results.

Phishing is a global problem. It allows attackers to circumvent existing protection mechanisms by attacking the user directly.

RSA at the Purdue Research Park tracks computer intrusions on behalf of its corporate customers and finds several troubling phishing trends:

- Estimated financial loses to phishing attacks are almost $6 billion every year
- Phishing attacks are increasing year-on-year and are unlikely to decline
- The United States is the largest target in the world for phishing attacks

Phishing detection is deployed in a form that most benefits the user:

- Email client plugin
- Browser webmail plugin
- Standalone email server scanning engine

The mechanism for meaning representation is the ontological semantics technology (OST) NLP system. Ongoing research here at Purdue aims to represent knowledge and language understanding in machine-usable forms.

CERIAS

PURDUE
UNIVERSITY