CERIAS

The Center for Education and Research in Information Assurance and Security

pSigene: Generalizing Attack Signatures

Christopher Gutierrez, Jeff Avery, Gaspar Modelo-Howard, Fahad Arshad, Saurabh Bagchi, Yuan Qi

Problem Statement

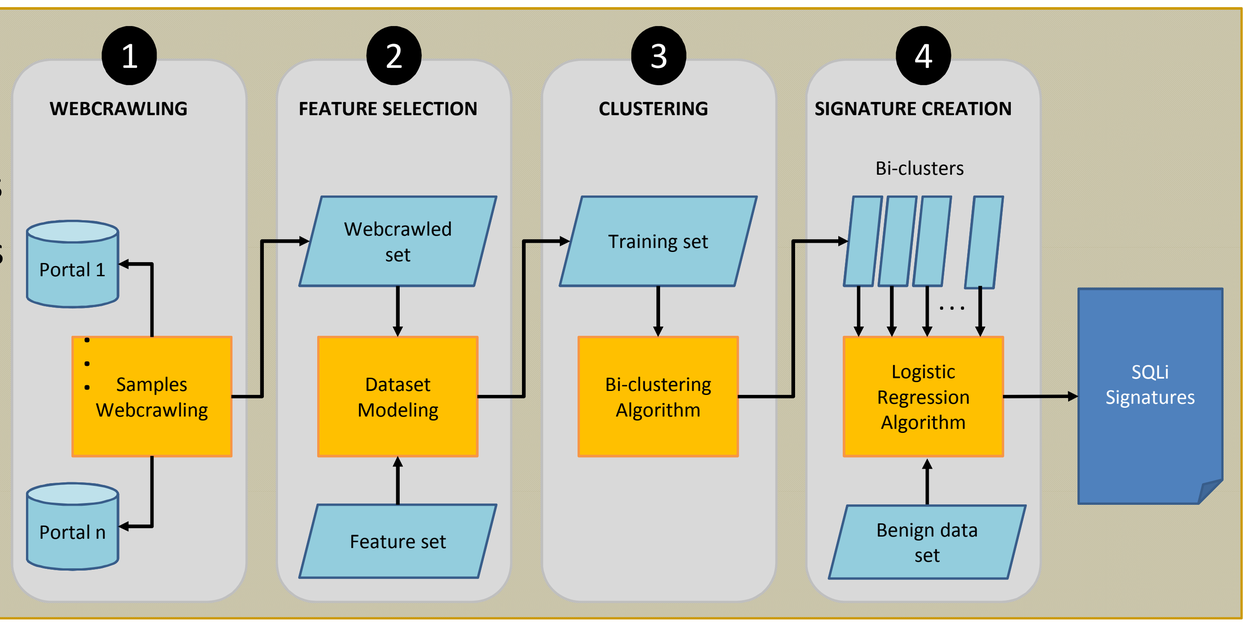
- Misuse-based detection systems rely on attack signatures
- In practice, signature creation and maintenance is a manual process

Specific Goals

- Define process to ***automatically generate detection signatures***
- Create **generalized signatures**, matching for attacks and its variations

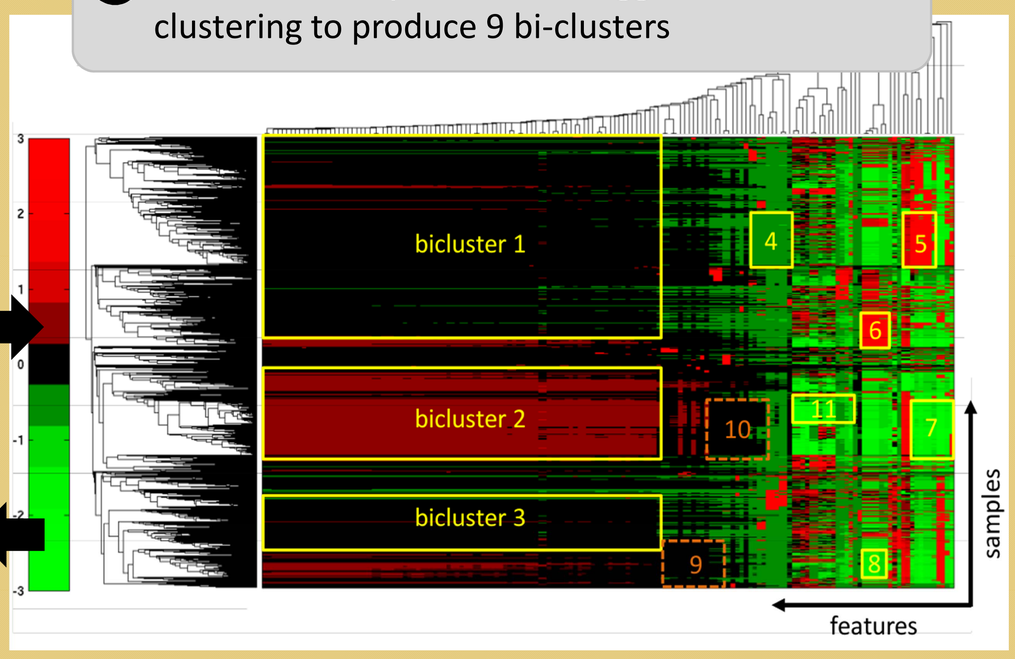
pSigene Architecture

1. WEBCRAWLING: Search cybersecurity portals to collect attack samples
2. FEATURE SELECTION: Extract a rich set of features from attack samples and detection signatures
3. CLUSTERING: Apply bi-clustering technique to samples, identifying distinctive features for each resulting bi-cluster
4. SIGNATURE CREATION: Generate generalized signatures, one for each bi-cluster, using logistic regression modeling



Experimental Results

1. Collect attacks samples (~30k)
2. Characterize each sample with ~160 features
3. Perform a 2-way hierarchical agglomerative clustering to produce 9 bi-clusters
4. Generate 9 generalized signatures for each bi-cluster



Evaluation

Test Set 1.4M (benign) and 7.2k (malicious) HTTP GET requests

Accuracy Comparison

RULES	TPR(%)	FPR(%)
Bro	73.23	0.00
Snort – Emerging Threats	79.55	0.1742
ModSecurity	96.07	0.0515
pSiGene (9 rules)	86.53	0.037
pSiGene (7 rules)	82.72	0.016

Ongoing Work – Phishing

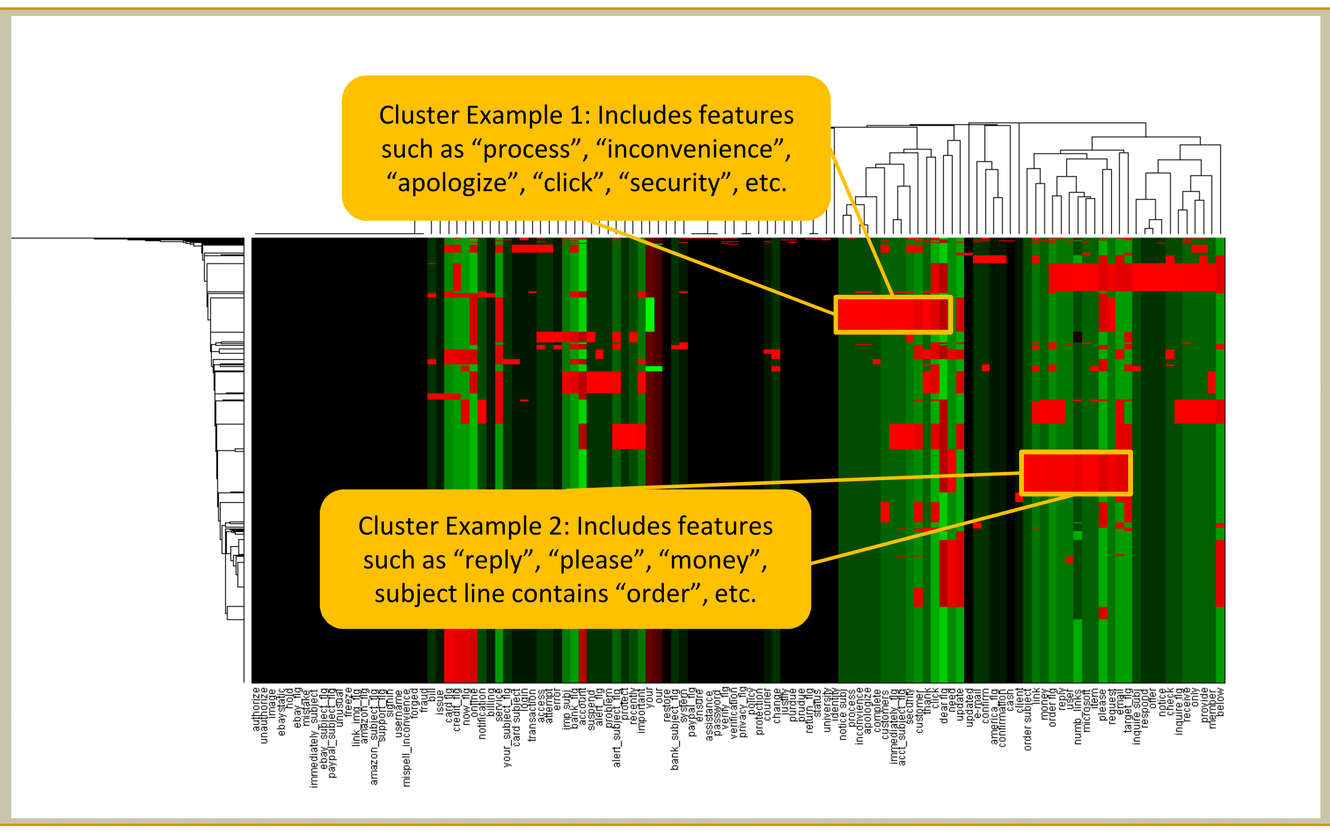
- Apply pSigene to phishing attacks
- Goal: automatically generate phishing signatures targeted towards universities

Preliminary Work

- ~70k phishing samples from ITaP
- ~120 features

Preliminary Conclusions

- Banks/financial institutions still primary target
- Images as links do not appear as prevalent technique
- Urgency seen when phishing for account credentials, not credit card information



PURDUE UNIVERSITY