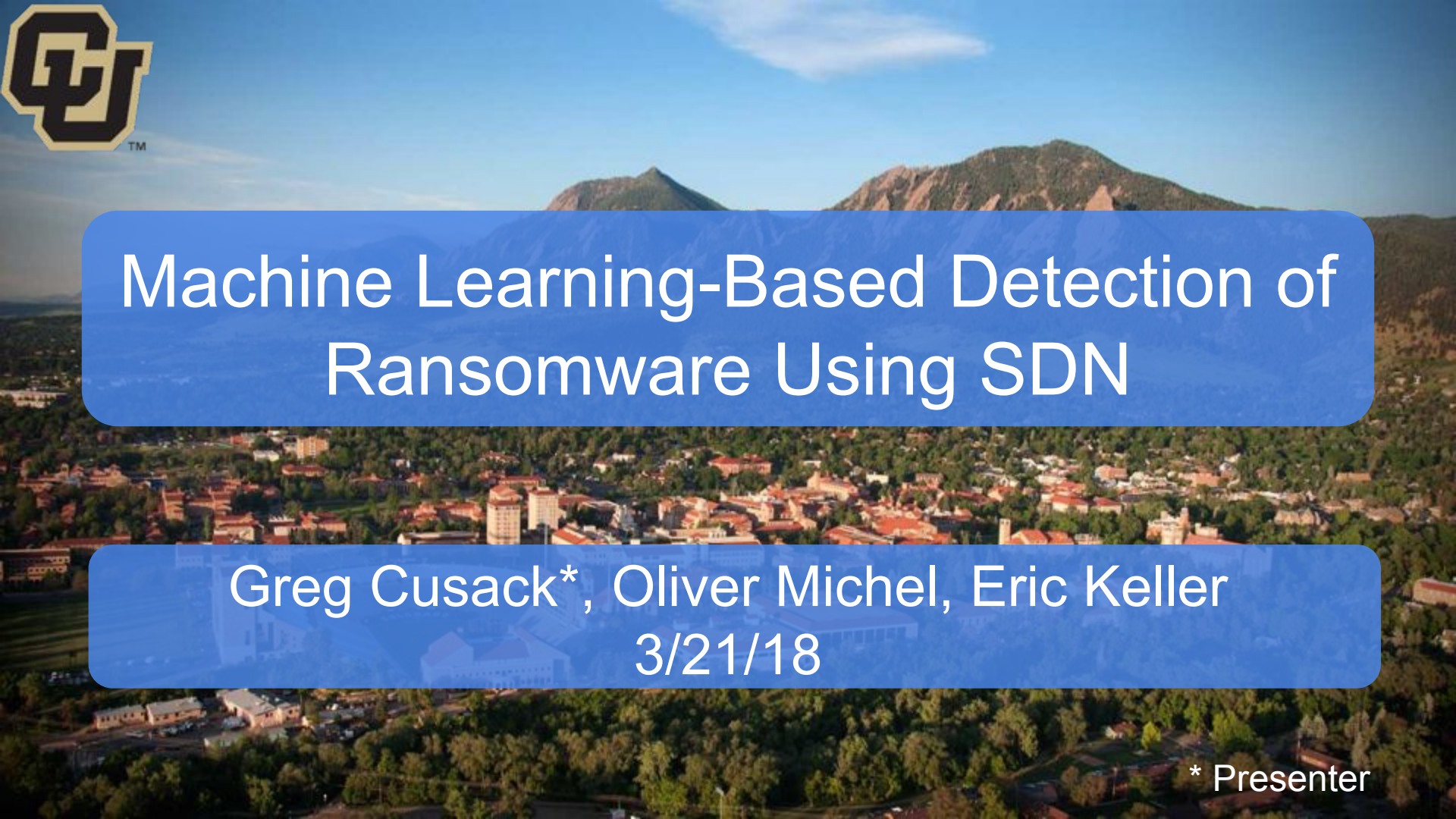


Machine Learning-Based Detection of Ransomware Using SDN

Greg Cusack*, Oliver Michel, Eric Keller

3/21/18

* Presenter

Overview

- Ransomware Overview
- Previous work
- Programmable Forwarding Engines (PFEs)
- Method
- Classification
- Results
- Current Progress

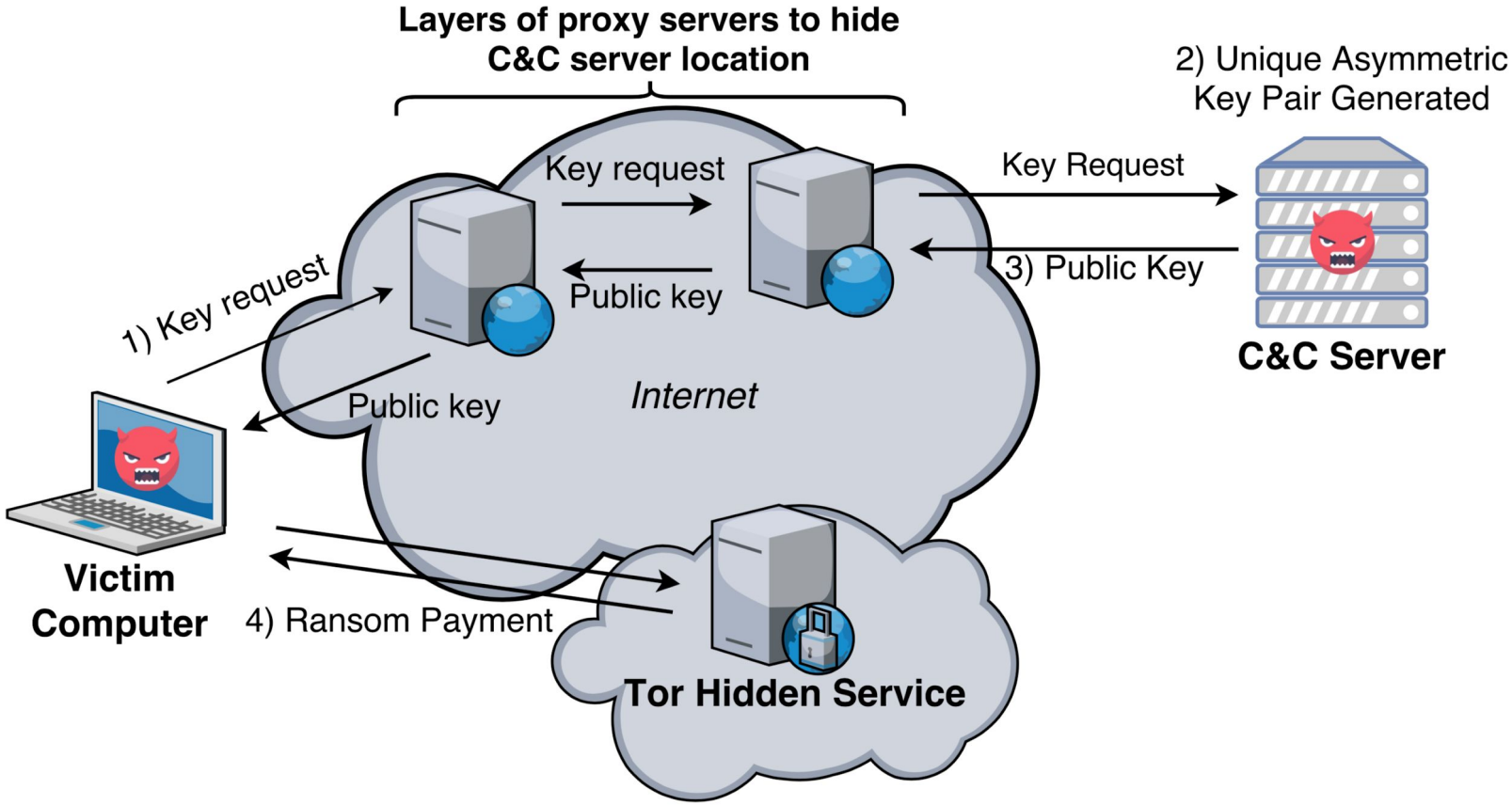
Ransomware

- Malicious software holds a victim's files at ransom
- Files held until ransom paid
- Two main types:
  - Locker
  - Crypto
- Difficult to develop long term solutions
- IoT boom -> More avenues for infection
- Ransomware as a Service (RaaS)

WannaCry Ransomware

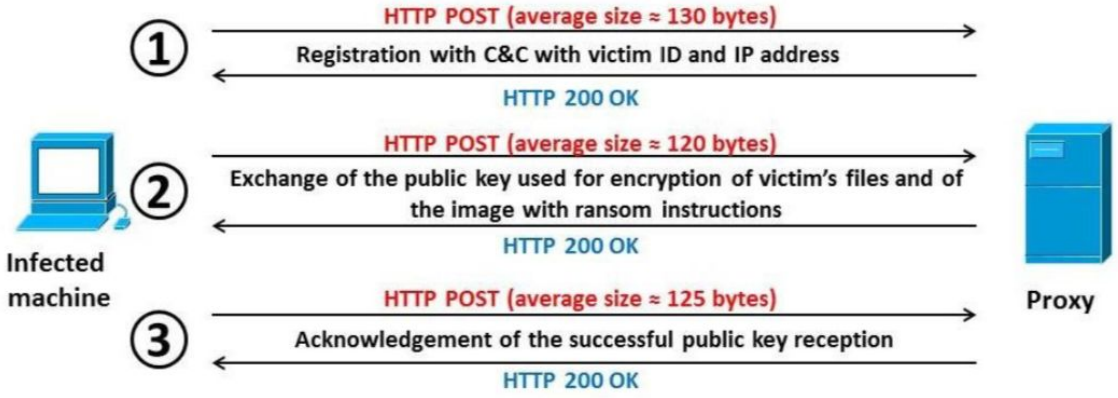
Source: https://www.pbs.org/newshour/science/everything-need-know-wannacrypt-ransomware-attack

Ransomware Data Flow



Previous Work

- EldeRan: Machine learning approach for ransomware classification
  - Track Windows API calls, file system operations, registry key operations, etc.
- Software-defined networking-based detection of crypto ransomware
  - Fingerprint HTTP traffic
- Most packet trace approaches are payload-based



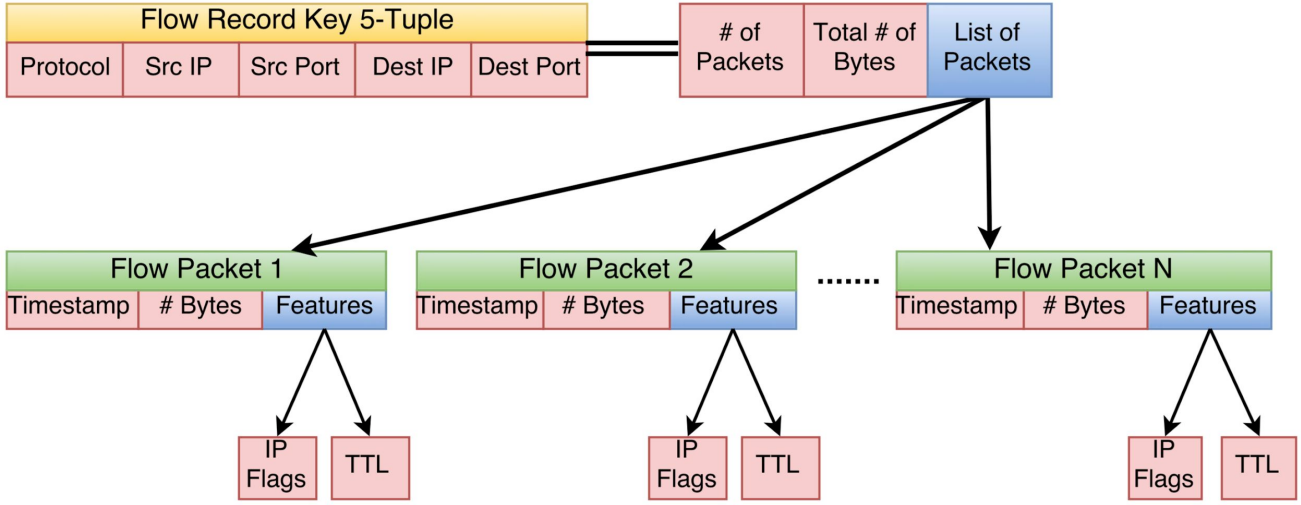
Source: K. Cabaj, M. Gregorczyk, and W. Mazurczyk. Software-defined networking-based crypto ransomware detection using http traffic characteristics. arXiv preprint arXiv:1611.08294, 2016

Programmable Forwarding Engines (PFEs)

- High-rate, programmable, network switches
- Supports the scalable generation of rich flow records
- Can process network data at high-rates of speed and extract vital, per-packet flow information
- Provides data and speed necessary for network, flow-based, traffic analysis and fingerprinting

Compact, Per Packet Flow Records

- Provides richness and scalability for large networked systems
- Tailored to fit a user's specific application



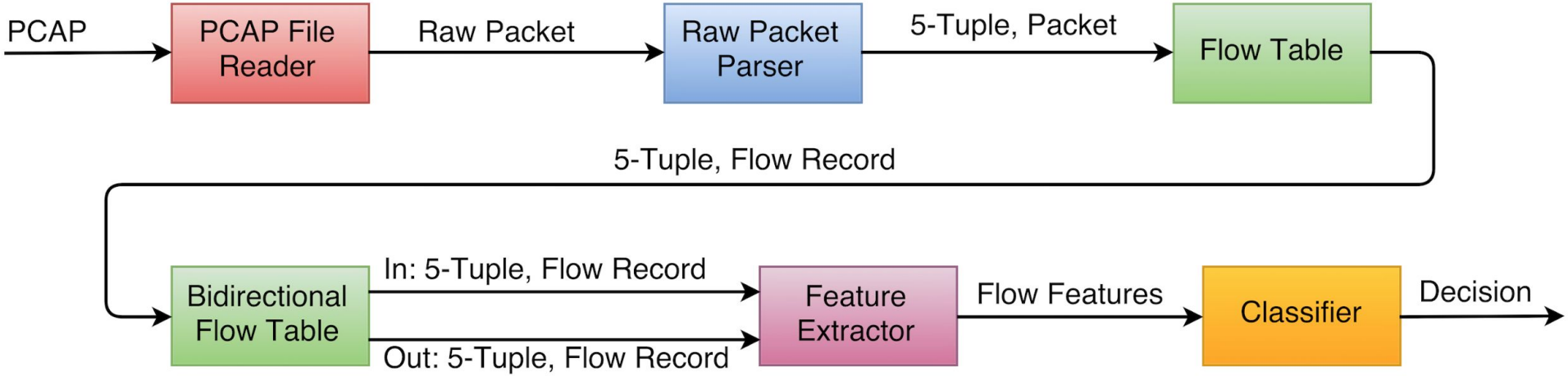
PFE Flow Record Overview and Features

Method

- Goal: Utilize machine learning and leverage the recent trend in switch hardware to identify ransomware via its network traffic signature
- Collect ransomware PCAP samples (>100MB)
- Collect clean traffic as baseline
  - Web browsing, streaming, file downloading, etc.
- Stream processor development
- Classification

Source: http://www.malware-traffic-analysis.net

Flow Records and Stream Processing

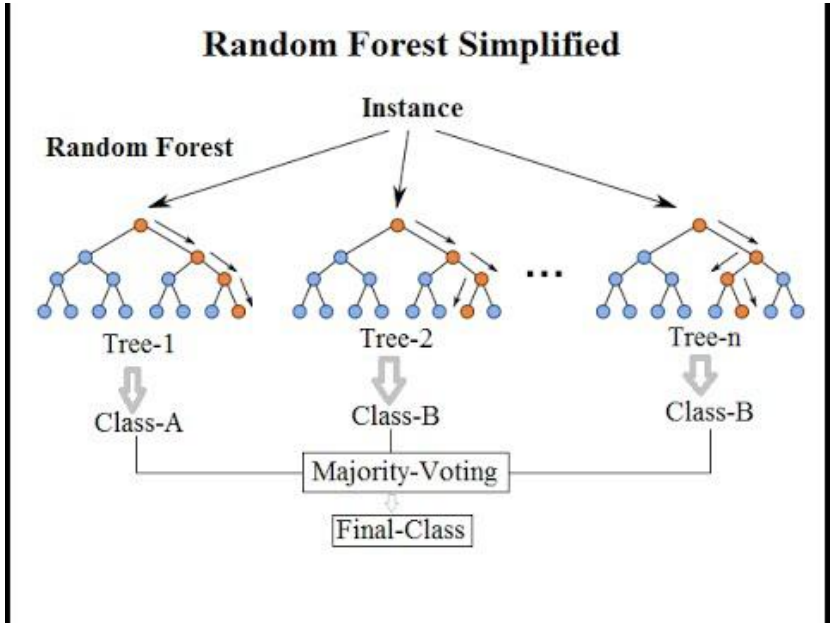


Flow-Based Features

- Flow Duration
- Interarrival Times
  - Minimum
  - Mean
  - Maximum
  - Standard deviation
- Packet Lengths
  - Minimum
  - Mean
  - Maximum
  - Standard deviation
- Burst Lengths
  - Minimum
  - Mean
  - Maximum
- Total number of packets
- Ratios:
  - Packets out/packet in
  - Bytes out/bytes in
- # of unique packet lengths

Random Forest

- Ensemble Algorithm
  - Divide and conquer approach
- Collection of decision trees
  - Avoids overfitting
- Random subsets of features used to build smaller, shallower trees
- Majority voting from decision trees to decide class
- Bagging used to improve stability, reduce variance, and increase accuracy

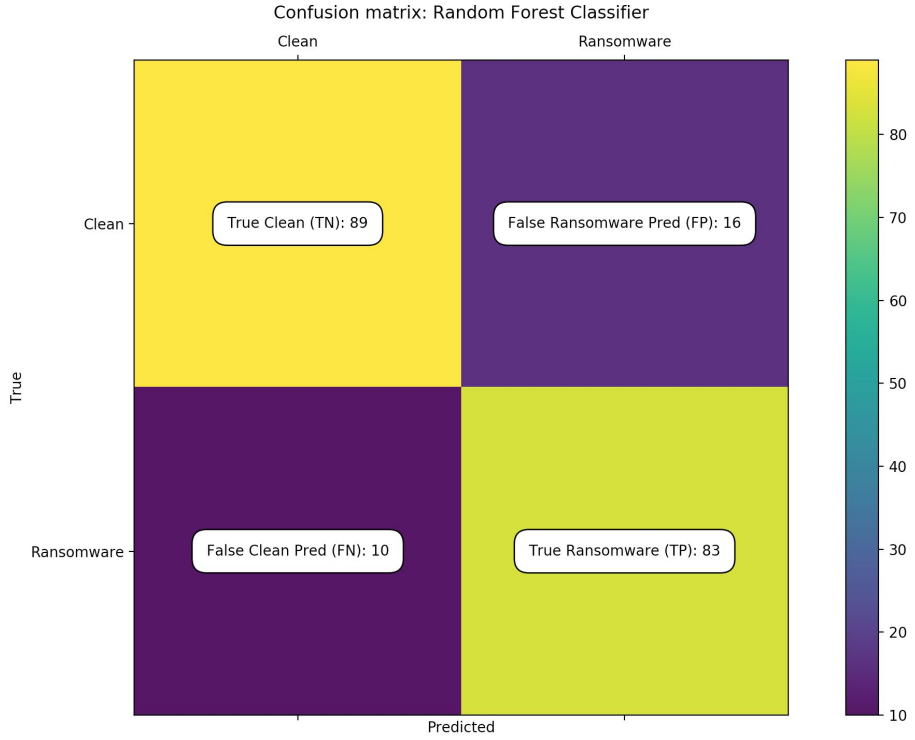


Source: https://www.youtube.com/watch?v=D_2LkhMJcfY

Results

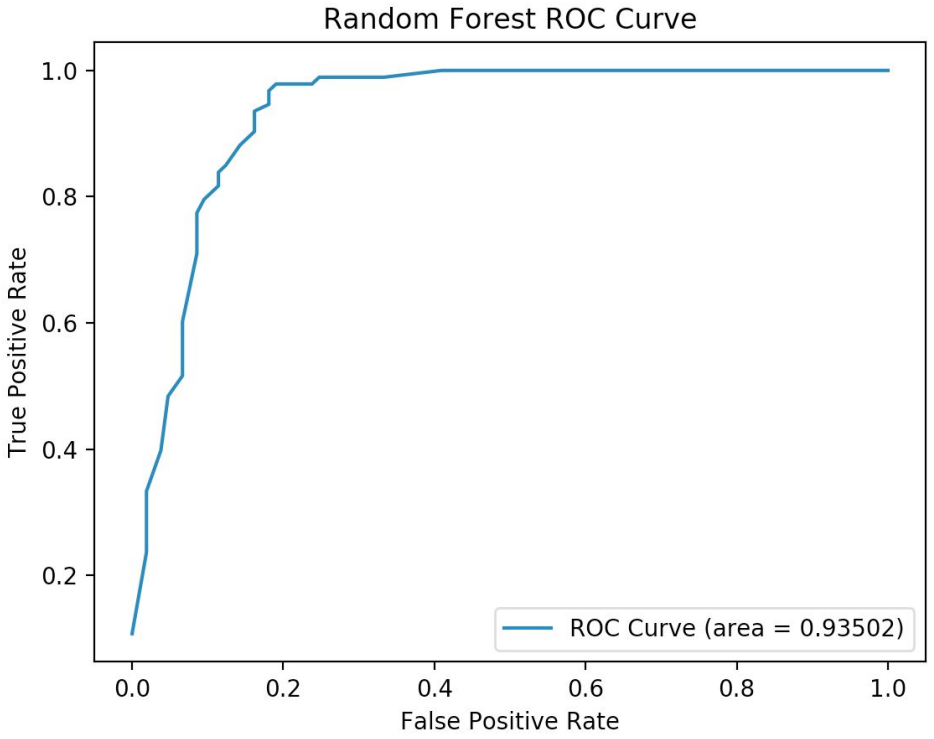
Confusion Matrix (28 Features)

- Accuracy
  - Correct / total = **0.8689**
- Recall
  - tp / (tp + fn) = **0.8925**
- Precision
  - tp / (tp + fp) = **0.8384**
- F1 Score
  - 2 * (R * P) / (R + P) = **0.8689**

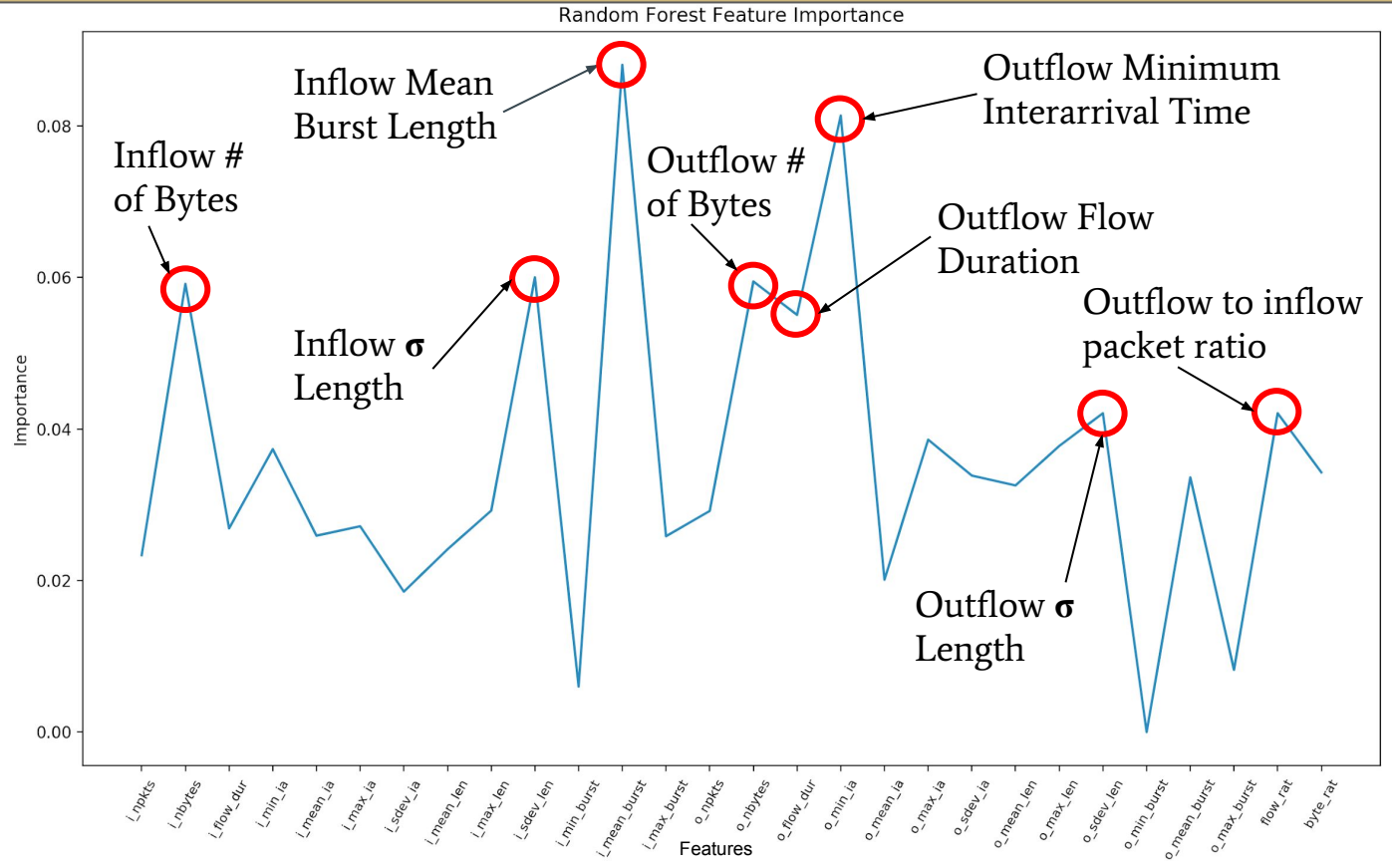


ROC Curve (28 Features)

- Area Under Curve (AUC)
  - 0.93502
- 10-Fold Cross Validation Score
  - 0.87301
- Decision Trees: 40
- Max Tree Depth: 15

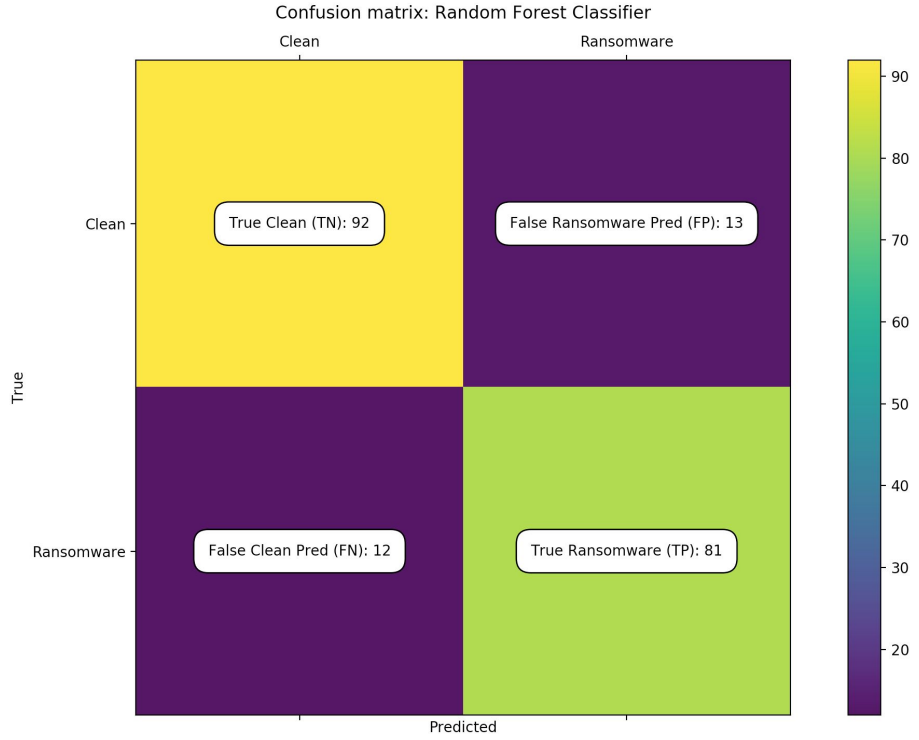


Feature Importances (28 Features)



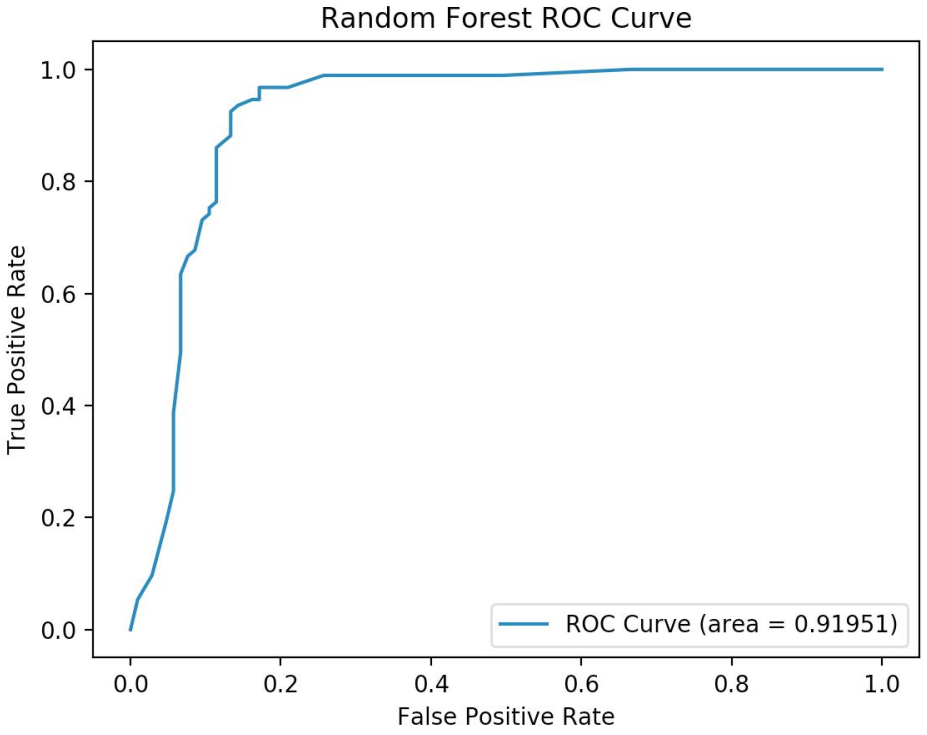
Confusion Matrix (8 Features)

- Accuracy
  - Correct / total = **0.8738**
- Recall
  - tp / (tp + fn) = **0.8710**
- Precision
  - tp / (tp + fp) = **0.8617**
- F1 Score
  - 2 * (R * P) / (R + P) = **0.8738**

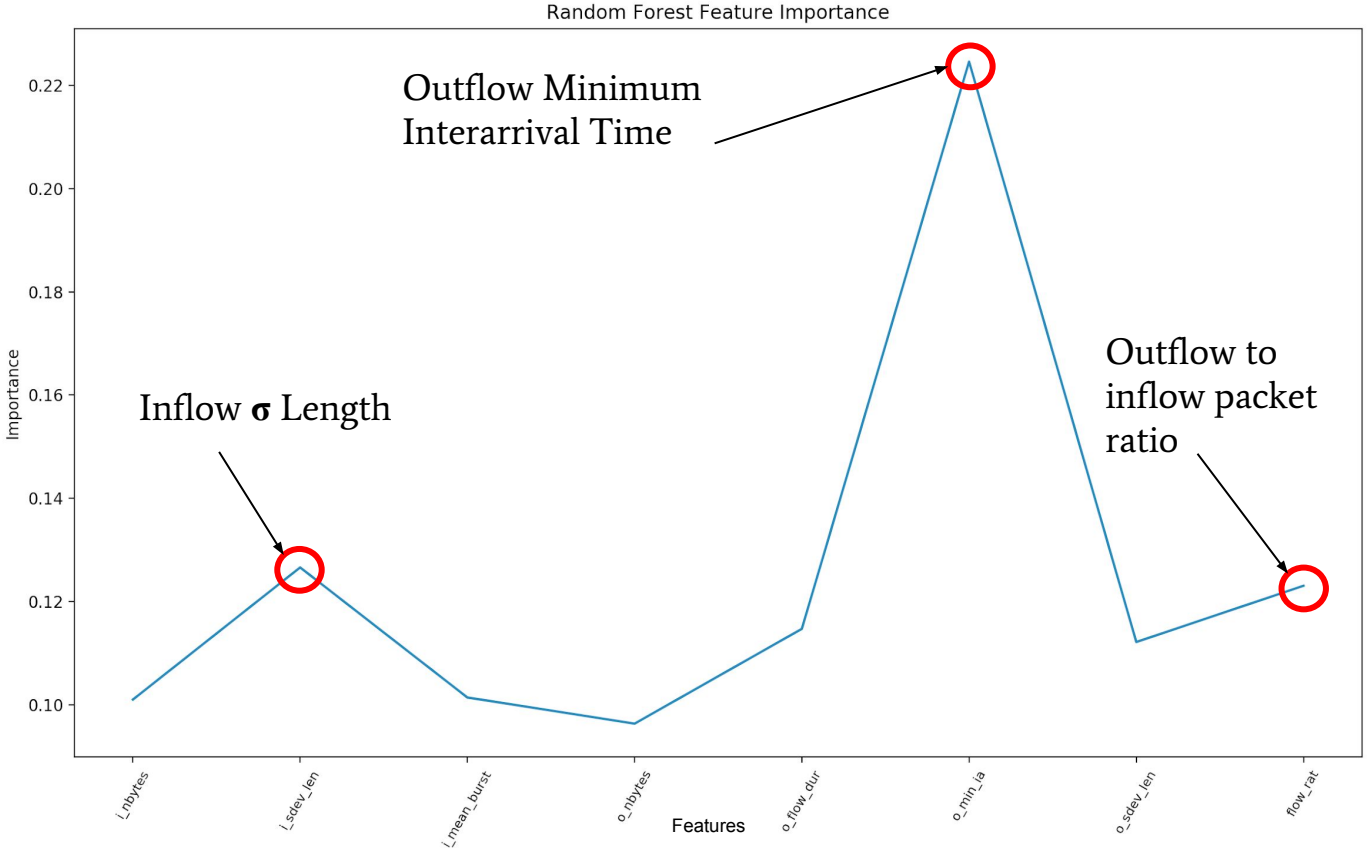


ROC Curve (8 Features)

- Area Under Curve (AUC)
  - 0.91951
- 10-Fold Cross Validation Score
  - 0.86827
- Decision Trees: 40
- Max Tree Depth: 15



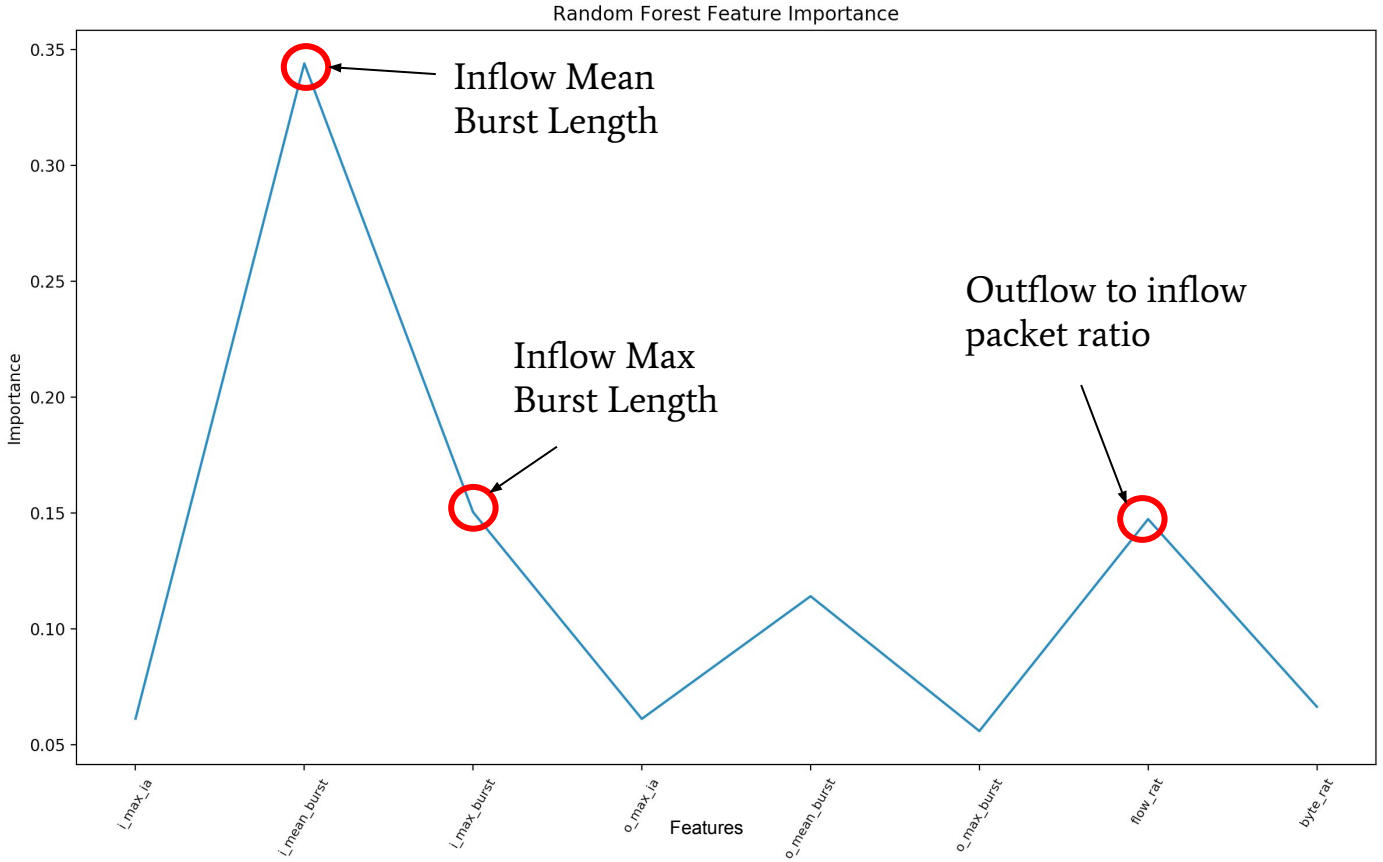
Feature Importances (8 Features)



Crypto-Based Cerber Ransomware Detection

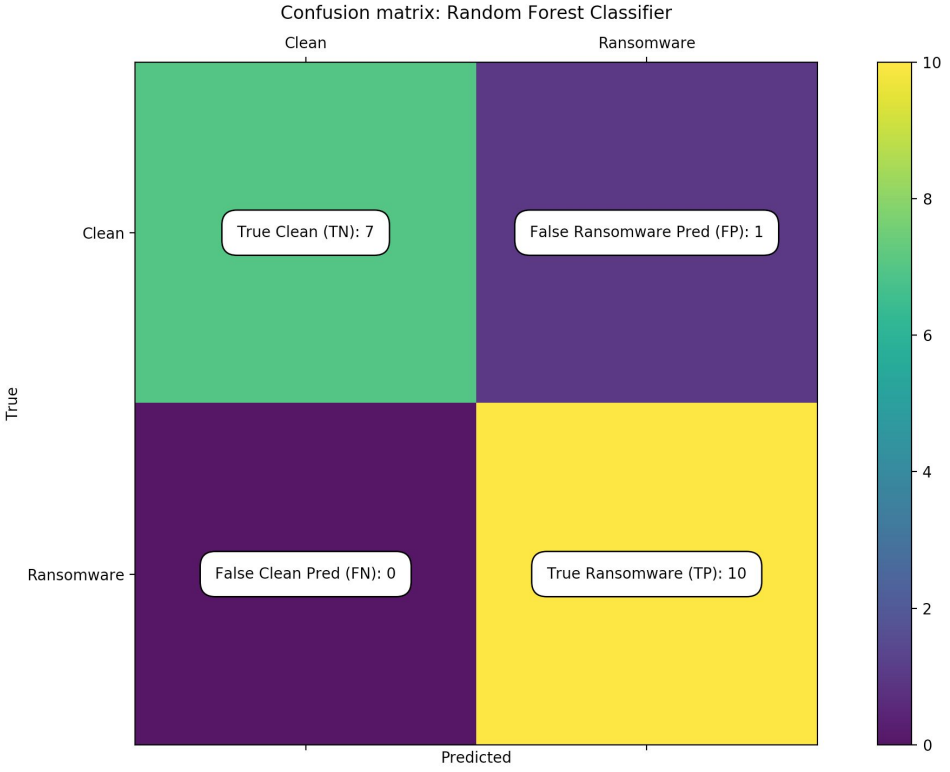
Can we identify a specific type of ransomware?

Cerber Feature Importances (8 Features)



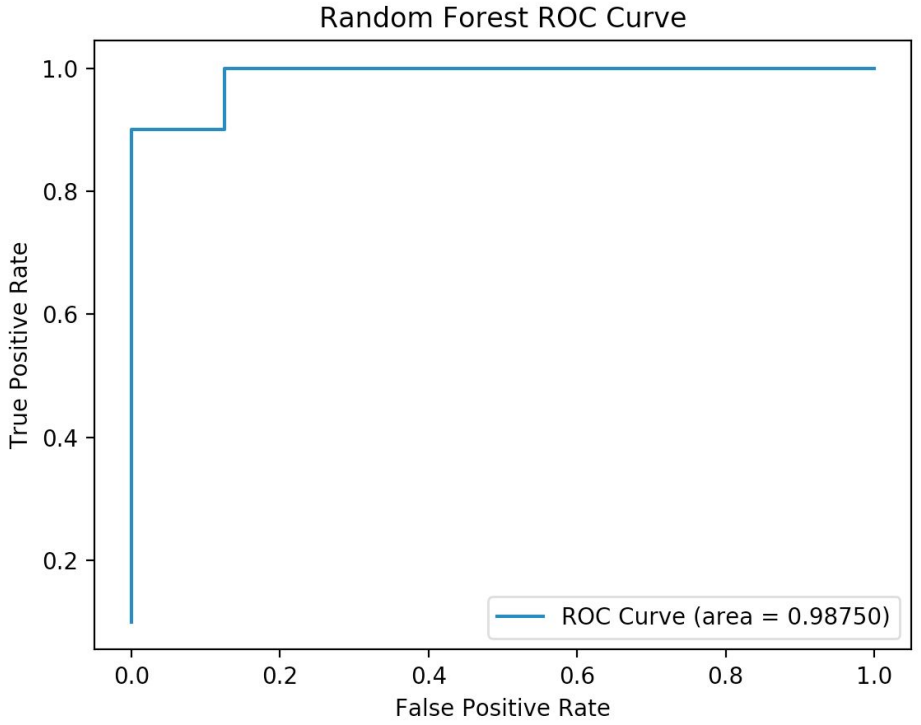
Confusion Matrix Cerber Ransomware

- Accuracy
  - Correct / total = **0.9444**
- Recall
  - tp / (tp + fn) = **1.000**
- Precision
  - tp / (tp + fp) = **0.9091**
- F1 Score
  - 2 * (R * P) / (R + P) = **0.9439**



ROC Curve Cerber Ransomware

- Area Under Curve (AUC)
  - 0.98750
- 10-Fold Cross Validation Score
  - 0.90500
- Decision Trees: 40
- Max Tree Depth: 15



Takeaways

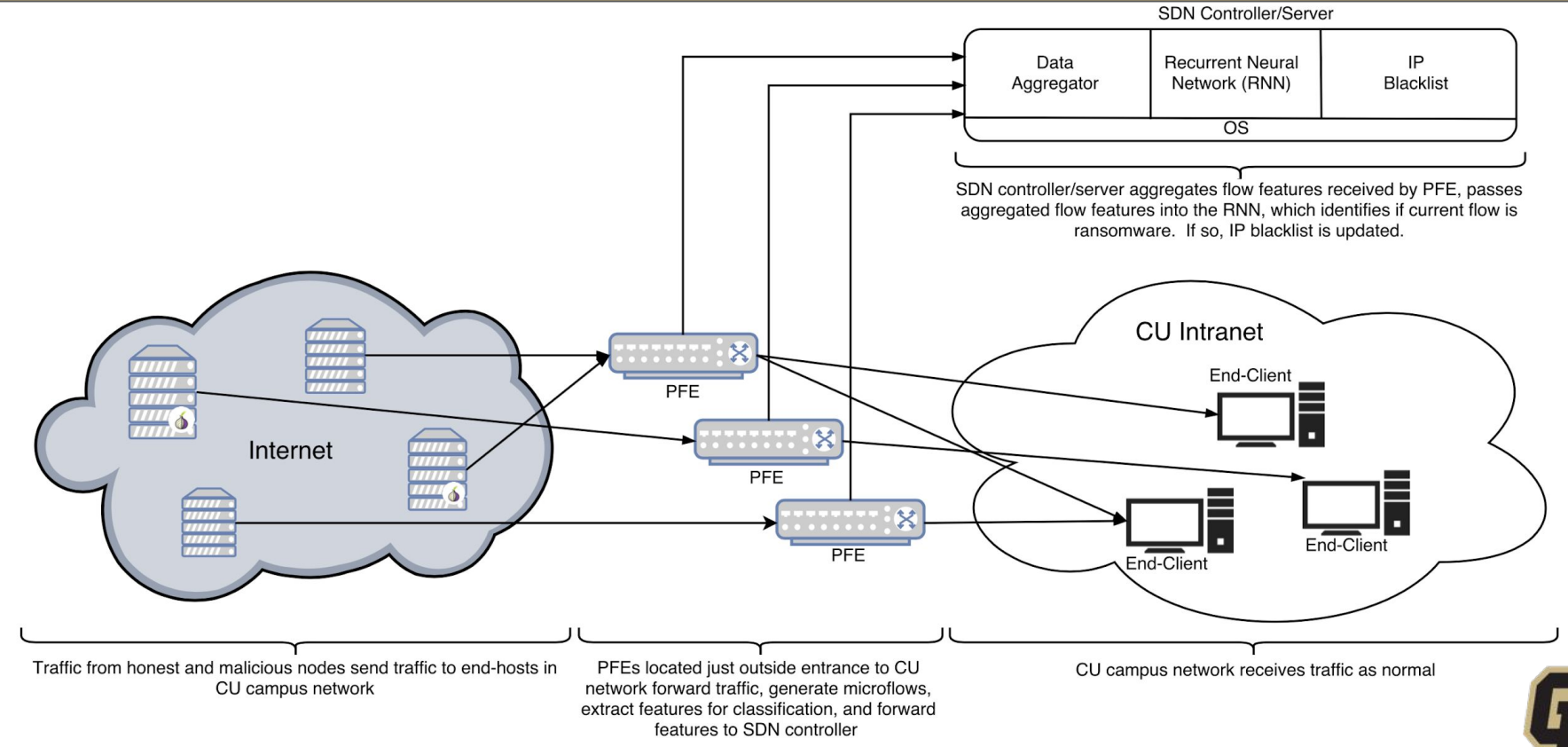
- Initial findings are promising but require further research
- Packet lengths, interarrival times, and flow ratios leave ransomware susceptible to identification
- Recent emergence of PFEs provide the right backbone for flow-based feature extraction

Work in Progress

- Sandboxing ransomware samples to collect network traffic
- Implementing stream processor on a PFE ASIC
- Developing LSTM Recurrent Neural Network
- System architecture redesign

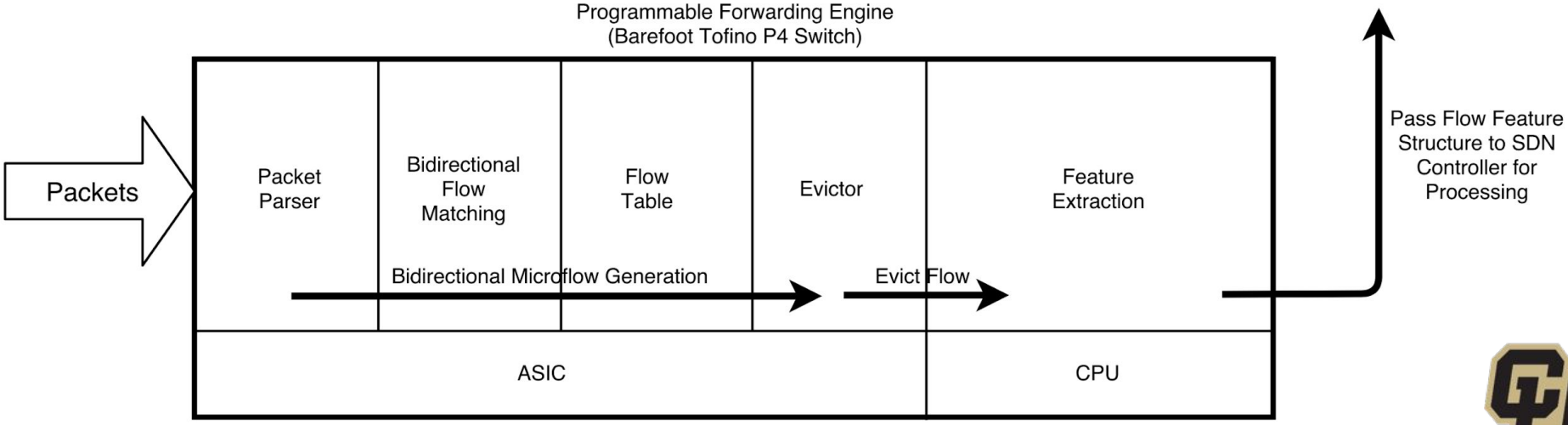
Questions?

Ransomware Detection System Overview

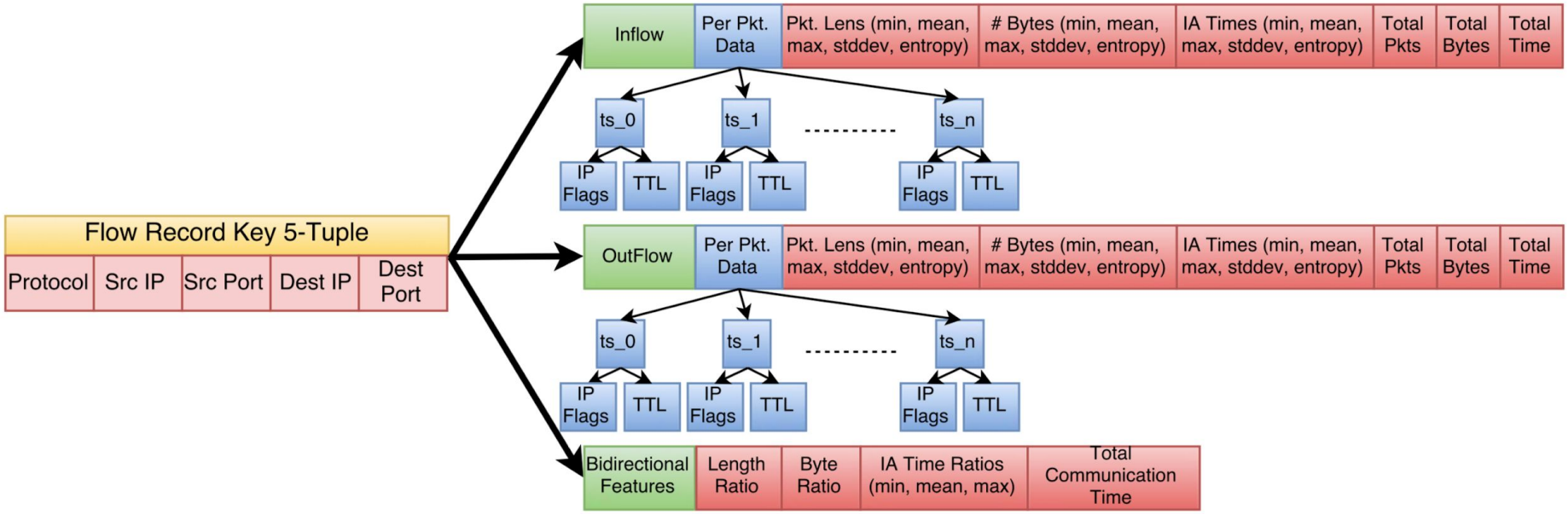


Hardware-generated, Bidirectional Microflows

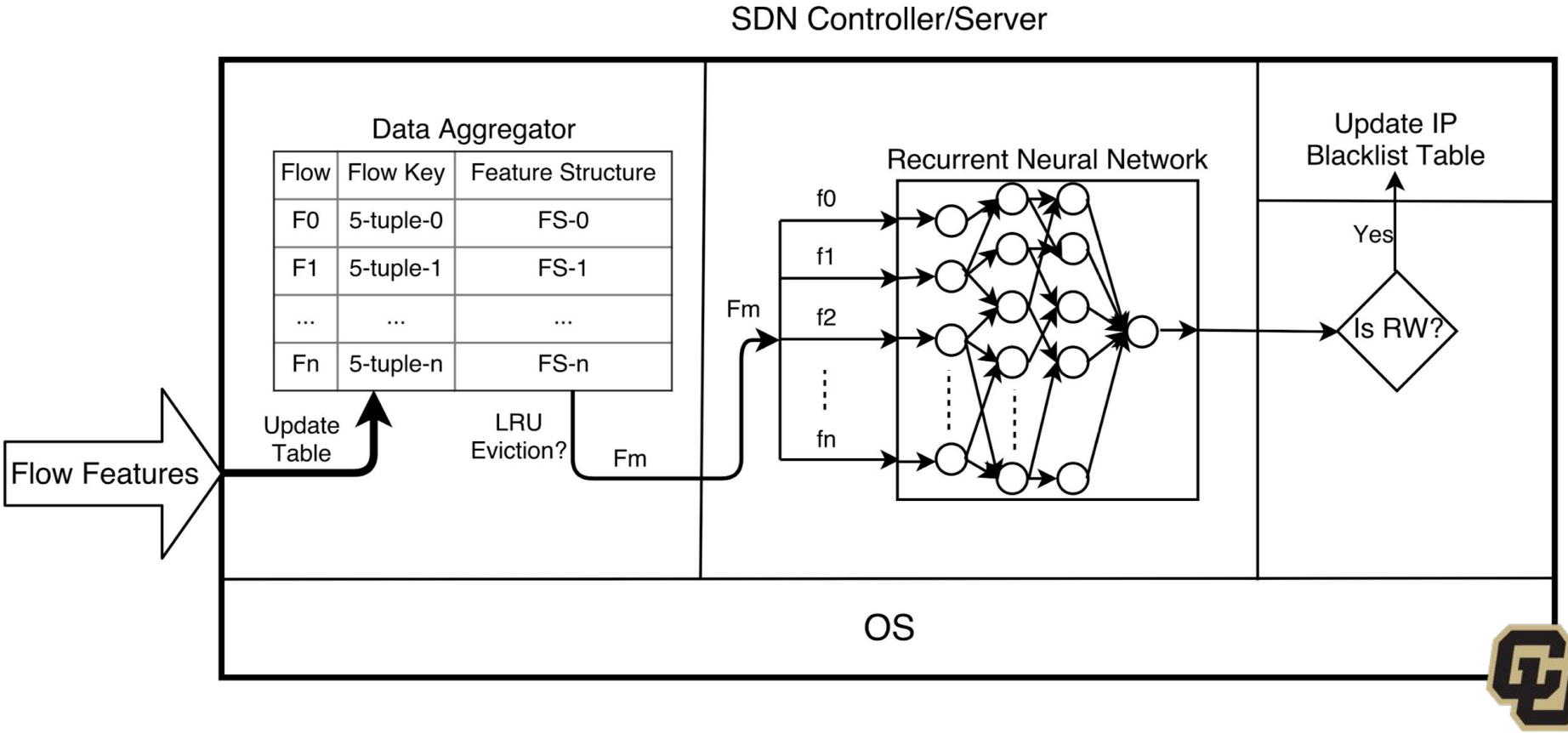
- Generated in switch ASIC
- Turn current *Flow flow table into bidirectional flow table
- Evict bidirectional microflows to CPU for feature extraction
- PFE data flow overview:



Flow Feature Structure



SDN Controller/Server Data Flow



Packet Length Frequency