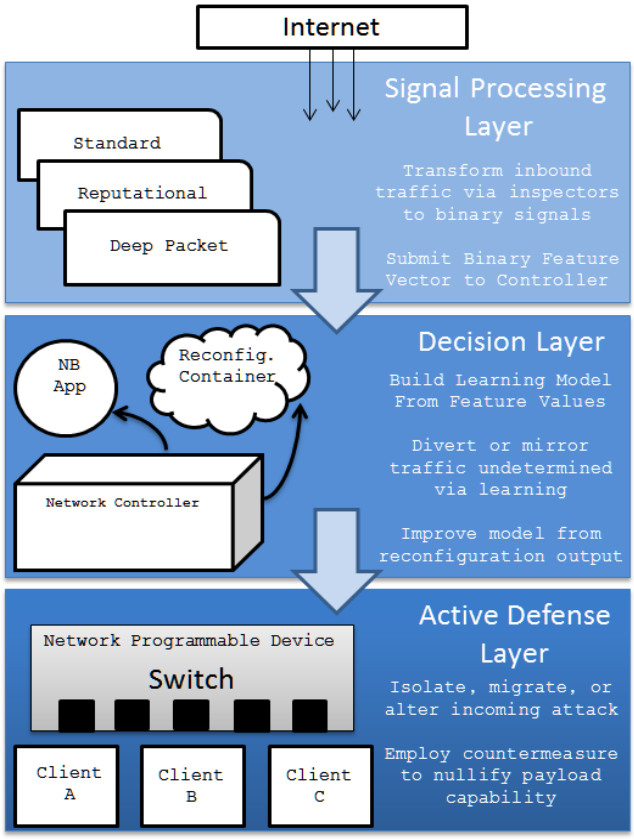
Christian J Johnson
Software Engineering Research Fellow, SEAM Lab
University of Maryland, College Park

# Dynamic Reconfiguration: A Model for Cyber Subterfuge and Active Defense

Information systems are ill-equipped to deal with the adversarial learning challenge modern-day malware poses. Armed with metrics and signature-based Intrusion Detection Systems (IDS), networks are often left vulnerable to evolutionary (self-modifying) malware featuring specialized behaviors that attackers patiently craft and target to meet an objective. The problem is compounded by the rapid adoption of encryption technologies that enable malicious payloads to be delivered securely over common network protocols and evade detection. We define a new dynamic reconfiguration framework that offers a rich array of active defenses in response to anomalous traffic. Our system enables reconfiguration of network topologies, allowing sandboxed analysis to improve prediction accuracy without blocking legitimate traffic. Component level reconfiguration further reduces application exposure by increasing the complexity in navigating through a program's attack surface.

Our approach to dynamic reconfiguration employees a modular design abstracted into three functional layers: signal, decision, and active defense. In the signal layer, a network programmable device (NPD) translates network conversations into feature vectors so that raw traffic can be represented as indicator data. In the decision layer, a learning model interprets features generated by the signal layer to assess whether a given network conversation should be allowed to proceed with compete certainty. Should the application have a substantial degree of uncertainty in arriving at a decision, it employs a *dynamic reconfiguration* API to safely generate more features, validate predictions and, if warranted, trigger active defenses. The active defense layer then communicates with the API to support reconfiguration tactics that mirror, redirect, or rebuild network pathways; interchange components; and alert applications to mitigate attacks. These mechanisms protect infrastructure and enhance behavioral classification of malware while expending the resources of an attacker.




This new approach has led to the successful development of learning models that identify specific classes of malware such as ransomware. These results have also expanded active defense capabilities at the network level in addition to existing reconfiguration functionality deployed at application and system levels.

RSAConference
Security Scholar

# Dynamic Reconfiguration: A Model for Cyber Subterfuge and Active Defense

Christian J. Johnson
Software Engineering Research Fellow, SEAM Lab
University of Maryland, College Park

## Problem Statement and Goals

```
'Request': 'HTTP/1.1 200 OK'
'Date': 'Tue, 13 Feb 2017'
'Accept-Ranges': 'bytes'
'Content-Length': '35731'
'Content-Type': 'text/plain'
'Connection': 'keep-alive'
'Server': 'Apache'
'Expires': 'Fri, 17 Feb 2017'
```

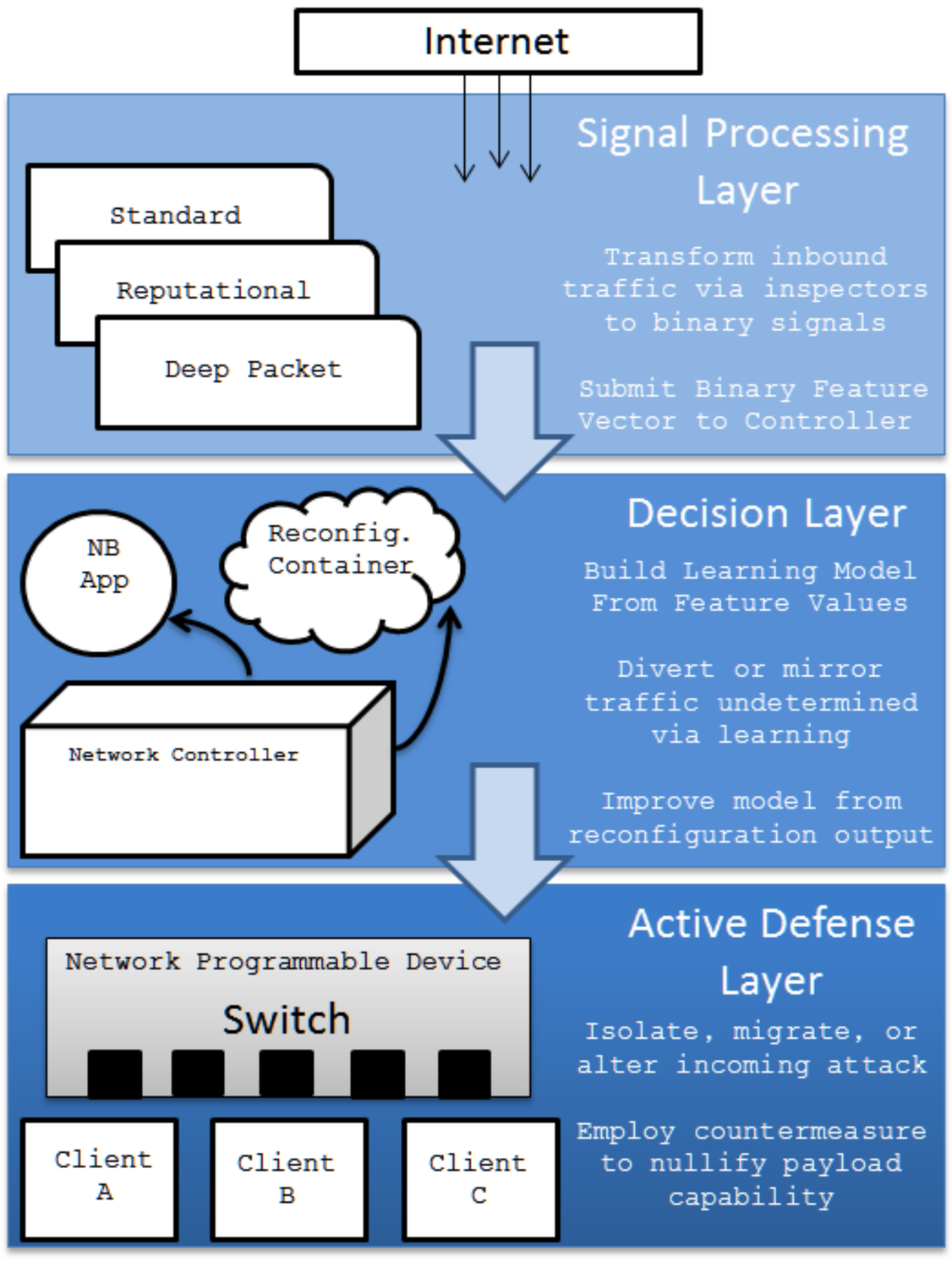
```
{DC1ÞpHwWQCq5F‹ ¹hJÿYh9d436VTNpKwWQGq
USÌGq5FtFhJGYh9d436ESCVTpK;VVG‰p,FhJ
N·SO‡CANê~!òETX€    ÓsETBÔe÷EMu3½6¾C
_Ü[A´1»ãqÊUV³uµðêFNpÂ:·^ñ~:ðŽÇ£¨FSz8:
‡b¿úp'GETX°i…S-Äì3¸;KÚ2Köžud~«u¦Í®½¶(
£ÚSTXACK"õ‰üMU ŸÎWæ¹k»Å^À2¿Ð^DC1ÊEë±
```

**Problem** : Metrics and signature-based Intrusion Detection Systems quickly flag previously recognized threats, but are poorly equipped to thwart zero-day or evolutionary malware. Obfuscation techniques allow malware to either evade detection or force the adoption of conservative blocking policies when the IDS is in doubt, resulting in performance loss.

**Solution** : A new dynamic reconfiguration framework offers a rich array of active defenses in response to anomalous traffic. Our system enables reconfiguration of network topologies, allowing sandboxed analysis to improve prediction accuracy without blocking legitimate traffic. Component level reconfiguration further reduces application exposure by increasing the complexity in navigating through a program's attack surface.

## Approach

- A network programmable device (NPD) translates network conversations into feature vectors so that raw traffic can be represented as indicator data.
- The NPD deploys northbound applications to digest indicator vectors in order to make predictions on the conversations' integrity.
- A *dynamic reconfiguration* API manipulates network flows having low-confidence predictions in order to safely generate more features, validate predictions and, if warranted, trigger active defenses.
- The API supports reconfiguration tactics that mirror, redirect, or rebuild network pathways; interchange components; and alert applications to mitigate attacks.
- These mechanisms protect infrastructure and enhance behavioral classification of malware while expending the resources of an attacker.




## Results

- Successful development of learning models that identify specific classes of malware such as ransomware.
- Expansion of active defense capabilities at network level in addition to existing reconfiguration technologies deployed at application and system levels.
- Future work to open-source framework and integrate solution into compatible software-defined networking environments.

***Special thanks to***

Professor James M. Purtilo whose research is supported by Office of Naval Research under contract N000141612107

SEAM
software engineering @ maryland

seam.cs.umd.edu