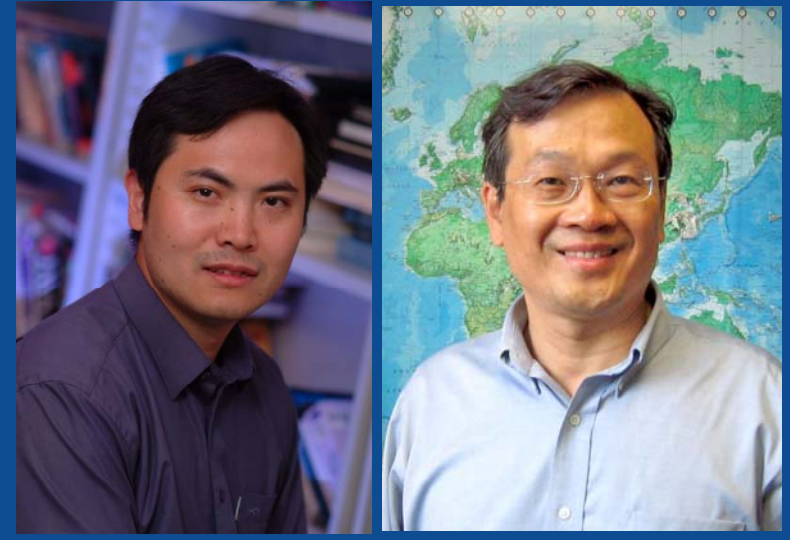


Router-Based Signature Generation for Zero-Day Polymorphic Worms

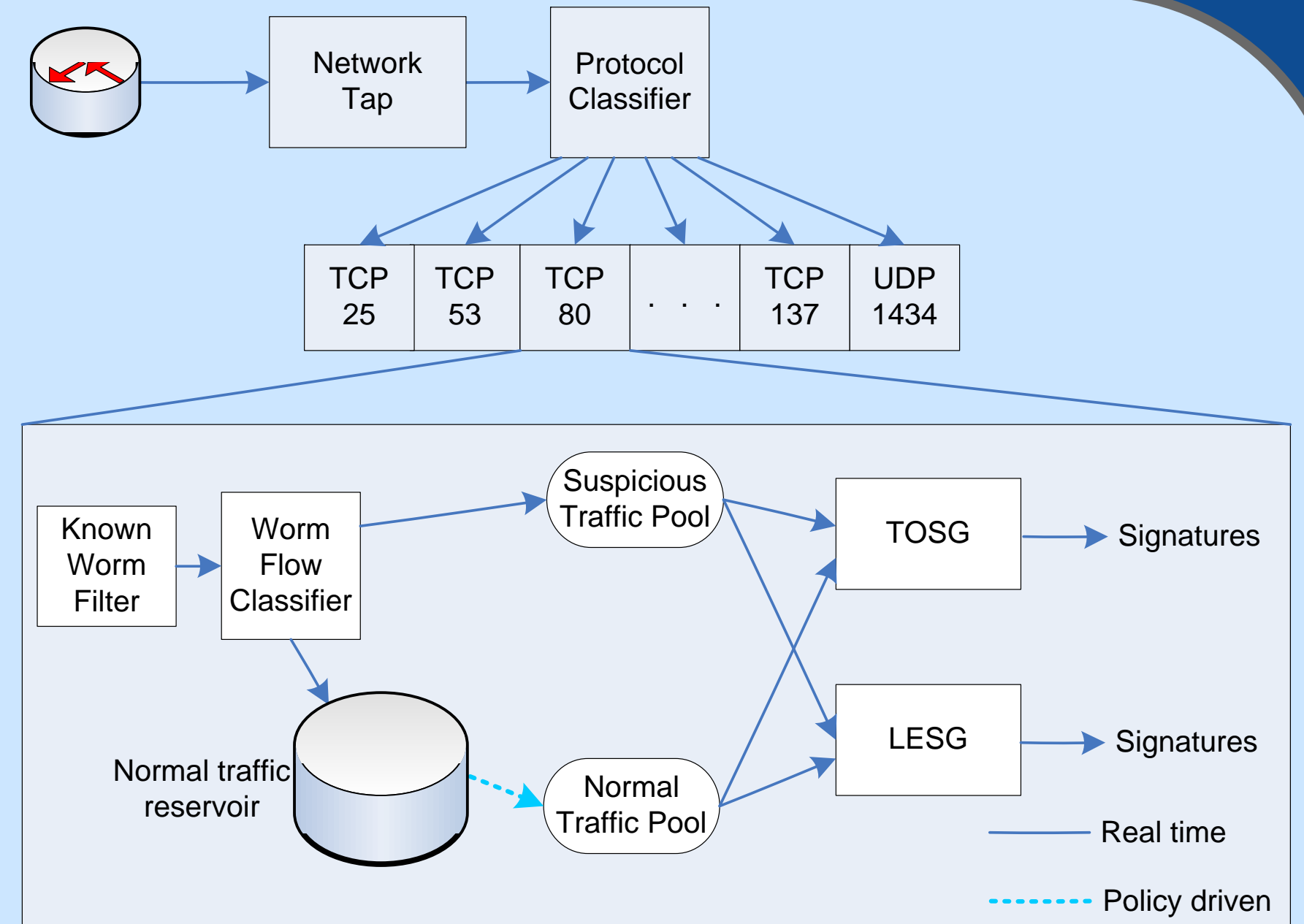
Yan Chen and Ming-Yang Kao

<http://list.cs.northwestern.edu/> CNS-0627751



Problem

Polymorphic worms or polymorphic botnet probes are serious threats to the Internet security. To generate the worm signatures on network level with adversaries is a hard problem.



System Diagram

Solutions

At earlier stage of worm propagation only limited worm samples can be observed. Network gateway is a better vantage point for detection.

We propose two network level signature generators with provable attack resilience guarantee under certain assumptions. The system can be deployed on network (or honeynet) gateways to thwart worms.

Approach and Impact

New approach

- Token-based Signature Generator (TOSG)
- Length-based Signature Generator (LESG)

Research Impact

- Fast response to zero day polymorphic worms in their earlier phases
- Provable attack resilience

Technique Details

- TOSG: Based on a realistic model of analyzing the uniqueness of invariant byte content of polymorphic worms, we propose a greedy based algorithm which is fast and with analytical attack resilience bound. [IEEE Symposium on Security and Privacy 2006]
- LESG: Based on the observation that buffer overflow is one of the most common vulnerability types exploited remotely and certain protocol fields might map to the vulnerable buffer. We propose a three-step algorithm to generate the protocol field length signatures with analytical attack resilience bound. [IEEE International Conference on Network Protocols (ICNP) 2007]

Outcome

Through simulations with real world worms, polymorphic engines and real world traffic, we demonstrated both signature generators are accurate, fast, noise-tolerant and attack-resilient.

TOSG (also known as Hamsa system) code released to research community upon several requests after being published.