Using Petri nets to model subtle network interactions to improve Intrusion Detection

Divyanshu Parikh, BS Computer Science Student
Mentors: Benjamin Mixon-Baca, PhD Student, Jedidiah R. Crandall, Associate Professor

School of Computing and Augmented Intelligence

QR CODE

Introduction

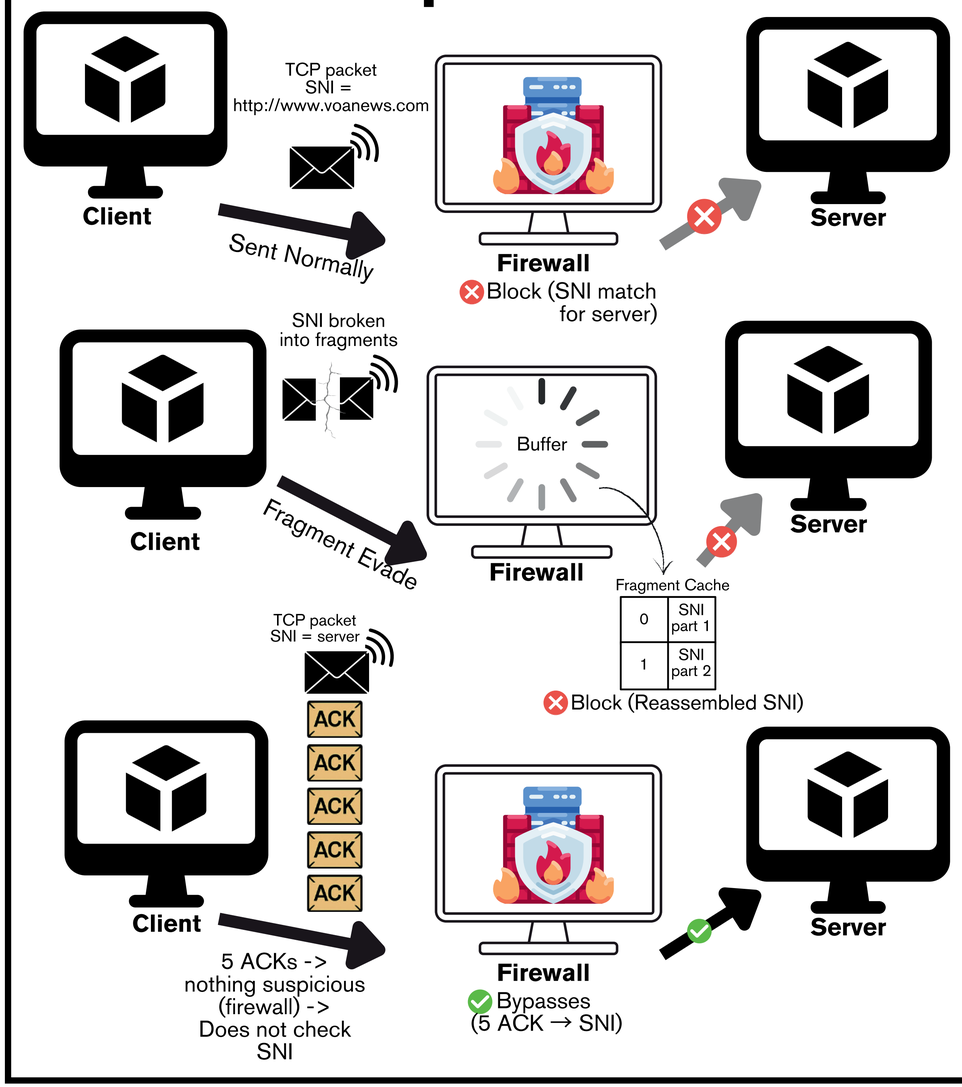
Modern firewalls rely on passive traffic monitoring to spot threats.

Unfortunately, after 30years, subtle packet-level behaviors remain a means for attackers to evade detection.

This research aims to use Petri nets to model the dynamic interplay of network packets, firewalls and VPNs, down from looking at "byte patterns", to capture the complete behavior, and reveal anomalies that would normally require exponential resources to identify.

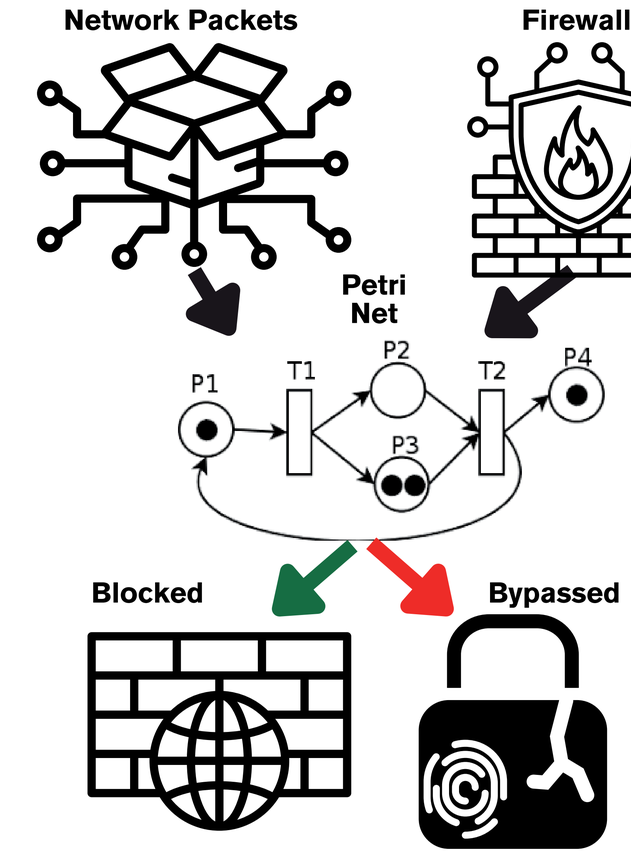
Identifying such anomalies has broad security implications from malware propagation to censoring circumvention.

Experiments



Network Censorship

By dissecting the techniques attackers use to slip past today's detection systems and encoding those tactics in Petri-net models, we build a framework for designing networks that resist both malware intrusions and censorship controls.



FURI

Ira A. Fulton Schools of Engineering
Arizona State University