Next Generation Firewalls for Dynamic Coalitions

Saritha Arunkumar (IBM Research UK), **Christian Makaya** (IBM Research USA), **Elisa Bertino** (Purdue),
Erisa Karafili (Imperial College), **Emil Lupu** (Imperial College), **Chris Williams** (DSTL), **Stephen Pipes** (IBM UK)

Overview

- Firewalls (FW) are used to control incoming and outgoing network traffic based on security rules
- Firewalls have evolved from being a simple filtering device to operate in conjunction with intrusion detection and prevention systems (IDS/IPS)
- Firewall rules are predefined and need to be updated to consider new requirements
- IDS/IPS used to monitor policy violations and prevent network vulnerability

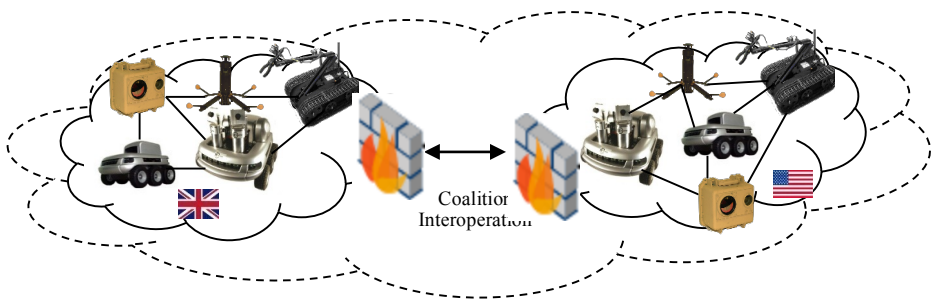
There is a need of new generation of firewalls that is able to quickly adapt to changes without requiring HIL

Challenges in Coalition Networks

- Current IDS/IPS/FW are often static and require manual configuration. Signature rules updated from remote repository
- Coalition members require secure and resilient information infrastructure that conforms to their policies
- Matching criteria in FW/IDS/IPS are based on regular expression against IP packet headers

Approach for Next Generation Firewalls

- Use ML/AI techniques to allow IDS/IPS and FW to generate policy rules for new and unseen traffic based on insights from history
- Firewall (Inference Management Firewall) auto-generate its own policies based on the context and changes in the network
- Use IDS/IPS to extract insights from the monitored traffic to be used to enhance and update firewall rules dynamically
- Use *Generative Policy* approach for automatic policy generation rather than relying on centralized policy management



Salient Future

- Design a framework to IDS/IPS that can be used to enhance and update firewall rules dynamically
- Generative policy model to enhance firewall and IDS/IPS operations
- Firewall automatically adapts its behavior when it encounters malicious traffic that does not conform to an existing threat patterns

Future Work

- Distributed firewall rules analysis framework to analyse and get insights from historical decisions
- Design policy template to enable autonomous generation of firewall rules
- Defense mechanisms to avoid the autonomous behavior of FW to be exploited for new attacks

Distributed Analytics and Information Science
International Technology Alliance
Annual Fall Meeting, September 2017