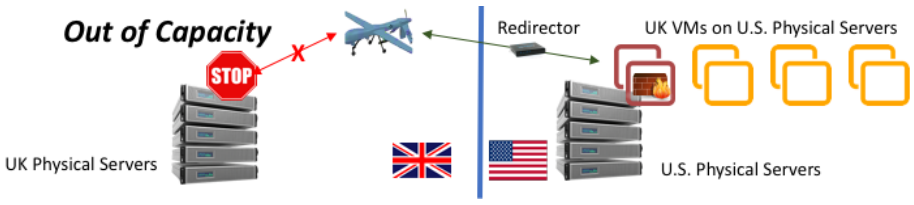
Generative Policy Architecture for Access Control Use Case

Elisa Bertino (Purdue University), **Seraphin Calo** (IBM Research), **Christian Makaya** (IBM Research), **Dinesh Verma** (IBM Research), **Christopher Williams** (DSTL)

Scientific Challenge

- Allow systems to generate their own policies dynamically
- Operate in highly dynamic environments where manual configuration is infeasible
- Restrict the autonomy of device within reasonable bounds

Scenario



- UK and US forces conducting a joint coalition operation
- Both forces have physical servers at their base camps
- UK needs to launch mobile drones for a surveillance mission
- Drones need to be supported by computing infrastructure at base camp – provided by a set of virtual machines
- UK servers are fully utilized, leading to the UK requesting virtual machines on U.S. servers
- US has free capacity, and can launch UK Virtual Machines with auto-scaling for dynamic resource control
- UK has no human administrator available to manage the VMs on U.S. servers

Key Innovation

Concept of Interaction Graph coupled with Discovery & Policy Generation Grammar

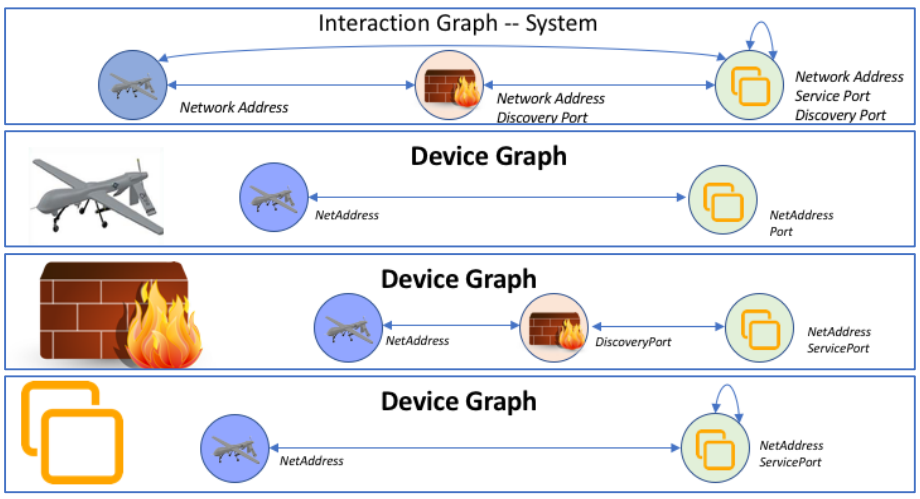
Generative Gammar for Demo

Start → **Default** | **Discovery** | **Access**
Default → **if** *Any Port & Any Address* **then** *Deny*
Access → **if** *Peer.NetAddress* == ***Y*** & *Peer.Port* = *Z* **then** *Allow*
Discovery → **if** *Peer.NetAddress* == ***RD*** & *Peer.Port* == ***SP*** **then** *Allow*
X = <*Role=VM, Attribute = DiscoveryPort*>
Y = <*Role = VM, Attribute=NetAddress*>
RD = <*redirector address*>, ***RD*** = <*redirector discovery port*>

Start → **Default**| **Discovery**| **Access**
Default → **if** *Any Port & Any Address* **then** *Deny*
Discovery → **if** *Local.Port* == ***D*** **then** *Allow*
Access → **if** *Mobile.NetAddress* == ***X*** & *VM.NetAddress* == ***Y***
& *VM.Port* = **Z** **then** *Allow*
D = <*Self, DiscoveryPort*>, ***X*** = <*Mobile, NetAddress*>,
Y = <*VM, NetAddress*>, ***Z*** = <*VM, Port*>

Start → **Default**| **Discovery**| **Access** | **Access**
Default → **if** *Any Port & Any Address* **then** *Deny*
Discovery → **if** *Local.Port* == ***D*** **then** *Allow*
Access → **if** *Peer.NetAddress* == ***X*** & *Local.Port* == **Y** **then** *Allow*
Access → **if** *Peer.NetAddress* == ***Z*** **then** *Allow*
D = <*Self, DiscoveryPort*>, ***X*** = <*Mobile, NetAddress*>
Y = <*Self, ServicePort*>, ***Z*** = <*VM, NetAddress*>

Interaction Graphs for Demo



Salient Features

- Automatic policy generation in dynamic systems – without need for a central configuration or policy server
- General Approach: Applicable to a variety of scenarios and policy types

Future Work

- Policy subset selection – based on mission goal and task
- Quantification of security risks with self-generation of policies
- Discovery schemes that work across variety of scenarios

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