Bohatei: Flexible and Elastic DDoS Defense

Seyed K. Fayaz, Yoshiaki Tobioka, Vyas Sekar, Michael Bailey

https://github.com/ddos-defense/bohatei
DDoS attacks are getting worse

High cost on victims
Increasing in number
Increasing in volume
Increasing in diversity

DDoS Attacks Cost $40,000 Per Hour
Incapsula, 11/12/2014

FBI WARNS OF INCREASE IN DDOS EXTORTION SCAMS
Threatpost, 7/31/2015

China Appears to Attack GitHub by Diverting Web Traffic
The New York Times, 3/30/2015

29% of Botnets Attack More than 50 Targets a Month
Imperva, 2015

The DDoS That Almost Broke the Internet
Cloudflare, 3/27/2013

Wave of 100Gbps 'mega' DDoS attacks hits record level in 2014
Techworld, 7/16/2014

NTP ATTACKS: Welcome to The Hockey Stick Era
Arbor Networks, 2/14/2014

Tsunami SYN Flood Attack
Radware, 10/7/2014
DDoS Defense Today:
Expensive Proprietary Hardware
Limitation: Fixed functionality

What if new types of attacks emerge?
Limitation: Fixed capacity

Attack vol. (Gbps)

Fixed capacity

$t_1$ $t_2$ $t_3$ $t_4$

time

Waste

Assets

Intranet
Limitation: Fixed location

- Additional traffic latency due to waypointing
- Routing hacks to enforce defense

![Diagram showing the concept of shortest path being obstructed by a fixed location.](image-url)
Need flexibility w.r.t. attack type
Need Flexibility w.r.t Attack Locations

Today:
  Hardware appliance res. footprint=240Gbps
Need Elasticity w.r.t. Attack Volume

Assets
Bohatei in a nutshell..

A practical ISP-scale system for Flexible and Elastic DDoS Defense via Software-Defined Networking (SDN) & Network Functions Virtualization (NFV)

→ React to 500 Gbps scale attacks in 1 min!
Outline

- Motivation
- Background on SDN/NFV
- Bohatei overview and challenges
- System design
- Implementation
- Evaluation
- Conclusions
Software-Defined Networking (SDN)

Centralized management + Open config APIs
Network Functions Virtualization (NFV)

Today: Standalone and Specialized

Proxy  Firewall  IDS/IPS  AppFilter

Commodity hardware
Why are SDN/NFV useful for DDoS defense?

Our Work: Bring these benefits to DDoS Defense
Outline

• Motivation
• Background on SDN/NFV
• Bohatei overview and challenges
• System design
• Implementation
• Evaluation
• Conclusions
Bohatei Vision:
Flexible + Elastic Defense via SDN/NFV

SDN/NFV Controller

attack traffic

VM

DC_1

DC_2

ISP

customer intranet
Bohatei Controller Workflow

Strategy layer

Resource management

Network orchestration

Predict attack pattern

Decide how many VMs, what types, where

Configure network to route traffic
Threat model: general, dynamic adversaries

- Targets one or more customers
- Attacker has a fixed “budget” w.r.t. total attack volume

```
do{
    Pick_Target()
    Pick_Attack_Type()
    Pick_Attack_Volume()
    Pick_Attack_Ingress()
    Observe_and_Adapt()
}
```
Bohatei Design Challenges

Strategy layer

Resource management

Network orchestration

Predict attack pattern

Decide how many VMs, what types, where

Configure network to route traffic

Resilient to adaptation?

Fast algorithms?

Scalable SDN?
Outline

• Motivation
• Background on SDN/NFV
• Bohatei overview and challenges
• System design
• Implementation
• Evaluation
• Conclusions
Naïve resource management is too slow!

Global optimization

- Compute/network resources
- Suspicious traffic predictions
- Defense library

Types, numbers, and locations of VMs? Routing decisions?

Takes hours to solve...
Our Approach: Hierarchical + Greedy

ISP-level Greedy

Compute/network resources

Suspicious traffic predictions

Defense library

How much traffic to DC_1

Per datacenter 1

Which VM slots in DC_1

...  

Which VM slots in DC_N

Per datacenter N

How much traffic to DC_N
A reactive, per-flow controller will be a new vulnerability
Idea: Proactive tag-based steering

Proactive per-VM tagging enables scaling
Dynamic adversaries can game the defense

Adversary’s goals:
1. Increase defense resource consumption
2. Succeed in delivering attack traffic

Simple prediction (e.g., prev. epoch, avg) can be gamed
Our approach: Online adaptation

• Metric of Success = “Regret minimization”
  → How worse than best static strategy in hindsight?

• Borrow idea from online algorithms:
  Follow the perturbed leader (FPL) strategy

• Intuition: Prediction = F (Obs. History + Random Noise)

• This provably minimizes the regret metric
Putting it together

Prediction strategy

Orchestration

Resource management

- Predicts volume of suspicious traffic of each attack type at each ingress
- Quantity, type, location of VMs
- Defense policy

launching VMs, traffic path set up

suspicious traffic spec.

suspicious traffic

attack traffic

customer intranet

DC1

ISP

DC2
Outline

• Motivation
• Background on SDN/NFV
• Bohatei overview and challenges
• System design
• Implementation
• Evaluation
• Conclusions
Defense policy library

- A defense graph per attack type
- Customized interconnection of defense modules
- Open source defense VMs

Example (SYN flood defense)

```
Analyze Srces:
  count
SYN – SYN/ACK per source
```

[Legitimate] → OK → [Legitimate]

[Unknown] → SYNPROXY

[Attack] → LOG

DROP
Implementation

Control Plane

Data Plane

resource manager  defense library ...

OpenDaylight

OpenFlow

FlowTags (Fayaz et al., NSDI’14)

Switches (OVS)

FlowTags-enabled defense VMs (e.g., Snort)

KVM

13 20-core Intel Xeon machines

https://github.com/ddos-defense/bohatei
Outline

• Motivation
• Background on SDN/NFV
• Bohatei overview and challenges
• System design
• Implementation
• Evaluation
• Conclusions
Evaluation questions

• Does Bohatei respond to attacks rapidly?

• Can Bohatei handle ≈500 Gbps attacks?

• Can Bohatei successfully cope with dynamic adversaries?
Responsiveness

- Hierarchical resource management:
  - A few milliseconds (vs. hours)
  - Optimality gap < 1%

Bohatei restores performance of benign traffic \(\approx 1\) min.
Scalability: Forwarding table size

Per-VM tagging cuts #rules by 3-4 orders of magnitude.
Proactive setup reduces time by 3-4 orders of magnitude.
Adversarial resilience

Bohatei online adaptation strategy minimizes regret.
Conclusions

• DDoS defense today: Expensive, Inflexible, and Inelastic

• Bohatei: SDN/NFV for flexible and elastic DDoS defense

• Key Challenges: Responsiveness, scalability, resilience

• Main solution ideas:
  – Hierarchical resource management
  – Proactive, tag-based orchestration
  – Online adaptation strategy

• Scalable + Can react to very large attacks quickly!

• Ideas may be applicable to other security problems