Jaqen: A High-Performance Switch-Native Approach for Detecting and Mitigating Volumetric DDoS Attacks with Programmable Switches

Alan Zaoxing Liu

Joint work with Hun Namkung, Georgios Nikolaidis, Jeongkeun Lee, Changhoon Kim, Xin Jin, Vladimir Braverman, Minlan Yu, Vyas Sekar
DDoS attacks are getting worse

• Increasing in \textit{volume}
• Increasing in \textit{diversity}
• Increasing in \textit{cost to defend the attacks}

Surge in DDoS attacks targeting education and academic sector

\textbf{CISA Warns of Increased DDoS Attacks}
\begin{flushleft}
Security Experts Say Remote Workforce, Online Learning Create Opportunities
\end{flushleft}
\begin{flushright}
9/10/2020 U.S. CISA
\end{flushright}

\textbf{DDoS Attacks Increase by 151\% in First Half of 2020}
\begin{flushright}
9/15/2020 Infosecurity
\end{flushright}

\textbf{European ISPs report mysterious wave of DDoS attacks}
\begin{flushright}
9/3/2020 ZDNet
\end{flushright}
Requirements for DDoS Defense

• Performance:
  handle *large volumes* with *low latency*

• Flexibility:
  handle *diverse attack vectors*

• Cost-effectiveness:
  handle attacks with *low capital and operational costs*
Current DDoS Solutions: Middleboxes

Attacker

Out-of-band Detection

Slow or inaccurate

Server Clusters

Inflexible, high cost

low performance, high cost

Victims

Hardware appliance

Can we do better?

E.g., 100 servers for 1000Gbps mitigation. [Security’15]
Trend: Network devices are more programmable

- Programmable Switch
- Switch ASICs

Increasing in-network programmability in ISP networks

- High line-rate performance (e.g., Tbps)
- High programmability using high-level language (e.g., P4)
- Cost effective with similar cost as traditional switches
Current DDoS Solutions: Switches for Scrubbing

- Scrubbing Center with programmable switches
  [Poseidon, NDSS'20]

- Still need out-of-band detection.
- Scrubbing approach adds large latency.
- Unscalable mitigation functions (e.g., Server-like SYN Proxy)
Opportunity: Programmable ISP Networks for DDoS Defense

Internet Service Provider (ISP)

- Near the source or victim of the attacks
- Provide defense-as-a-service to the clients
Can we design ISP-based DDoS defense that fully leverages programmable switches?
Jaqen: Switch-Native DDoS Defense for ISP

- Detection + Mitigation integrated “switch-native” solution.
- Designed for ISP networks where there are a LOT of switches.
Jaqen’s Full Stack Design

1. Broad-Spectrum Detection
2. Dynamic Resource Allocation
3. Fast On-demand Mitigation

Victims
Broad-Spectrum and Always-On Detection

- A wide-spectrum detection of volumetric attacks.
- Compact design with future-proof universal sketches.
- Detection metric API: Query (proto, func, mode, freq)

- Attack types
- Attack volumes
- Unidentified

Packet Parser → Universal Sketches → Attack Signatures

e.g., elephant flows, distinct flows, heavy sources, entropy
Fast On-Demand Mitigation

Detection results

Available resources

Quick resource allocation
(Optimization solver)

Mitigation Modules:
M1, M2, M3, ...

• Cannot afford preloading all possible mitigation modules.
Switch-Optimized Mitigation Library

Best-practice mitigation

- SYN Cookie/proxy [BSDC’02, RFC4987]
- Block-List [WDFIA’07]
- Allow-List [WDFIA’07]
- ICMP block
- DNS filter

...\n
Switch-optimized library

- Sketches
  - Bloom filters
  - Counting bloom filters
  - SYN Proxy with filters
  - Exact-match table
  - Rater limiter

...\n
Mitigation API

- RateLimit(identity, rate)
- ExactBlockList(identity, size)
- ExactAllowList(identity, size)
- ApproxBlockList(identity, config)
- ApproxAllowList(identity, config)
- ActionAndTest(action, List(predicate))
- HeaderHashAndTest(identity, action)
- UnmatchAndAction(action, List(predicate))
- KVStore(key, value, size)
- ReportCtr(identity, type)
- Recirculate(identity, type)

- Preserve $O(10 \text{ Million})$ legitimate connections with $O(10 \text{ MB})$ on-switch memory.
- Support mitigation strategies on 21 attacks.
Switch-Native SYN Proxy

Client -> SYN Proxy -> Server
- SYN
- SYN-ACK w/ cookie
- ACK w/ cookie+1
- Seq. # adjustment

SYN Proxy [NDSS’20]

Client -> SYN Proxy -> Server
- SYN Cookie & conn table
- Verify cookie
- SYN
- SYN-ACK
- ACK
- Per-conn state!

Jaqen SYN Proxy

Client -> Switch -> Server
- SYN
- Error SYN-ACK w/ cookie
- RST w/ cookie
- Verify cookie +allowlist
- Cookie w/o states
- SYN
- SYN-ACK
- ACK
- Jaqen SYN Proxy
Evaluation – Single Attack

- Comparison with Poseidon [NDSS'20].
- Single Intel Tofino switch.
- 40Gbps attack traffic with 2M legitimate TCP connections.

<table>
<thead>
<tr>
<th>Defense (40G)</th>
<th>Poseidon (FPR / FNR)</th>
<th>Jaqen (FPR / FNR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN proxy</td>
<td>2M, 25.2% / 1.3%</td>
<td>2M, 0.0% / 1.3%</td>
</tr>
<tr>
<td>DNS/NTP defense</td>
<td>2M, 1.2% / 3.7%</td>
<td>2M, 0.7% / 3.1%</td>
</tr>
</tbody>
</table>

- Mitigation with probabilistic data structures is more scalable.
Evaluation – Dynamic Attacks

- 6 volumetric attacks (SYN, ICMP, UDP, DNS, NTP, Memcached)
- 380Gbps total volume, 3.2 Tbps Intel Tofino switch

High detection accuracy and high mitigation effectiveness
Conclusions

• ISP DDoS defense compromises performance, flexibility and cost-effectiveness.

• Appealing programmable network devices (e.g., programmable switches)
  * High line-rate packet processing
  * Full packet programmability with low cost

• Jaqen: Switch-native DDoS defense for ISP networks
  * Broad-spectrum detection integrated with on-demand mitigation
  * Network-wide resource management
  * Switch-optimized library for best practice mitigation

Contact: Alan Liu
zaoxing@bu.edu
http://zaoxing.github.io/