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

Aug 2021

30th USENIX Security Symposium

25 citations

جاکن: راهکاری با کارایی بالا سوییچ‌پومی برای شناسایی و رفع تهدید حملات منع‌خدمت توزیع شده حجیم با استفاده از سوییچ‌های برنامه‌پذیر

ISP ها به دلایل زیر می‌توانند نقطه خوبی برای مقابله با حملات باشند:

- جریان‌های زیاد عبوری که منجر به وقوع انواع مختلف حملات خواهد شد. راهکارهایی مثل پوسایدن که مخصوص scrubbing center ها بودند در اینجا کاربرد نخواهند داشت.
- ترافیک کاربران را هدایت می‌کند اما به اطلاعات سطح لایه کاربرد دسترسی ندارد (نکته مثبت)، لذا محرمانگی کاربران حفظ می‌شود و برروی تجربه کاربران عادی تاثیری نمی‌گذارد.

از طرفی راهکاری که می‌خواهیم طرح کنیم باید ویژگی‌های زیر را داشته‌باشد؛

- اضافه نکردن دستگاه‌های اضافی و تنها با استفاده از سوییچ‌ها پیاده شود.
- مفهوم مرکزی‌بودن ISP ها را درنظر داشته‌باشد.

روش‌های قدیمی از سخت افزارهای مخصوص استفاده می‌کردند. راهکار ما باید طیف وسیعی از توابع تشخیص و مقابله با حملات را روی سخت افزارهای محدود سوییچ‌های barefoot پیاده سازی کند. روش ما همچنین باید سازگار پذیر با حملات در حال تغییر (دینامیک و هیبرید) باشد. روشهای قبلی که قسمت شناسایی را حل شده در نظر می‌گرفتند (یا یک بخش جدا برای مانیتور داشتند که باعث ایجاد تاخیر می‌شد) . یا تنها از سوییچ‌ها به عنوان شتاب‌دهنده استفاده می‌کردند، کاربرد ندارند. از یک API استفاده می‌کنیم تا استراتژی‌های دفاعی را تغییر دهیم. همچنین یک مدیر شبکه داریم که به صورت بهینه ای منابع تشخیص و مقابله را با تغییر حملات، تغییر منابع سوییچ‌ها، تغییر حجم ترافیک تخصیص می‌دهد. در ابتدای کار ماژولهای تشخیص را به صورت کامل روی سوییچ‌ها پیاده کرده ایم اما ماژولهای رفع تهدید در صورت نیاز در نقاط موردنیاز فعال خواهند شد.

معماری سوییچ‌ها:

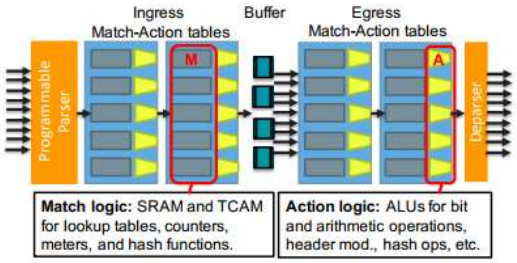

Figure 1: Protocol Independent Switch Architecture.

figurable match-action tables. Developers can program the packet parser to support user-defined packet headers, specify the matching fields and types (e.g., exact, range, and ternary matching), and configure supported actions (e.g., CRC hash, header field modification, register read/write via arithmetic logic unit (ALU), arithmetic operations using , and metering). We refer readers to §7 for more details.

بروی یک چیپ ASIC سوار هست و شامل یک parser برنامه پذیر و چندین جدول MA [1]تنظیم‌پذیر می‌باشد.

مدل درنظرگرفته‌شده برای مهاجم: حملات در لایه در لایه کاربرد و link flood ها بررسی نمی‌شوند. همچنین تنها حملات منع خدمت حجیم بررسی خواهدشد. البته می‌توان عملکرد سوییچ را برای شناسایی حملات غیرحجیم (مراجعه شود به مرجع) برنامه نویسی کرد. همچنین فرض می‌شود سوییچ های برنامه پذیر غیرقابل حمله توسط مهاجم هستند.

ISPها می‌توانند جاکن را همانند یک سرویس در کنار سرویس‌های دیگر پیاده‌سازی کنند.

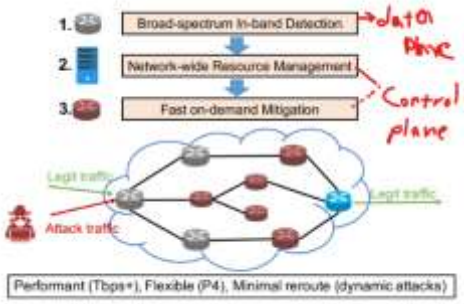

Figure 2: Overview of Jaqen

[1] Match-Action table

طریقه کار:

- تشخیص: از تنها یک الگوریتم استفاده می‌کند. از universal sketch برای شناسایی و ردیابی و تخمین متریکهای تابه‌حال دیده نشده (بدون دانش قبلی) احتمالی مربوط به حمله استفاده می‌کند. برخی حملات که متریک‌هاشون داده های رمز شده بودند یا برای شناسایی نیاز به محتوای کامل پیلود بسته‌ها را شناسایی نمی‌کنند. از دو لایه داده و کنترلر تشکیل شده است. لایه داده که شامل همین انگاره ها[2]ست که می‌تواند توسط کنترلر دریافت شوند. لایه کنترلر یک API دارد که با استفاده از آن می‌تواند sketch ها (multiple universal sketch instances and a single signature detector) را تنظیم کند، متریک های مختلف را کویری (Query(proto,func,mode,freq)) بزند و دریافت کند و بر اساس آنها تصمیم بگیرد. با استفاده از sketch counter های مربوط به حمله که از لایه سوییچ گرفته است حجم احتمالی هر نوع حمله را تخمین می‌زند.

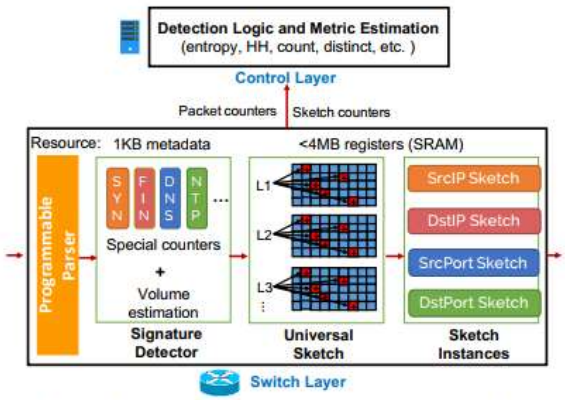

Figure 3: Switch detection design w/ universal sketches.

- رفع تهدید: از سه کامپوننت تشکیل شده‌است که باهم در ارتباط هستند. هر بخش نیز توابع‌اش بر مبنای API پیاده‌سازی شده‌است:

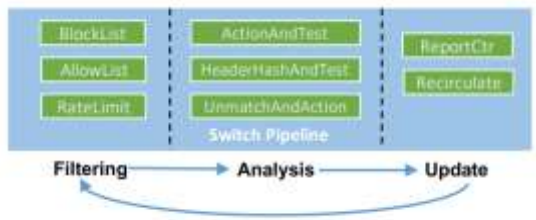

Figure 5: Abstraction of mitigation strategies.

  - فیلتر: شامل سه اقدام drop,allow,rate limit traffic می‌باشد. دارای پنج تا تابع می باشد:
    - Exact Allow/Block List (identity,size)
    - Approx Allow/Block List (identity,config) : شبیه Exac ، اما قانونهای بیشتری می‌شود نوشت. از Blocked Bloom Filter در Allow Lsit استفاده می‌شود که تنها مشکل آن برای مثال False Posite ها در Allow list هست. لذا به کاربران عادی صدمه نمی‌زند.
    - RateLimit(identity,rate)

[2] الگوریتم های تقریبی که مشخصه‌های آماری شبکه را می توانند تخمین بزنند.

- آنالیز: اگر در مرحله قبلی ترافیک دورانداخته نشده بود یا اجازه عبور داده نشده بود، ترافیک بد را شناسایی می‌کند. شامل چهارتا تابع می‌باشد:
  - Action&Test(action,list[predicate]) : just drop & forward
  - HeadHash&Test(identity,action)
  - UnmatchAndAction(list[predicate],action:drop&forward+insert and delete)
  - KVStore(key,value,size)
- آپدیت: جداول موجود در بخش فیلتر را در صورت نیاز بر اساس ترافیک‌های برچسب گذاری‌شده مرحله قبل بروز می‌کند تا از ورود ترافیک‌های مربوط به آن جریان جلوگیری کند (هر موقع ضرورت داشت این کار را انجام می‌دهد تا از بروز تاخیر جلوگیری کند). شامل توابع زیر است:
  - ReportCtr(identity,type): یکی از سه جدول allow,drop ویا rate limit را آپدیت می‌کند.
  - Recirculate(identiy,type): همانند متود بالا با این تفاوت که پیغام از کنترلر عبور نمی‌کند.

با استفاده از زبان p4 می‌توان استراتژی‌های جدیدی تعریف کرد.

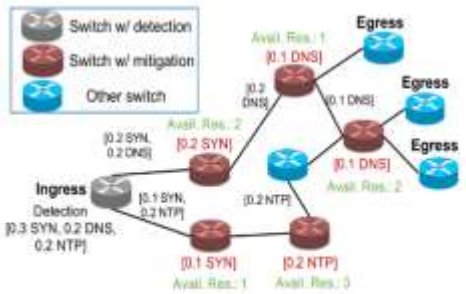

Figure 8: Example network-wide resource management on a simplified Claranet topology [71].

مقابله با پویایی توسط یک بخش مدیریت: این بخش وظیفه محاسبه تخصیص منابع[3] جدید برای هدایت ترافیک به سمت آن سوییچ‌ها[4] با درنظرگرفتن (ماژولهای تشخیص و رفع تهدید را به آن سمت هدایت می‌کند) حداقل هزینه ممکن برای مقابله را عهده‌دار می‌باشد. این کار را به یک مسئله MIP تبدیل می‌کند و راه‌حلی برای آن پیدا می‌کند. از روش BFS برای تخصیص استفاده می‌کند که برای ISP های بزرگ حداکثر ۱۵ ثانیه تاخیر خواهد داشت.فرض می‌شود که ISP یک کنترلر مرکزی دارد که تمامی تصمیمات میسریابی و مدیریت ترافیک را بر عهده دارد (همانند SDN که در آن یک کنترلر مجازی مرکزی هست که تمامی تصمیمات مسیریابی تمام جریانهای موجود در شبکه را می‌گیرد) . این کنترلر تمام اطلاعات شبکه را aggregate کرده است (میزان pipeline,resource هر سوییچ-توجه شود که هر سوییچ شامل چندین خط pipeline و چندین ماژول هست-).

[3] Resource allocation
[4] Traffic distribution

معایب بالقوه: جاکن برای اقدام متقابل و واکنش (مهاجم سریع می تونه در اون چند ثانیه تکنیک خودرا عوض کند) نیاز به چند ثانیه زمان خواهدداشت. همچنین جاکن محتوای کامل بسته‌ها (محتوای داده‌ای) را پایش نمی‌کند.

پیاده‌سازی بستر[5]: بر روی barefoot switch با زبان p4 پیاده می‌شود. بخش کنترلر مرکزی (همانی که ترافیک را هدایت می‌کند) را نیز با استفاده از پایتون راپیاده سازی کرده‌ایم (الگوریتم BFS).

ارزیابی: ترافیک ۶.۵ ترابیت بر ثانیه با یک سوییچ و ۱۰ سرور که از یکی برای ایجاد ترافیک حمله و دیگران به عنوان مقتول استفاده می‌شود. نصب DPDK بر روی همه سرورها صورت می‌گیرد. معیارهایی که اندازه می‌گیرد: درستی تشخیص ترافیک (با netflow هم مقایسه می‌کند) ،FNR،FPR ،reaction time. با روش پوسایدن هم مقایسه‌ای انجام می‌دهد که در ترافیک ۴۰ گیگ با ۲ میلیون ارتباط[6]، تاخیری ندارند اما مثبت کاذب و منفی کاذب پوسایدن بالا می‌رود.

[5] Testbed
[6] connection

ارتباط با موضوع:

- دسته بندی حملات منع خدمت
- {۷۷} و {۷۸} ترافیک واقعی برای تست
- {۷۹} ابزاری برای تولید ترافیک‌های DDoS حجیم از نوع ICMP/SYN flood
- Mininet
- {۸۳} local DNS