Network Monitoring & Bro

Michel Laterman
Our setup

- We have a monitor set up that receives a mirror from the edge routers
- Monitor uses an ENDACE DAG 8.1SX card (10Gbps) & Bro to record connection level info about network usage
  - Can’t simply do full packet captures for everything because of size and ethics
- Throughput logging tool written in C
Monitor receives a full mirror of all traffic that goes to/from the Internet

Around 2 Gbps Peak inbound (mostly TCP)

Almost constant 0.5 Gpbs UDP (outbound)
  ◦ Used to be 1–2 Gbps

about 22 TB of traffic a day
  ◦ 50 GB (compressed) logs generated by Bro per day
  ◦ Bro Collects and rotates logs hourly
  ◦ Another program collects throughput information at 1 min intervals
Sample Weekly Throughput

U of C Network Traffic Breakdown 2015

Traffic Volume (Gbps)

Outbound

Other
TCP
UDP
ESP
ICMP

Sun, Mar 15  Mon, Mar 16  Tue, Mar 17  Wed, Mar 18  Thu, Mar 19  Fri, Mar 20  Sat, Mar 21
Strange Traffic

Dec 16, 2014

Total Throughput

- Total
- TCP
- UDP

Throughput (Gbps)

Time

Dec 16, 2014
What is our Traffic?

- TCP Traffic mostly comes from ports 80 & 443
  - Expected behavior
- We used small pcap traces to find out what was happening with out UDP traffic
  - Lots of packets from port 123 (NTP) coming out of campus (about 60% of UDP traffic)
    - Unpatched servers on campus being used in a DDoS
  - Lots of BitTorrent peers connecting in the trace (about %30 of UDP traffic)
    - 23k peers connecting at 4am on a Sunday…
‘Other’ Traffic
- ‘Other’ traffic is non-IP or IP traffic that does not have a listed protocol.
  - ARP, GRE, …

ESP traffic
- Second largest non-udp, non-tcp protocol

ICMP
- Can see all ICMP activity in Bro’s Connection log
  - We found a server on campus scanning the Internet
  - We can see many computers scanning the campus
    - Most are from other Academic institutions…
**Introduction to Bro**

- **What is Bro?**
  - “Bro is a passive, open-source network traffic analyzer. It is primarily a security monitor that inspects all traffic on a link in depth for signs of suspicious activity. More generally, however, Bro supports a wide range of traffic analysis tasks even outside of the security domain, including performance measurements and helping with trouble-shooting”

- **Bro is not a standard IDS**
  - More capable than just signature detection

- **Extensive set of logs**
  - Turing complete event based scripting language that can be used to analyze traffic
Architecture

- Bro monitors a network connection and generates events based on packets that it sees.
- Events are evaluated by a set of scripts and actions such as raising notifications or logging may be taken.
Bro uses analysis trees when decoding protocols.

Bro does not strictly rule that all TCP connections on port 80 are HTTP – but it starts with that assumption.

PIA – Protocol Identifier analyzer

Figure 1: Example analyzer trees.
Signature & Intel Frameworks

- Standard IDS signature detection possible with signature framework
  - Not the preferred tool
  - We use it to detect bittorrent over UDP

- Intelligence Framework
  - Consume data from incident reports
    - “Data in the Intelligence Framework is the atomic piece of intelligence such as an IP address or an e-mail address along with a suite of metadata about it such as a freeform source field, a freeform descriptive field and a URL which might lead to more information about the specific item”
- DAG card is capable of splitting the incoming stream (and steering)
- We mirror the stream from the router fully onto 2 streams, and have 24 substreams to Bro workers
Our Usage

- Our monitor has libpcap compiled with DAG support; Bro runs on top of that
- Hourly log rotation handled by broctl
- 24 workers, 4 proxies
  - Found this to not crash
- Backups to group fileserver daily with rsync
  - Fileserver backs up to west grid daily...
- Mostly vanilla installation: Log extra info about HTTP requests (req/resp length & duration)
  - Capture loss logging enabled
  - Bruteforce detection included
- BitTorrent uTP detection script deployed
- logging packet inter–arrival times for HTTP & SSL Connections (ports 80 & 443)
What are we looking for?

- **Anomalies:**
  - Server makes a few million SSL connections to a server we never heard about…
  - SSH attacks
  - ICMP scanning
  - Strange DNS activity…
- **Web traffic breakdown**
  - Resp. Codes, methods, domains, content-type,…
- **HTTPS Breakdown**
  - Server name, bytes transferred, connection duration, …
- **Video Traffic**
  - I’m looking at Twitch & Netflix and trying Youtube…
Event based language.
- `new_conn(c:connection)`
- `http_event(c:connection, event_type:string, detail_string)`
- `http_reply(c:connection,version:string, code:count, reason:string)`

Frameworks allow other actions – i.e. logging, notification, summarization, etc.
Logging

- By default Bro logs as plain text
  - If Bro is ran using broctl, logs are rotated and zipped
- Writer for sqlite available
- Writer for elasticsearch available
- Old writer for DataSeries (binary format) available

- Our monitor uses plain text logs
How do I handle 50GB/day?
  ◦ Poorly (I’m getting better)

First attempt was with Python
  ◦ First iteration wrote my own wrapper for records
    • Reading a 1 hour log took ~ 45 min
    • Don’t do this
  ◦ Second iteration switched to use Pandas library
    • 3–4 min read per log
    • Load an hour’s logs, analyze, repeat
    • 3.5 hours to analyze 1 day

Switched to using bash (grep+awk)
  ◦ 1.5–.175 hours to analyze a day
  ◦ Low(ish) memory usage (~8GB max, 24 GB cached).
  ◦ Easy to utilize more processors.
Related Work

Vern Paxson

*Bro: A System for Detecting Network Intruders in Real-Time*


H. Dreger, A. Feldmann, M. Mai, V. Paxson, R. Sommer

Dynamic Application-Layer Protocol Analysis For Network Intrusion Detection

Proc. USENIX Security Symposium, 2006

- [www.bro.org](http://www.bro.org)