DDoS Detection and Alerting

Daniel Romão  Niels van Dijkhuizen
DDoS attacks are commonly seen in the SURFnet network
- Mostly flooding attacks
- Customers are heavily affected and complain

These attacks are cheap and easily performed
BOOTERS / DDOSERS / STRESSERS

DON'T MAKE ME DDOS YOU

I HAVE JAYS BOOTER 5.0!
What does SURFnet currently use?
- Fixed threshold alerting
- IP fragmentation alerting
- BGP off-ramping and traffic washing

Can we make it better?
“Can we derive DDoS mitigation rules from the available production data in near real-time in order to alert and mitigate?”

- What kind of DDoS attacks can we detect?
- Can we detect them in near real-time?
- Can we extract enough information for mitigation?
WHAT WE PROPOSED
1. Collect one week NetFlow data
   - One on hundred sampling

2. Filter interesting application protocols
   - 53/udp (DNS), 123/udp (NTP), 80/tcp (HTTP), ...

3. Categorize traffic by behavior

4. Create baselines
   - Application protocols
   - Rest of the traffic (icmp, tcp, udp)
MODEL
FINDING NEW ANOMALIES

 UDП Flows

 Residual/Non-profiled UDП Flows

 Days of the week

 Number of Flows

 Resulting Flows

 Days of the week

 Number of Flows
Correlations:
- Bytes per packet
- Source – Destination ratios (symmetry)

Categories identified:
- Regular traffic without noise (e.g. HTTP/TCP)
- Regular traffic with noise (e.g. DNS/UDP)
- Non-regular traffic (e.g. NTP/UDP)
EXAMPLE OF BEHAVIORS

Flows for 53/udp

Flows for 123/udp

Days of the week

Days of the week
Smoothing: (friedman)

IQR rule for outliers:

Smoothing + offset:
For the other categories our statistical analysis was not as effective

- Traffic without noise -> baseline but hand-picked offset
- Non-regular traffic -> threshold
OUR PROTOTYPE

- NfSen plugin written in Perl and HTML/PHP
  - Run every five minutes
  - Run-time: 10 seconds
- Baselines and configuration stored in a SQLite database
- Adaptive baseline
  - Weighting value
- E-mail alerting

Subject: Dythraoth: Packetsize is too big for destination traffic on 'ssdp_udp'.
From: student@surfnet.nl
Date: 01/31/2014 07:31 PM
To: student@surfnet.nl

Anomalies detected: - threshold dstflows: 272 > 150
What kind of DDoS attacks can we detect?
- We can detect anomalies based on high volume. However...
- Verified for profiled application protocols and rest.
- Due to constraints, we didn’t dive into low-rate anomalies.

Can we detect them in near real-time?
- Yes, within a 5 minutes interval (or even faster)

Can we extract enough information for mitigation?
- No, but we expect that to be possible with further development of the plugin
FUTURE WORK

- Automate analysis
- Gather more information to detect the type of the anomaly
- Make the model distributed
- Integration with a mitigation system
Cool, right?

THANK YOU!