Privacy-Aware Intrusion Detection in High-Speed Backbone Networks - Design and Prototypical Implementation of a Multi-Layered NIDS

Authors: Mario Golling, Robert Koch, Gabi Dreo Rodosek

Speaker: Marcus Knüpfer
Agenda

- Insight into the Global Threat Landscape
  - Service Provider Threats
  - Attack Characteristics

- Existing Approaches
  - Flow Based Intrusion Detection
  - Shortcomings

- Multi-Layered NIDS Architecture
  - Overview and Implementation
  - Evaluation Setting
  - Evaluation Results

- Conclusion
Insight into the Global Threat Landscape

- Internet Insecurity remains a world-wide Problem

- Different Perception of Threats depending on:
  - Private Network
  - Corporate Network
  - Hosting Providers and Data Centers
  - Tier 1 Service Provider
  - Tier 2/3 Service Provider
  - ...

Framing the Problem

- What are the threats a high-speed backbone providers is exposed to/concerned about the most?
- What are the characteristics of these threats?
- What defense mechanisms are already in place?
- What are the disadvantages of existing, in use defensive measures?
Service Provider Threats (1)

 Experienced Threats

![Survey Respondents vs Threats](chart)

- 77% DDoS attacks towards your customers
- 49% DDoS attacks towards your services
- 49% Infrastructure outages
- 47% DDoS attacks towards your infrastructure
- 39% Bandwidth saturation
- 4% Other

Service Provider Threats (2)

Expected Threats

- 69% DDoS attacks towards your customers
- 59% DDoS attacks towards your infrastructure
- 50% DDoS attacks towards your services
- 44% Infrastructure outages
- 38% Bandwidth saturation
- 8% Other

Service Provider Threats (3)

- Reasons for „Bandwidth saturation“/Wrap-up of Threats of Interests for a Backbone Provider

Attack Duration:
- „The average attack duration in 2015 was 58 minutes, which is relatively consistent with previous results“

Threat Detection Tools

Threat Detection Tools in General:

- 78% Netflow based analyzers
- 64% Firewall logs
- 51% SNMP-based tools
- 51% IDS/IPS
- 48% Performance management/monitoring solutions
- 48% Customer call/help desk ticket
- 38% In-house developed scripts/tools
- 37% Inline DDoS detection/mitigation
- 37% Security Information and Event Management (SIEM) platforms
- 3% Other

On Flow Based Intrusion Detection

Flow: “a set of IP packets passing an observation point in the network during a certain time interval; all packets belonging to a particular flow have a set of common properties”

No Problem with regard to the what kind of attacks can (theoretically) be detected and the increased detection time
Shortcomings of Threat Detection Tools

➢ Where exactly is the Problem?
  – High False Alarm Ratio
  – Costs
  – Legal/Contractual Limitations
  – It’s a business decision: Mitigation is not always the strategy of choice
Objective of the architecture

- Classically, the objective of an IDSs is
  - to maximize True Positive + True Negative and accordingly
  - to minimize False Positive + False Negative

- Objective of High-Speed Backbone-Provider
  - not to identify as many positive results as possible (high True Positive rate), but
  - to reduce the False Positives, even if this could mean that the False Positives go down at the expense of an increase in the False Negatives.
Wrap-up of Existing Approaches

- What are the threats a high-speed backbone providers is exposed to/concerned about the most?

- What are the characteristics of these threats?
  - Most important for this paper: Average time of 58 minutes; High resource utilization

- What defence mechanisms are already in place?
  - Mainly: Flow-Based Intrusion Detection

- What are the disadvantages of existing, in use defensive measures?
  - High False Alarm Ratio

Overview of the Architecture

Reconfiguration / Implementing Countermeasures

Flow Collector
Flow-Based IDS
Detections

A

Backbone Network
Core Router

B

DPI-Based IDS
(e.g. Snort)

Manager
IP GeoInfo
Geo-Database
(e.g. IPInfoDB)

Flow-Based IDS
(e.g. SiLK)

On Geolocation

- Geolocation is used after the Flow-Based Intrusion flags traffic as suspicious

- Main ideas
  - Prioritize Traffic
  - Legal/Contractual Limitations (that forbid certain countermeasures)

- Assumptions
  - 1. Temporal correlation: After a certain time, a Geo-Correlation shall no further be given
  - 2. Spatial correlation: A new connection only gets correlated to an already known, malicious connection if the distance is lower than a specific threshold
  - 3. Fog of time: The older the information (IP known to be malicious in the past), the less important shall this information be
  - 4. Accuracy level: The more accurate the Geolocation is (which is also closely linked to the density of the population), the smaller the distance for Geo-Correlation
Implementation

- Reuse of well-established/state-of-the-art solutions
- Flow Collector/Flow-Based IDS
  - only a small number of solutions is available as a real product / software solution
  - In the open source community, there are just a few popular tools:
    - Stager (a system for aggregating and presenting network statistics); not maintained since 2010
    - nfdump (and its web component nfSen)
    - SiLK (System for Internet-Level Knowledge, which is developed by Carnegie Mellon)
      - We have chosen SiLK (better suited, easier to adapt)
      - Nevertheless: Similar Results with nfdump
- DPI-Based IDS: Snort, the de-facto standard
- Geolocation: IPInfoDB
Evaluation Setting

- **Phase 1: Recording Real-World Data**
  - To simplify the evaluation and (ii) to reduce external effects as well as to (iii) to allow a better comparison of individual systems, real traffic data was recorded in advance.
  - Special focus has been placed on obtaining a representative data stream.

- **Phase 2: Ground Truth**
  - In order to know the Ground Truth, we have then analyzed the original data set (slowly) with the use of (several) DPI-based IDSs for the presence of attack traces.

- **Phase 3: Synthetic Enrichment**
  - Synthetic portion (background noise and synthetic attacks)
  - Objective (again): representative data stream

- **Phase 4: Replay Traffic with Traffic Generators and test of the prototype**
  - The sampling rate we used was 1-in-100 (frequency in which the packets are analyzed; on average, 1 in every 100 packets is captured and analyzed) with a polling-interval of 30 sec (timeframe in which the network device exports Flows to the collector)
Evaluation Results

Evaluation Results

Conclusion

- Detection Time is not the issue
- Reuse of State-of-the-Art Solutions using commodity hardware is possible
- Quality of Protection is either defined by contract or by legal obligations
  - Countermeasures that are allowed
  - Level of Detection (e.g., The Netherlands have forbidden DPI unless motivated by solid justification)

Performance SLA
Quality of Service (QoS)
- Expected performance
  - Network outage
  - Latency
  - Packet loss
  - Average jitter
  - Maximum jitter
  - ...
- Procedure for monitoring and reporting
- Consequences when not meeting the agreed service level
- Procedure for handling problems with the service

Security SLA
Quality of Protection (QoP)
- Security requirements that the provider will commit to
  - Process of monitoring security, including what evidence to collect, present and who will be responsible for it
  - Process of reporting problems, threats or security related incidents
  - Consequences when not meeting the agreed security service level
  - Procedure for handling problems with the service
  - Legal and regulatory issues