**Motivation**

- **Trouble shooting**
  - What happened before a fault?
- **Security Monitoring (“Forensics”)**
  - Break in 3 days ago!
  - How? What else have they done?
- **Network packet traces are invaluable for forensics**
- **High traffic volume prevents naive bulk-recording**

**Approach**

- **Buffer packets, using a connection cutoff**
- **Leverages heavy-tailed nature of network traffic**
- **Buffer several days of high-volume traffic**
- **Provide flexible, automated query interface**
- **Interface to other security devices (e.g. NIDS)**
- **Time Machine allows us to “travel back in time”**

**Summary**

- **Connection Cutoff (15 kB) reduces the capturing volume by 90%**
- Can store a week worth of data with reasonable disk size
- Can handle Gigabit links; Runs on commodity hardware
- Enables allocation of resources to different classes of traffic
- Offers highly flexible and fast queries
- In use at TUM and LBL
- Interface with Bro operational

**Impact of Connection Cutoff**

- Probability that a connection is of a certain size (vertical line at 20 kB).
  - ⇒ only 12–15% of the connections are larger than 20 kB.

**Memory consumption**

- Memory consumption for different eviction times $T$, and cutoff.
  - ⇒ The cutoff reduces the memory needs dramatically, allowing up to four days retention within less than 120 GB.

**Retain time**

- Retention time (in days) for different classes (cutoff 20 kB, TCP 90 GB, UDP 30 GB, Other 10 GB) of traffic.
  - ⇒ Even those small memory buffers allow up to three days of retention

**Indexing**

- **Used to allow easy access to the stored packets (via time-intervals).**
- **Connection 5-tuple, IP address pairs and single IP addresses are the most common index keys (additional indexes are possible).**
- The indexes to packets in memory are kept in memory and the indexes for packets on disk are kept on disk.
- Index files are sorted for fast access.
- Index files on disk are aggregated by a separate thread.

**Integration with NIDS’Es**

- A Network Intrusion Detection System (NIDS) can
  - control TM to, e.g.:
    - permanently store malicious traffic for forensics
    - dynamically tune operation parameters
  - query TM to retrospectively analyze traffic to e.g.:
    - perform in-depth analysis of past traffic originating from detected attackers
    - examine traffic it did not see
      (due to resource trade-offs, gaps)