Measurement for Cooperative Network Defense: DEMONS and BlockMon

Brian Trammell

Communication Systems Group, ETH Zürich

Flocon 2012, January 11, Austin, Texas USA

The problem

- The attack landscape has become more *complex* and *cooperative.*
  - Botnets, XSS, APT, *(scary_buzzword_ary++)
- Network defense remains largely isolated.
  - Siloed within single administrative domains
- → Tools and processes for defense must become more cooperative than (implicit) processes for attack.

Centralization of Traffic Data

- Passive measurement collects enormous amounts of data.
  - "Congratulations, you just pointed a ten gig firehose at yourself"
- (Almost) all of it is simultaneously
  - quite sensitive,
  - and completely uninteresting.
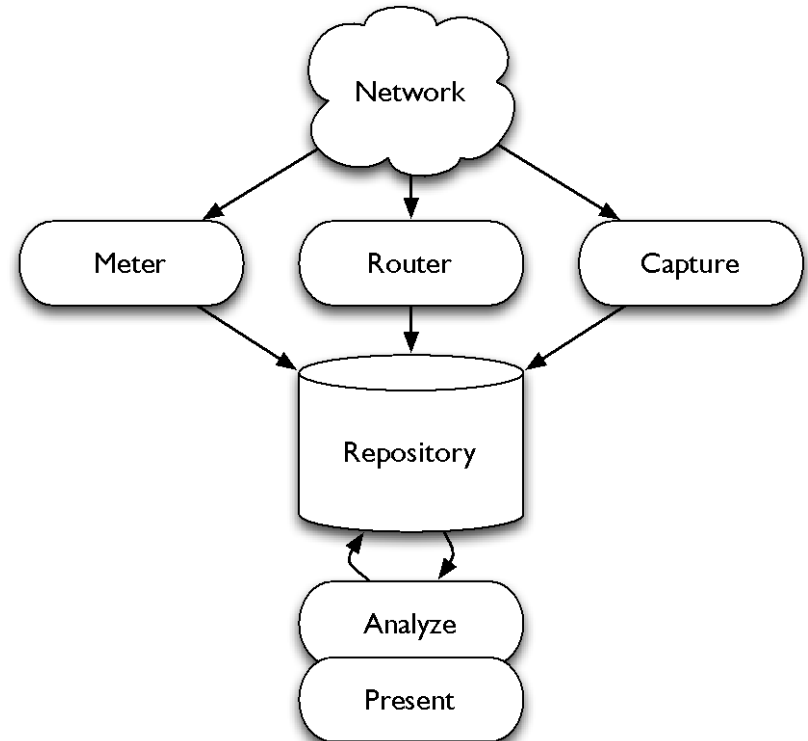
Sharing Traffic Data
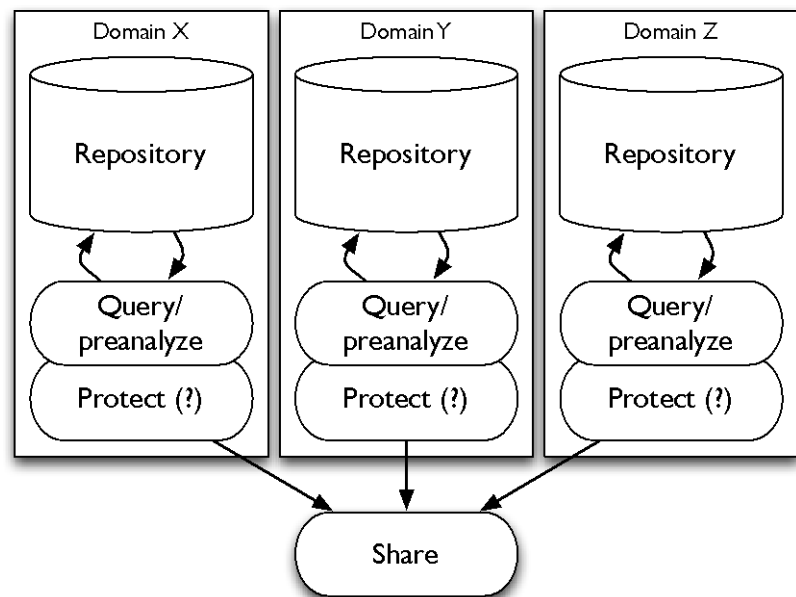
- Cooperative incident handling requires sharing of data across domains.
- *Data sharing is fraught with peril.*
  - Legal, regulatory, and business-sensitivity restrictions on data protection and disclosure
  - Anonymization not a solution to the problem
    - Pattern injection on Internet traffic practically undetectable [1]; partial offline reversal of anonymization possible.

[1] Burkhart et al., "The Role of Network Trace Anonymization Under Attack", ACM Computer Communications Review, vol. 40 no. 1, January 2010
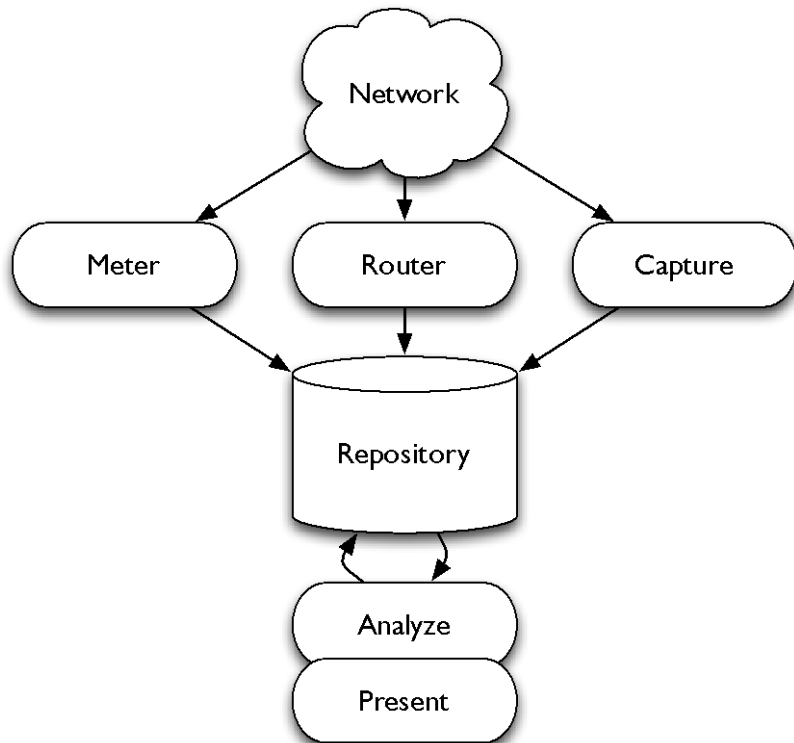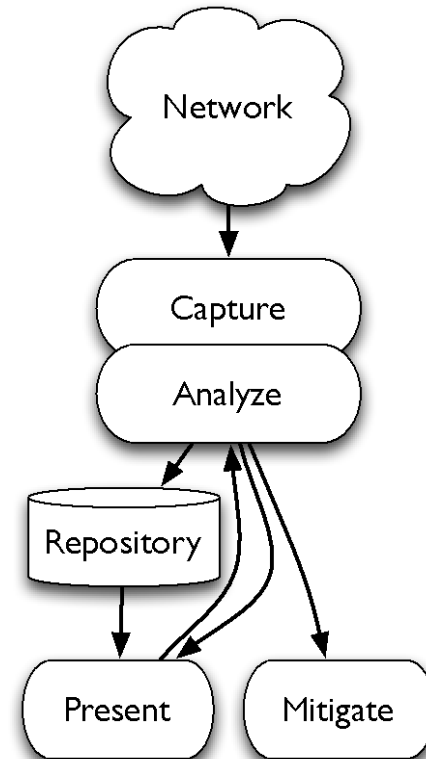
Cooperative Network Defense

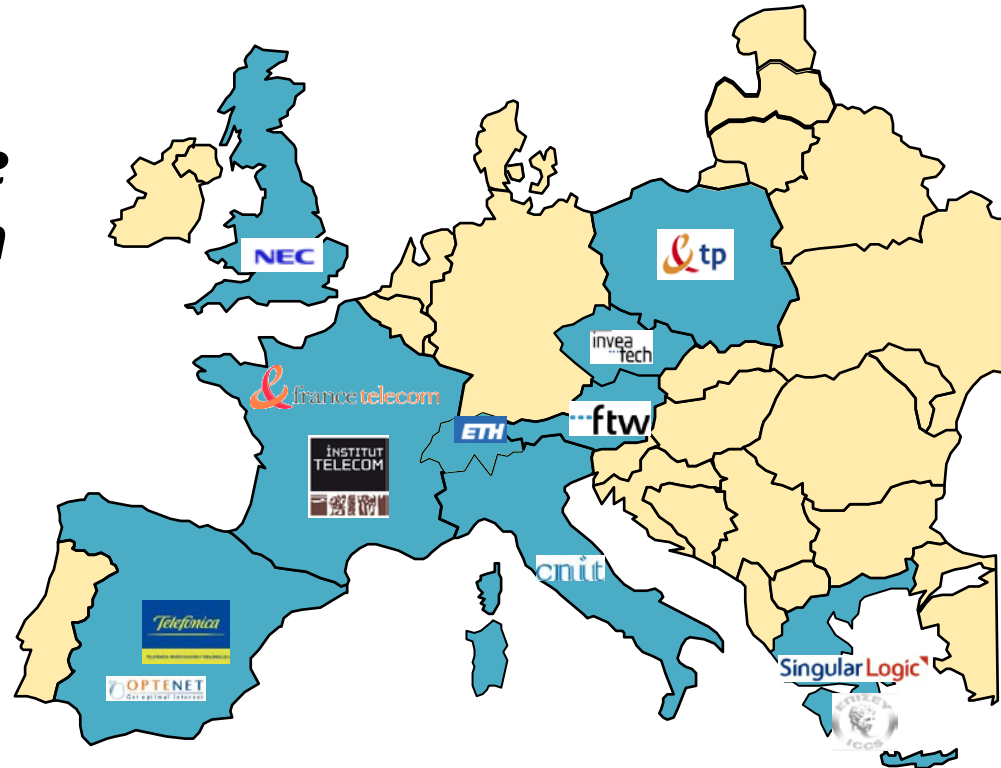# DEMONS

The DEMONS Approach

Centralized

DEMONS

DEMONS: The Project

- EC-funded, FP7 ICT IP, Sep 2010–Mar 2013

- Goal: ***Enable cooperative detection and mitigation of incidents effecting network stability and security.***

- Consortium of 13 in 9 countries, includes three network operators (Telefónica, FT, TP)

# The DEMONS approach: decentralization

- *Move processing to the edge*
- Support iterative analysis on live traffic using programmable edge devices.
- Emphasize stream processing over retrospective analysis, use existing processes for forensics.
- Data reduction on the measurement device improves scalability and reduces sensitivity of collected data.
- Integration with existing mitigation processes.
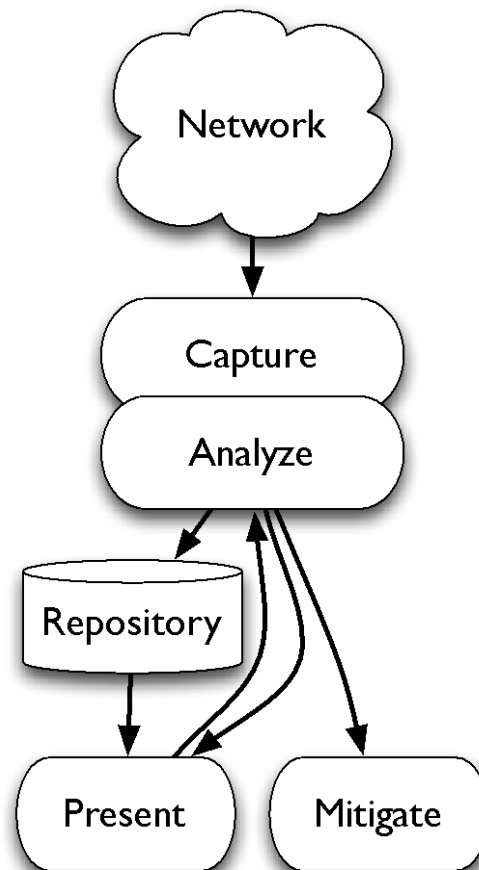
The DEMONS approach: sharing

- *Share analysis, not data*
- Analyses built by composition of well-defined processing modules
- Inspection of intermediate results before export
- Application of secure multiparty computation schemes, where appropriate
- Realism about technical limitations of data protection
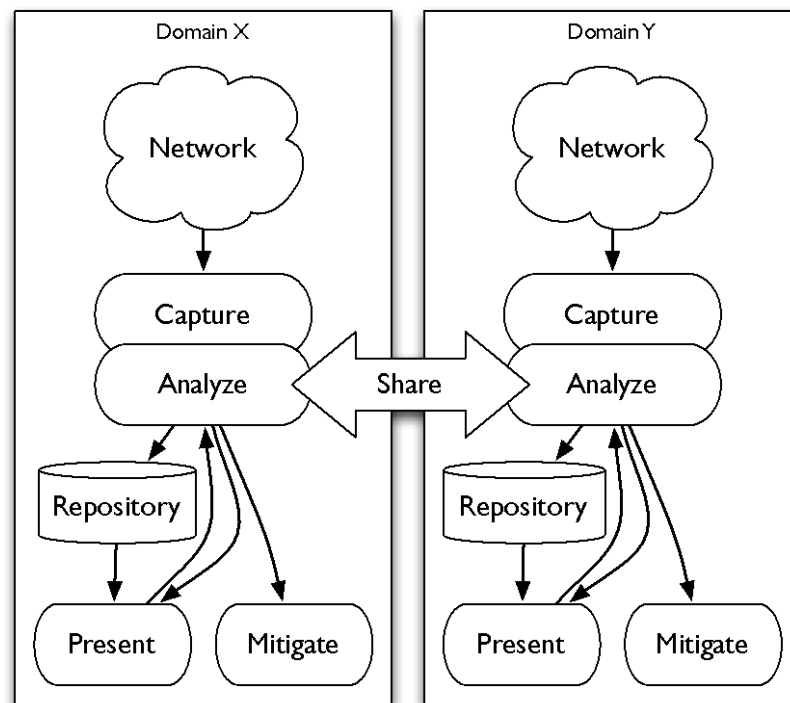
DEMONS Components and Interfaces

- Measurement layer nodes provide capture and analysis.

- Interdomain exchange point (IXP) provides "sharing" interfaces to external domains.

- Mitigation control point (MCP) provides interface to existing processes.
  - Additional research within the project WRT policy-driven pseudo-automatic mitigation, MPLS-based quarantining
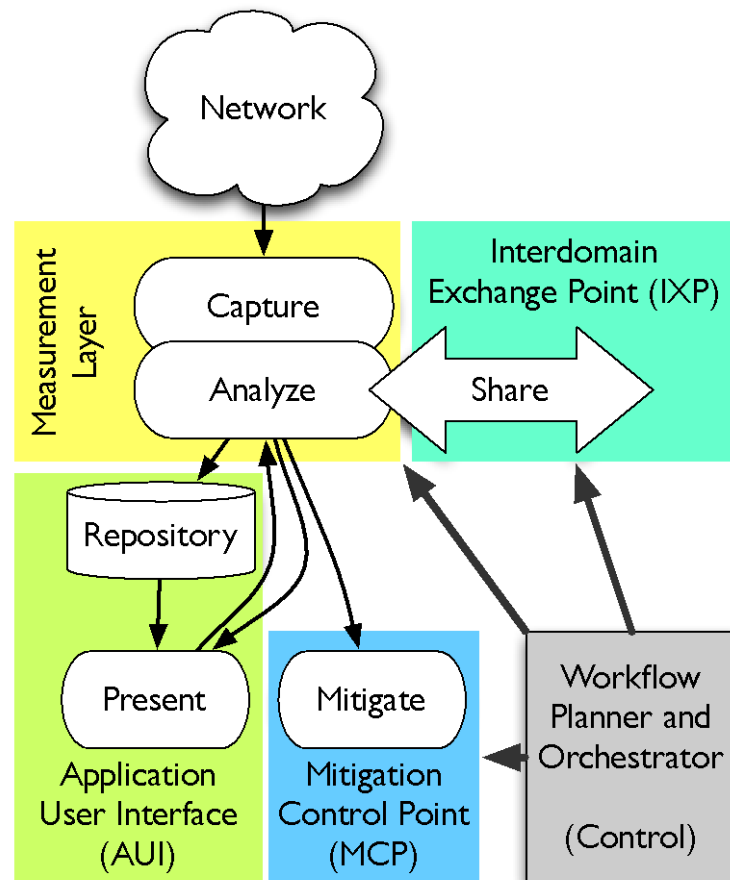
Composable Network Measurement
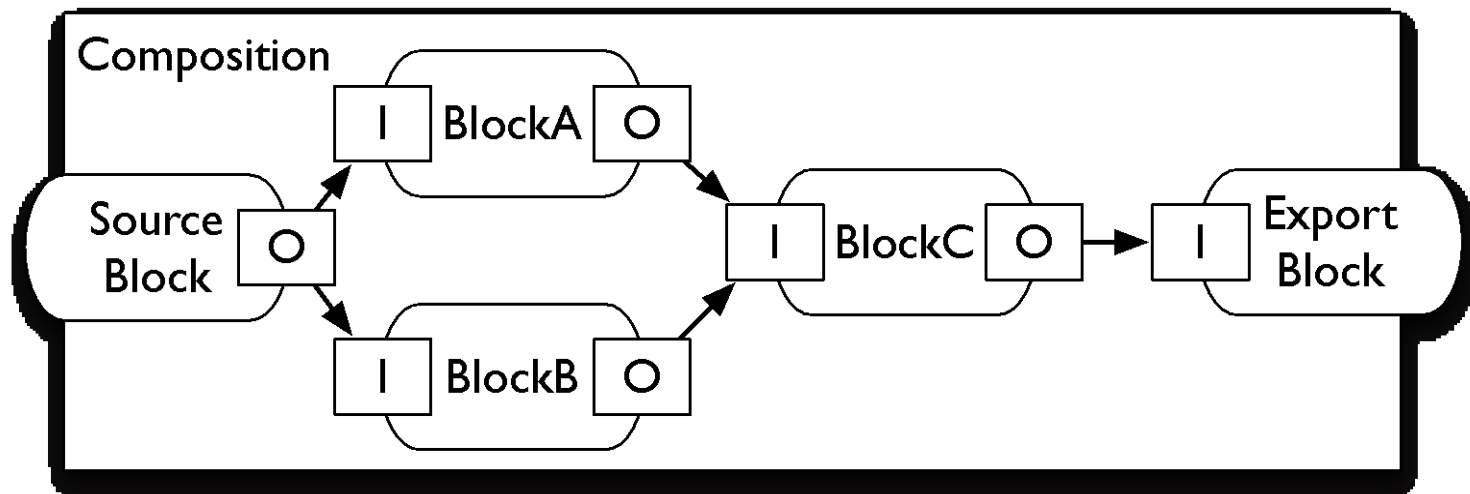
BLOCKMON

Introducing BlockMon: Goals

- Composable measurement using small blocks
  - Increases parallelizability, measurement performance on multicore hardware
  - Code reuse for measurement development
- Platform for understanding composable measurement application development
- Enable code and analysis interchange in the form of compositions of modules from a standard, trusted base

BlockMon

- Compositions of *blocks* exchange *messages* connected via *gates.*
- Blocks are implemented in C++, framework and scheduling in C++, focus on performance
- XML-based composition schema
- Python-based CLI and JSON-RPC daemon

BlockMon: out-of-box experience
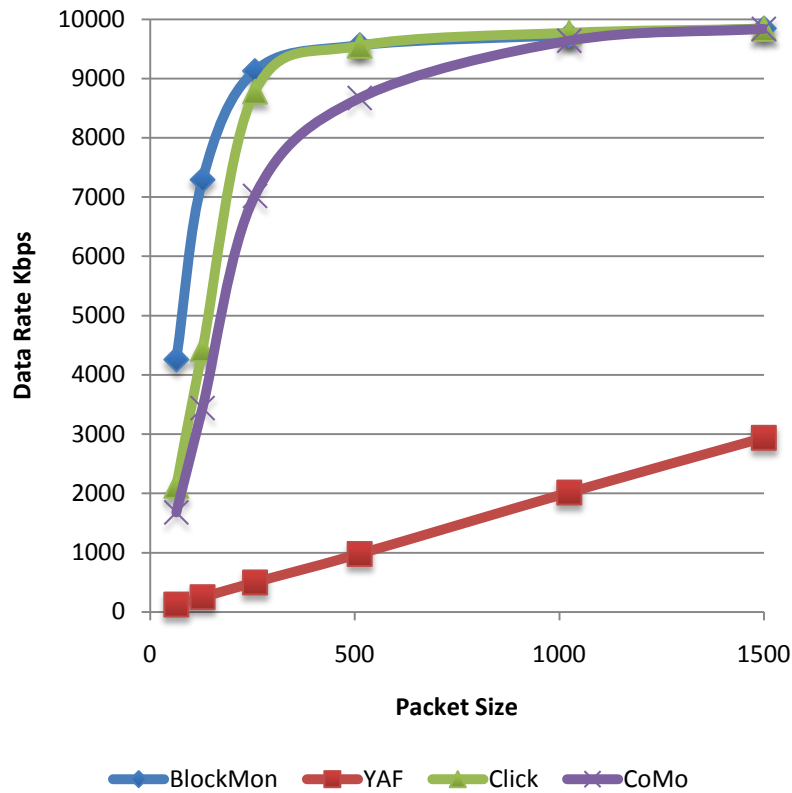
- Core messages, bridged to IPFIX
  - Packet, with lazy parsing & cache-aware allocation
  - Flow, allows use of BlockMon as a streaming flow analysis tool
  - Message base class allows *tagging* for adding features or annotations to a message in flight
- Source, exporter, simple counter blocks
- Current work on taxonomy of blocks
  - filters, metrics, features, correlations, feedback

BlockMon:
How fast is fast?

Synthetic traffic (10Gbps)

Trace replay (6Gbps peak)

CDR input file
(sorted by timestamp)

parse CDRs

check if
<caller,callee> is new
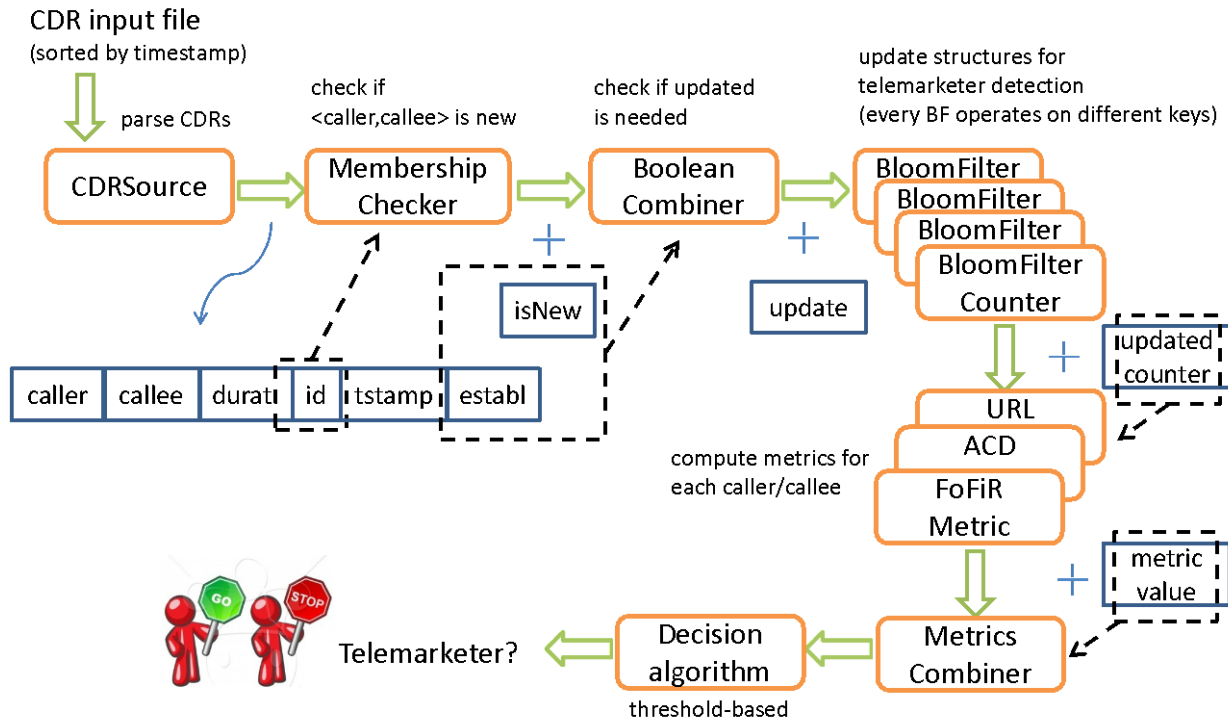
check if updated
is needed

update structures for
telemarketer detection
(every BF operates on different keys)

CDRSource → Membership Checker → Boolean Combiner → BloomFilter / BloomFilter / BloomFilter / BloomFilter Counter

isNew

update

updated counter

caller | callee | durati | id | tstamp | establ

compute metrics for
each caller/callee

URL / ACD / FoFiR Metric

metric value

Telemarketer? ← Decision algorithm ← Metrics Combiner

threshold-based

- Every Block is active, processes a CDRMsg (composition of PairMsg and Tags), and appends its own tag to it.
- BloomFilterCounters blocks are configured to work on a time-window base (i.e., 6hour long).

Play Along at Home

- BlockMon to be released as open-source software, BSD licensed.

- Development of the core presently *very active*

- Find me this week or e-mail <trammell@tik.ee.ethz.ch> if you're interested.

Conclusions

- Current attacks require cooperative defense.

- Data sharing is fraught with peril.

- Move processing to the edge.

- Share analysis, not data.

- Composable measurement makes it possible.

Acknowledgments

- FP7-DEMONS project
  - funded by the European Commission

- BlockMon Team
  - NEC Laboratories Europe
  - CNIT (Consorzio Nationale Interuniversitario per le Telecomunicazioni)