DEcentralized, cooperative, and privacy-preserving MONitoring for trustworthiness

Dr. Sathya Rao
KYOS; Switzerland, Sathya.rao@kyos.ch
Motivation

Today’s monitoring systems
- Centralized
- Huge amount of exported/collected data
- Hard/no cooperation across domains
- Poor flexibility in access control to monitored data (little more than Y/N)

Hardly coping with
- Higher link rates and traffic volumes
- Networks pervasiveness & capillarity
- Distributed, cross-domain, threats

Cluster meeting, Padova, 6 Sep. 2012
Vision

Overlay of in-network monitoring devices
From data-gathering probes to **collaborative P2P computing and filtering devices**

<table>
<thead>
<tr>
<th>Innovation pillars</th>
<th>Target Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-network processing and distributed intelligence</td>
<td>Scalability</td>
</tr>
<tr>
<td>Application-tailored data reduction and protection</td>
<td>Privacy preservation</td>
</tr>
<tr>
<td>Resilient autonomic monitoring overlay</td>
<td>Flexibility and resilience</td>
</tr>
<tr>
<td>Cross-domain interworking</td>
<td>Cross-domain threat detection and mitigation</td>
</tr>
</tbody>
</table>

Exchange only the information strictly necessary for a given monitoring and analysis objective
The DEMONS Approach: Decentralized data analysis

- **Centralized**
- **DEMONS**
  - *In-network processing*
    - Programmable devices
    - Move analysis to data
  - *Stream processing*
    - Least data collection
    - Fast & scalable
  - “smart” orchestration & Integration with existing mitigation processes.

Cluster meeting, Padova, 6 Sep. 2012
The DEMONS approach: cross-domain sharing

- Inspection of intermediate results before export
  - Condition sharing to *global* occurrence of events

- Collaborative analysis without disclosing input data
  - Secure multiparty computation schemes

- Realism about technical limitations
  - Inter-domain protocols
  - Inter-domain deployment issues

*Share analysis, not just data*
DEMOnS functionalities

- **Measurement layer:**
  - capture and analysis
  - Distributed in the network

- **Interdomain exchange:**
  - IXP: "sharing" interface to external domains.

- **Mitigation:**
  - MCP: interface to existing processes.

- **Orchestration and control**
  - Workflow specification & enforcement
  - Access control
  - Programmable Composition of analyses
What is a Blockmon

- **Blockmon** is a modular system for flexible, high-performance traffic monitoring and analysis.
- Based around the notion of:
  - *Blocks*: modules that perform a small amount of traffic of data processing (e.g., filtering for a specific UDP port number)
  - *Gates*: the input and output ports of blocks
  - *Compositions*: a set of interconnected blocks, akin to a monitoring or anomaly detection application (e.g., heavy hitter detection)
Blockmon tested and released as open source

- Blockmon provides the best from both worlds: flexibility plus high performance
- Conducted extensive performance experiments to verify this
- Available as open source
- Implemented three applications:
  - SYN flood detection
  - Heavy hitter statistics
  - VoIP anomaly detection
Towards execution

Cluster meeting, Padova, 6 Sep. 2012
Workflow deployment

Cluster meeting, Padova, 6 Sep. 2012
The IXP is a functional component that may be seen as a collection of modules and interfaces.

- Interfaces: external design
- Modules: internal design

Some interfaces are exposed to external domains, and some other to the internal DEMONS deployment (to the other components).
DEMONS features two GUIs
- Programming and Administrative Interface (PAI)
  - Programming, administering and maintaining DEMONS
  - DEMONS programmers
- Application User Interface (AUI)
  - Monitoring by users within a given domain
  - DEMONS applications users

Single user interface for PAI/AUI
- Controlled on user roles
- Allowing switching among GUIs
Dissemination: Main channels used

• Project Website  www.fp7-demons.eu
• Press Release, Fact sheets, Public presentations
• Publications: Workshops, conferences, Journals
• Standards: Contribution to
  • ETSI: INS and MOI ISGs
  • IETF: 2 RFCs published, 5 I-Ds as WG items, 1 interop hosted, 1 WG founded
  • ITU: SG17 Liaison, Contribution to Q4
    • SG17 chairman is our advisory board member
  • ENISA: Joint activities; Summer school
Dissemination: publications

General awareness
- Project factsheet
- Project presentation
- Press release
- Public deliverables

Technical publications
- 28 Scientific Papers
- 21 events (conf., exhibitions, invited,..)
- 2 Book chapters
- 4 journal publications
- 7 Workshop sessions organised

Available on the website www.fp7-demons.eu

Cluster meeting, Padova, 6 Sep. 2012
KYOS is one of the partners in DEMONS and their business activities are...
Thank you

Contact:
Sathya.rao@kyos.ch