AMON: An Extensible Open Source Framework for Online Monitoring, Statistical Analysis and Forensics of Multi-Gigabit Streams

Abhishek Balaji Radhakrishnan (USC/Merit)

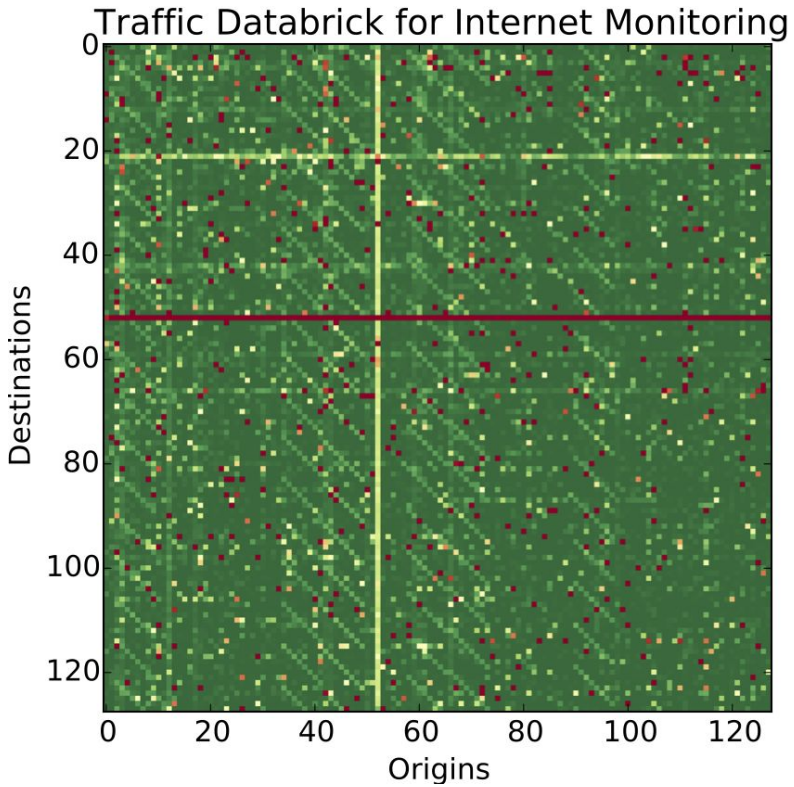
M. Kallitsis (U. of Michigan/Merit), Z. Gao(U. of Michigan), S. Stoev (U. of Michigan), G. Michailidis (U. of Florida)

Motivation

- Attacks grow in variety and sophistication
- Increasing DDoS attacks, IoT explosion and vulnerabilities, scanning events, etc.
- Commercial appliances prohibitively pricey

Our approach

- AMON – All-packet MONitor
- Open-source, software-based
- Passively monitors traffic (tap)
- Runs on PF_RING: can scale to 40Gbps+ links on commodity hardware



Challenges

- Challenging to monitor multi-10Gbps Internet streams
- Constrained by memory and compute resources
- Industry uses Netflow -- usually heavily sampled

Main AMON features

- Data products (“databricks”) that couple together detection, visualization and identification
- 3D real-time of a network’s traffic intensity and structure
- Boyer- Moore majority vote algorithm for heavy-hitters

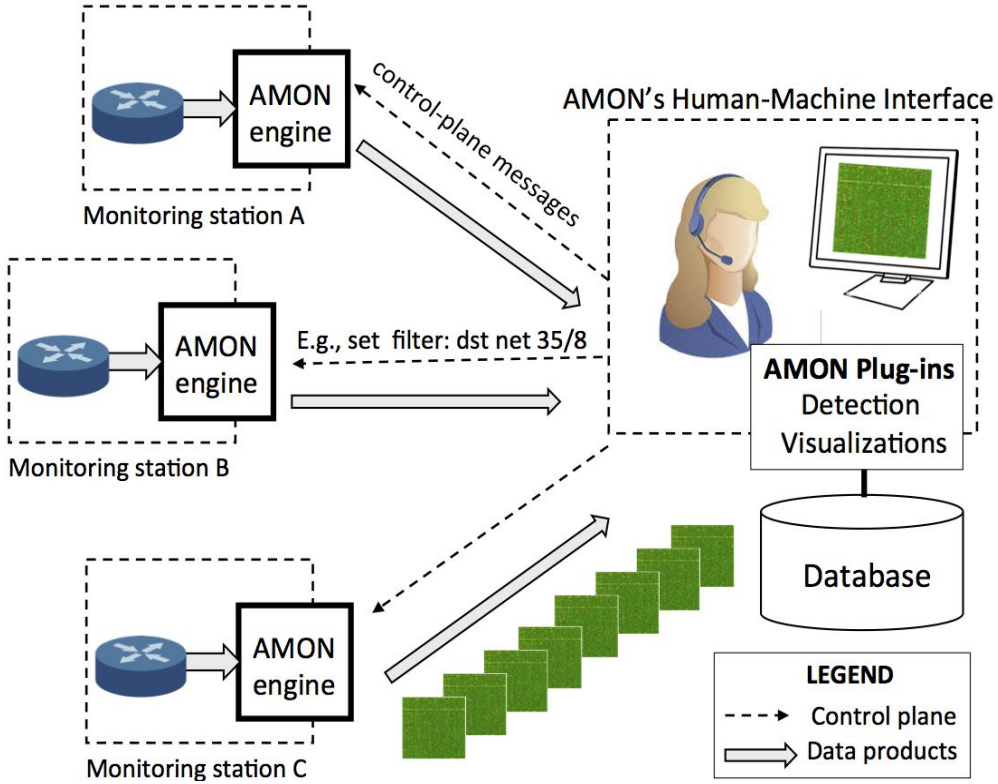
Work in Progress and Future Directions

Programmability

- Program distributed AMON instances
- Slice network traffic (e.g., BPF filters)
- Hash-based filtering

Scale to 40Gbps+ streams

- Currently 20Gbps on a CPU core
- Multi-core implementation as new modules, new applications (e.g., DNS) are added



New detection plug-ins

- Databrick fusion, aggregate databricks from different sites
- Community-based detection techniques

Data sharing

- Share data with downstream customers
- Privacy preserving

Tools and datasets will be made available through DHS IMPACT: https://impactcybertrust.org

Acknowledgements: NSF SaTC and DHS S&T

Thank You!

Abhishek Balaji Radhakrishnan
aradh@merit.edu

Questions?