

New data structure allows rapid tracking and policing of network data

October 5 2017

To protect networks from malicious threats, cyber-security solutions must track all the data flowing through the network—just like security guards checking travelers in airports. However, it is hard to design a solution that works fast enough to process all the information in real time, and to block threats before they can strike. Now, A*STAR researchers have designed a way to structure data that is robust against cyber-attacks and allows it to be processed in record time.

The team's work improves on widely-used data structures called 'hash tables'. "A hash table maps values to specific locations, labeled with indices," explains Vrizzlynn Thing from the A*STAR's Institute for Infocomm Research, who led the study. "To find a value, the hash table performs computations to quickly identify the indices and thus, its location. The challenges are that millions of values need to be stored, and the values are generated and transmitted extremely quickly."

Traditional hash tables are becoming inefficient as the internet grows and data flows get larger. Researchers have developed data structures known as Cuckoo and Peacock, but when they are under attack, these hash tables fill up quickly, eroding performance.

The new data structure developed by Thing and her team is called REX. "The name REX stands for Resilient and Efficient data Structure (X for structure)" says Thing. Jokingly, Thing explained that this data structure was named REX (after Tyrannosaurus Rex) to signify a stronger creature than the Cuckoo and Peacock as it outperforms both tables.

REX works by exploiting some inherent characteristics of internet traffic. For example, it takes into account the 'heavy-tail' behavior of data flows (there are a few large 'elephant flows' which contribute to a larger percentage of the total volume than the many small 'mice flows'), by employing a hierarchy of sub-tables increasing in size from top to bottom. This structure effectively segregates the different types of flows.

"We also utilized the special processing property of computer RAM," says Thing. "Our design features both fast, expensive Static RAM and slower, cheaper Dynamic RAM." The faster SRAM is used to process the few large, important flows, allowing fast tracking and frequent updates, while DRAM handles the low priority flows in secondary sub-tables.

In tests using real recorded network traffic, REX was faster and more efficient at analyzing data than Cuckoo and Peacock. "We will further investigate the efficiency and scalability of this new data [structure](#) for security analysis in larger scale environments," says Thing.

More information: Dinil Mon Divakaran et al. REX: Resilient and efficient data structure for tracking network flows, *Computer Networks* (2017). [DOI: 10.1016/j.comnet.2017.03.004](https://doi.org/10.1016/j.comnet.2017.03.004)

Provided by Agency for Science, Technology and Research (A*STAR), Singapore

Citation: New data structure allows rapid tracking and policing of network data (2017, October 5) retrieved 27 April 2024 from <https://phys.org/news/2017-10-rapid-tracking-policing-network.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private

study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.