Secure Diagnostics and Forensics with Network Provenance

Ang Chen
University of Pennsylvania

4/3/2017 at 10:30 am
CoRE A 301

Abstract

Distributed systems are behind many important services that we use every day, such as online banking, social media, and video conferencing. However, in a large-scale distributed system, many things can go wrong: routers can be misconfigured, programs can be buggy, and computers can be compromised by an attacker. To investigate these problems, system administrators need to play the role of 'part-time detectives'. Their tasks would be much easier if there were a way for them to ask the system to explain certain events, such as 'Why was this particular route chosen?'.

My work leverages data provenance - a concept from the database community - to enable distributed systems to offer such explanations. At a high level, provenance tracks causality between network states and events, and produces a detailed, structured explanation of any event of interest. Such information can be a helpful starting point when investigating a variety of problems, ranging from benign misconfigurations to malicious attacks.

In this talk, I will present one technique in detail that can accurately pinpoint the root causes of problems by comparing the provenance of 'correct' and 'incorrect' events. I will then give an overview of my other work on network provenance, including an extension of provenance to repair network programs, and an application of secure provenance to the Internet’s data.

Bio

Ang Chen is a fifth-year Ph.D. student in the Department of Computer and Information Science at the University of Pennsylvania, advised by Professor Andreas Haeberlen. His research interests are distributed systems, networking, and security. Besides network provenance, he has also worked on systems and network security, including projects on detecting covert timing channels, mitigating attacks in cyber-physical systems, and defending against DDoS attacks.
Faculty Host: Santosh Nagarikatte