SAND2017-7570C

The Center for Cyber Defenders

Expanding computer security knowledge

Laika BOSS

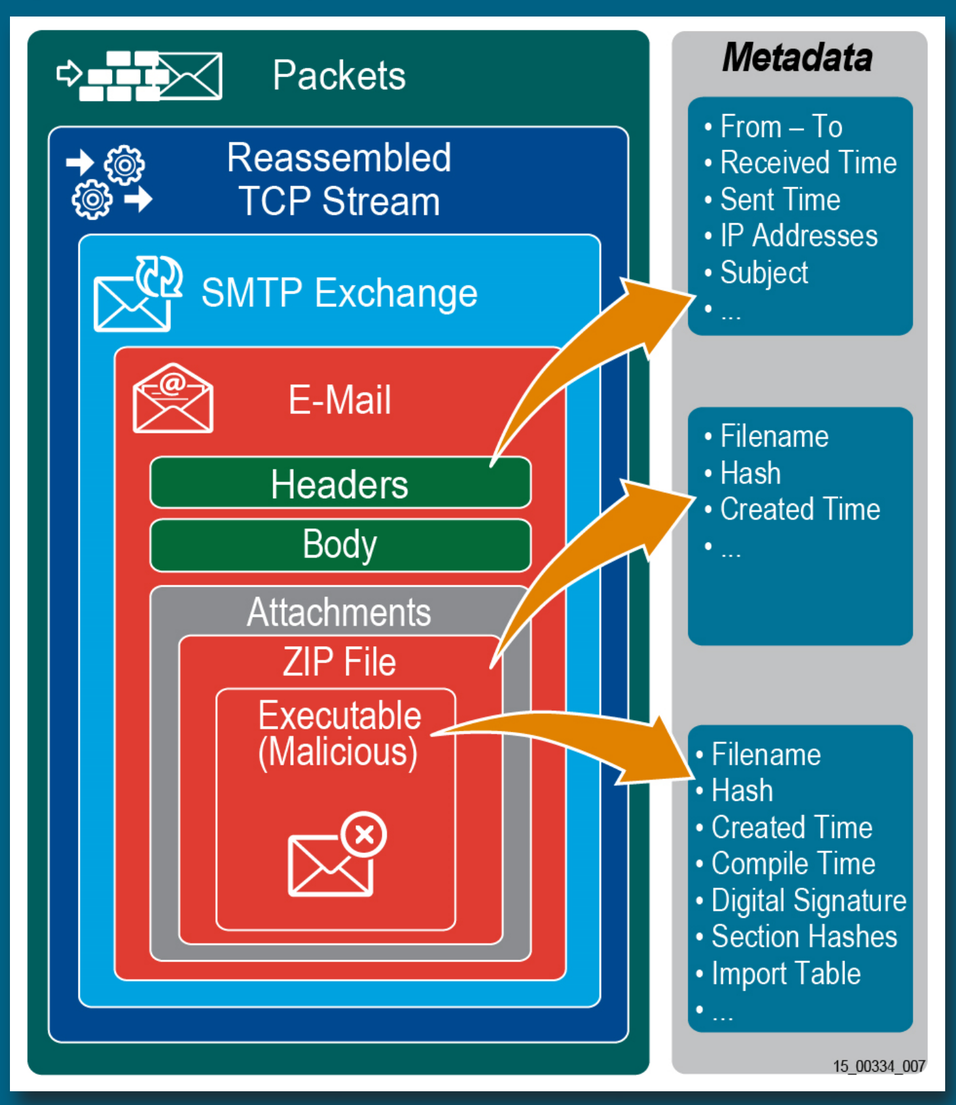
File-Centric Intrusion Detection

Greg Walkup, Purdue University

Project Mentor: Charles Smutz, Org. 9312

Problem Statement:

- Laika BOSS (Binary Object Scanning System) is an intrusion-detection and scanning system that operates on individual files and file-like objects, while extracting more files recursively.



Objectives and Approach:

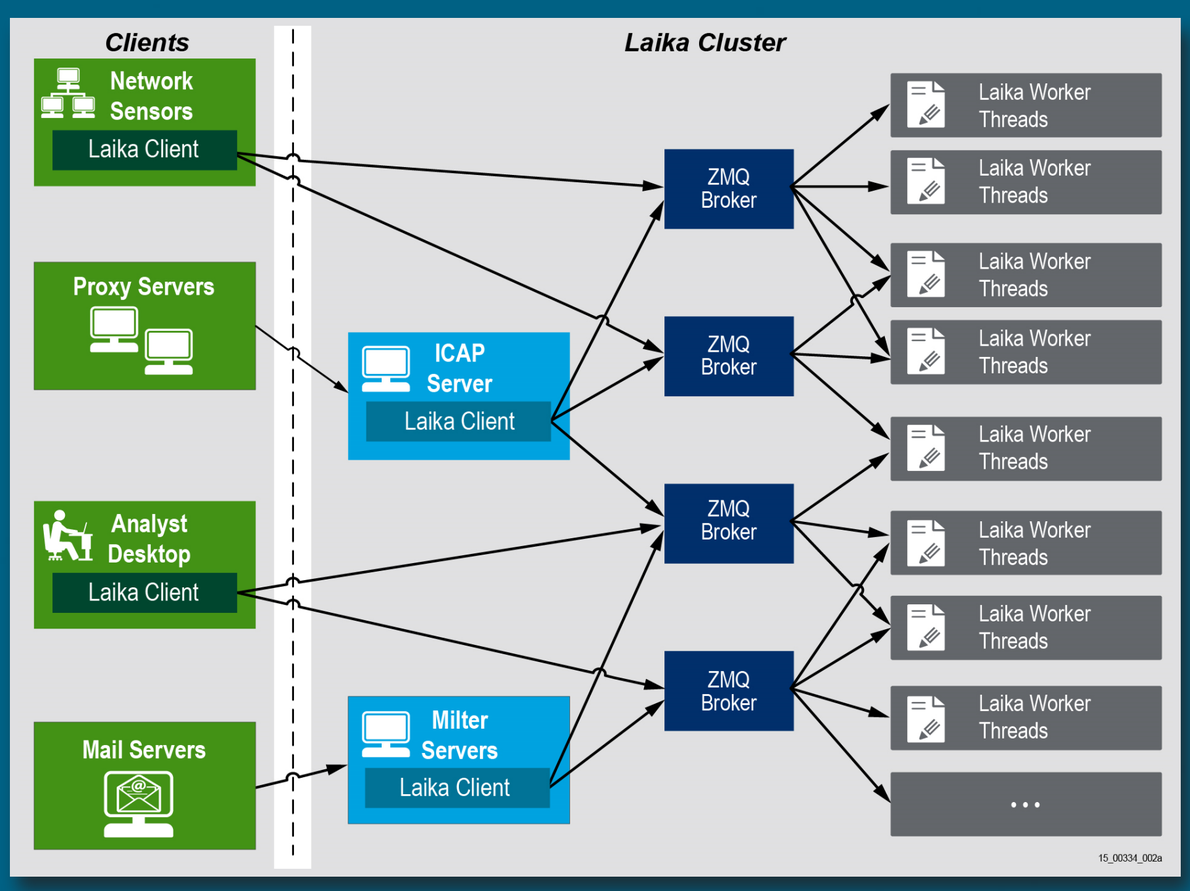
- Create modules for new file types and explore new methods of analysis for existing file types
- Optimize existing modules and subsystems
- Maintain and improve features ahead of deployment at Sandia

Results:

- Increased the speed of a key subsystem by about an order of magnitude
- Developed extraction and metadata modules for new types of files
- Added new configuration items for greater customizability

Impact and Benefits:

- The efficiency of a key subsystem was greatly increased (formerly took ~25% of CPU time)
- Created new modules that support Sandia's internal cybersecurity efforts
- Contributed features and bugfixes back to the open-source project



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.