### Question 1

Prompt: Summarize Trent Jaeger's talk. You should describe the motivation, problem(s), and approach(es). You should also identify the intellectual nugget(s). Link: <https://youtu.be/shP5n3oczdQ>

Trent’s talked centered around research he and his team did regarding the safety of stack objects in unsafe languages such as C, which is still the #3 most widely used language in the world. The motivation behind the research was to come up with a way to validate and protect most stack objects from all types of memory errors, while reducing performance overhead.

There are existing defenses for unsafe stack objects currently, such as stack canaries to protect the integrity of return addresses, safe stack to protect integrity of code pointers, baggy bounds to prevent spatial errors and TypeSan to prevent type and temporal errors. However the problem is that using each of those defenses toegether has significant performance cost. Which is why most will implement only one, if that.

This is where the intellecutla nugget of the research comes in. They came up with a process called DataGuard.

It’s a 3 step approach where they identify error classes of stack objects, collect safety contraints about those stack bojects , and verify stack object safety.

The third step in the approach is the most important because they created a static analyzer to verify safe stack objects, reducing the need to do dynamic runtime checks on the validation of safe objects, saving in performance overhead.

In their research findings when applying their datagaurd process to unsafe stack objects, they found it validated 90% of stack objects are safe from spatial, type and temporal errors. DataGuard proved that a comprehensive and accurate analysis can both increase the scope of data protection while reducing perofrmance overheads.