Splitting the Bug

Motivation
Writing secure code is difficult. You don’t believe me? To the Research: In 2012 researchers found that a) most programs relying on TLS don’t use it correctly, and b) many Android programs don’t use cryptography correctly. In both cases all bets concerning security are off, and that’s just two of a myriad of examples.

If writing secure code is difficult, how about the problem of finding out which parts of a program even have security requirements? Also difficult. That’s bad, because we have become good at protecting “small” parts of programs and program data using Trusted Execution Environments.

So, are we all doomed? Well, what if we could get a computer to do the splitting for us? Now there is an idea … Thing is, if we do program splitting in a provable secure way, it’s not really usable any more. Hypothesis: For a subset of security critical software, we do not need provable secure, but we would love having something that works. This is where you come in!

Project Description
Goals
• Design and implement a heuristic tool for automatic program splitting
• Evaluate your tool vs. an existing secure solution

Background
• You should love tinkering with compilers, for example LLVM

Deliverables
• Your tool + documentation
• A report showing how powerful your tool is

Scope and Credits
Studies: INF SEW TEL MATH
The scope, effort, and credits of this project are scalable

Advisor/Contact
daniel.hein@iaik.tugraz.at

Graz University of Technology
Institute for Applied Information Processing and Communications
http://www.iaik.tugraz.at/