Attack Surface Prioritization with Crash Dump Stack Traces

Manuscript Review
Chris Theisen, Kim Herzig, Brendan Murphy, Laurie Williams
Change, Complexity, Boundary

Three new types of attack surface metrics:

*Attack surface change over time*: what code was added, what was removed, what’s stayed the same (versions, time)

*Complexity = vulnerabilities?*: do more “fan-in” and “fan-out” edges to code make vulnerabilities more likely?

*Boundary of software systems*: More likely for vulnerabilities to be discovered on the entry and exit points?
Agenda

• Submitting to USENIX on Thursday
  – Our lab has never submitted there, looking for feedback
  – Sections? High-level missing pieces?
• Are the arguments properly motivated?
• Properly blinded?