Vulnerability Discovery

Task 1: Automated and Sound Vulnerability Discovery

Vision: Automatically check DoD software systems for exploitable bugs
Discover vulnerabilities automatically in compiled x86 applications
- “Zero false positives”
- Automatically generate an exploit for each vulnerability; no source code necessary

This project combines expertise from both SEI/CERT and CMU

Task 2: Low-Power Low-Bandwidth System Vulnerabilities

Focuses on vulnerability discovery in Things that have enough compute power to pose a threat to a network they are attached to, but not enough for somebody to think of them as a computer.

1. How do vulnerability discovery techniques for LPLB systems differ from those for traditional computing systems? Are there techniques that do not transfer well? Are there techniques that have shown efficacy in traditional computing but have not showed up on the LPLB side? Why?

2. What processes, tools, and techniques are most effective at improving the security of LPLB systems? For developers and creators of such systems For acquirers, deployers, and operators of such systems

3. What metrics can be applied to assess the efficacy and/or efficiency of those processes?

Contact: Joji Montelibano <jmm137@cert.org>

©2016 Software Engineering Institute
