From: Yan I <yan@trailofbits.com>
Subject: Automated Exploitability Reasoning (AER) Project Update
Date: December 1, 2015 at 12:52:49 PM EST
To: "Law, Joe CIV USARMY RDECOM (US)" <joe.law.civ@mail.mil>
Cc: Andrew Ruef <andrew@trailofbits.com>

Joe,

Since last week’s meeting fell on Thanksgiving, wanted to provide a brief update on the project via email.

We have been focusing on building a proof of concept for a system capable of tracking tainted input to a crashing condition. To that effect, we've been looking at a few directions: the implementation of '!exploitable' extension to WinDbg, and dynamic analysis platforms like Angr and Triton.

We are currently working on two open problems: A way to implement a subset of '!exploitable' rules that we extracted from its source in Triton (or Angr), and determine these tools' capability for taint analysis.

We are currently focusing on Linux binaries due to the amount of documentation and support for that platform, but the tools should be portable to Windows.

In terms of staffing, Andrew Ruef and myself (Yan Ivnitskiy) are the investigators on this project.

If you have any questions, please don't hesitate to get in touch.

Thanks!
Yan