UNIVERSITY of HOUSTON

DEPARTMENT OF COMPUTER SCIENCE

Hacking Oil Rigs for Profit

Weston Hecker
Principal Application Security Engineer/Principal Pentester at NCR Corporation

Date: Friday, March 10, 2017
Time: 3:00 PM – 4:00 PM
Place: Shamrock AB room, Hilton Hotel
University of Houston, Houston, TX

Abstract: This talk will go into detail about how drilling systems communicate and some of the attacks that could be performed on a drilling rig. This includes throwing off toolface information and burning out motors and BITs, Disabling H2S and sour gas detection systems, changing survey data to cause the drilling crew to drill out of zone causing sidetrack and time drilling operations that can cost millions of dollars to a drilling rig. And finally modifying chromatograph information and mud weight causing a blow out and potentially burning a rig to the ground. Infection methods include excel files used by directional drillers and Measurement While Drilling (MWD) staff and 3rd party's.

Research Background: Using a honeypot run as a disposable mail service on TOR, Weston Hecker came across custom tailored malware including several versions of SAMSAM and Cryptolocker. In early May of 2016 he came across a sample that is targeting Wellsite Information Transfer Specification (WITS) and Measure While Drilling (MWD) systems associated with land based drilling platforms. This leads him to do research the attack surface of a drilling rig.

About the Speaker: Weston Hecker has been pen-testing for 11 years and has 12 years of experience doing security research and programming. Weston has recently spoken at Blackhat 2016, Defcon 22, 23 and 24, Enterprise Connect 2016, ISC2-Security Congress, SC-Congress Toronto, BSIDESBoston, TakdownCON, HOPE 11, and at over 50 other speaking engagements from telecom regional events to Universities on security subject matter. Weston works with a major university's research project with Department of Homeland Security on 911 emergency systems and attack mitigation. He attended school in Minneapolis Minnesota and studied Computer Science. Weston found several vulnerabilities in very popular software and firmware, including Microsoft, Qualcomm, Samsung, HTC, and Verizon.

Open to Public. Please register for the talk to help us prepare for the event.
Parking available at Hilton hotel and at the Welcome Center.
Contact: Melissa Nieto (713-743-3350)