CYBERSECURITY LECTURE SERIES

A TOOL FOR REVERSE ENGINEERING MASK ROM FIRMWARE

Feb 27th, 2023 at 3:30 P.M.

DMC Theater, LSU Digital Media Center

Travis Goodspeed

ABSTRACT

After chemically decapsulating, delayering, and staining a microchip, its ROM can be photographed to reveal the physical bits, allowing for its contents to be recovered. This talk will describe how I wrote an open tool in Qt6 and C++ for annotating these photographs to painlessly extract tens of thousands of bits for reverse engineering. The GUI is designed around a QGraphicsScene. The underlying data objects use the QT coordinate system, with floats for better-than-pixel precision. After loading a ROM photograph, the user places Columns and Rows onto the photograph. Every intersection of a column and a row is considered to be a bit, and a configurable color threshold determines the value of that bit. Where the photograph is misread, you can also force the bit to a known value. Once all of the bits have been marked and the threshold chosen, the software will mark every light bit as blue (0) and every dark bit as red (1). These bits are then aligned into linked lists of rows for export as ASCII, for use in other tools. While the primary interface is the GUI, a CLI is also available for scripting and testing.

SPEAKER BIO

Travis Goodspeed (@travisgoodspeed) is a reverse engineer from East Tennessee, where he drives old Studebakers and knows all the good dogs by name. His past projects include a replacement module for calculator watches, a web API for identifying functions in Thumb2 firmware, and the International Journal of PoC||GTFO (Proof-of-Concept or Get the F*** Out) - a journal focused on offensive security, reverse engineering, and file format internals, where contributors must submit working proofs-of-concept together with their articles to prove their ideas work in practice.