Thesis Defense

Computer Science Master's Program

"SPOS: An Attestation Solution for the Detection and Mitigation of Point of Sale Malware"

By **Damian Dhesi**

Abstract:

Securing 95% of card present transactions, accounting for billions of transactions a year, has made EMV the premier protocol for card-based payment. Created by and named after Europay, Mastercard, and Visa, the EMV protocol provides multiple solutions to resolve security concerns with the outdated, swipe-based, magnetic stripe payment. Such solutions are Chip and PIN which provides a more secure transaction at a significant time cost and EMV contactless which provides improved security to Chip and PIN at greater ease of use with its quick, tap-to-pay based payment. However, regardless of how secure the EMV protocol makes the card side of a transaction, little has been done for the Point of Sale (POS) devices involved. While the EMV protocol ensures the validity of the card and the identity of the cardholder, no such checks are made for the POS device during the transaction. All types of card-based payment, EMV or not, are simply at the mercy of how merchants choose to secure their POS devices as there is no choice but to assume a POS device is secure if a transaction is to occur. While this may seem to be a reasonable assumption, the infamy of POS malwares like PoSeidon and BlackPOS prove the danger of relying solely on merchants for POS security. Hence, this thesis presents Secure Point of Sale (SPOS) as a solution leveraging a Hardware Root of Trust (HRoT) installed in the POS device to provide attestation updates to a verification entity that will determine POS integrity. Thus, freeing POS security from being solely reliant on the merchant.

Date: Friday, May 23rd, 2025
Time: 3:00 PM – 5:00 PM
Location: 14-232b
Zoom: https://calpoly.zoom.us/j/6103899523
Committee: Dr. DeBruhl, Dr. Beard, and Dr. Fang