Md Lutfor Rahman
PhD Student, UCR
mrahm011@ucr.edu

The goal of my research is to investigate human-centered security by concentrating the human brain using machine learning approach. I used brain-imaging technology to examine what happens when users make security and privacy related decisions. The goal is to search for clues that could help to find a solution, which would protect the users from malicious maneuvers. I am giving a brief description of my works below.

Exploring Feasibility of Identifying Human Intention Based on EEG in the Context of Accessing Privacy Related Devices on Personal Computing Devices (Work in Progress)

Summary: Can we capture human intention from brain signal? We will explore this feasibility by collecting EEG data with commodity emotiv device from users while playing apps and analyzing EEG data using machine learning(deep learning) algorithms. Human intention can be used in giving permission to some highly sensitive resources like camera, location, and microphone, etc. on personal computing devices.

PEEP: Passively Eavesdropping Private Input via Brainwave Signals. (Under Submission)

Abstract—New emerging devices open up immense opportunities for everyday users. At the same time, they may raise significant security and privacy threats. One such device, forming the central focus of this work, is an EEG headset, which allows a user to control her computer only using her thoughts.

In this paper, we show how such a malicious EEG device or a malicious application having access to EEG signals recorded by the device can be turned into a new form of a keylogger, called PEEP, that passively eavesdrops over user's sensitive typed input, specifically numeric PINs and textual passwords, by analyzing the corresponding neural signals. PEEP works because user's input is correlated with user's innate visual processing as well as hand, eye, and head muscle movements, all of which are explicitly or implicitly captured by the EEG device.

Our contributions are two-fold. First, we design and develop PEEP against a commodity EEG headset and a higher-end medical-scale EEG device based on machine learning techniques. Second, we conduct the comprehensive evaluation with multiple users to demonstrate the feasibility of PEEP for inferring PINs and passwords as they are typed on a physical keyboard, a virtual keyboard, and an ATM-style numeric keypad. Our results show that PEEP can extract sensitive input with an accuracy significantly higher than a random guessing classifier. Compared to prior work on this subject, PEEP is highly surreptitious as it only requires passive monitoring of brain signals, not deliberate, and active strategies that may trigger suspicion and be detected by the user. Also, PEEP achieves orders of magnitude higher accuracies compared to prior active PIN inferring attacks. Our work serves to raise awareness to a potentially hard-to-address threat arising from EEG devices which may remain attached to the users almost invariably soon.

A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings (CCS'15)

Abstract: Detecting phishing attacks (identifying fake vs. real websites) and heeding security warnings represent classical user-centered security tasks subjected to a series of prior investigations. However, our understanding of user behavior underlying these tasks is still not fully mature, motivating further work concentrating at the neuro-physiological level governing the human processing of such tasks.

We pursue a comprehensive three-dimensional study of phishing detection and malware warnings, focusing not only on what users' task performance is but also on how users process these tasks based on: (1) neural activity captured using Electroencephalogram (EEG) cognitive metrics, and (2) eye gaze patterns captured using an eye-tracker. Our primary novelty lies in employing multi-modal neuro-physiological measures in a single study and providing a near realistic setup (in contrast to a recent neuro-study conducted inside an fMRI scanner). Our work serves to advance, extend and support prior knowledge in several significant ways. Specifically, in the context of phishing detection, we show that users do not spend enough time analyzing key phishing indicators and often fail at detecting these attacks, although they may be mentally engaged in the task and subconsciously processing real sites differently from fake sites. In the malware warning tasks, in contrast, we show that users are frequently reading, possibly comprehending, and eventually heeding the message embedded in the warning.

Our study provides an initial foundation for building future mechanisms based on the studied real-time neural and eye gaze features, that can automatically infer a user's "alertness" state, and determine whether or not the user's response should be relied upon.