Abstract:

The proliferation of wearable devices, e.g., smartwatches and activity trackers, with embedded sensors, has already shown its great potential on monitoring and inferring human daily activities. In this talk, I will present a serious security breach of wearable devices in the context of divulging secret information (i.e., key entries) while people accessing key-based security systems. Existing methods of obtaining such secret information rely on installations of dedicated hardware (e.g., video camera or fake keypad), or training with labeled data from body sensors, which restrict use cases in practical adversary scenarios. I will show that a wearable device can be exploited to discriminate mm-level distances and directions of the user’s fine-grained hand movements, which enable attackers to reproduce the trajectories of the user’s hand and further to recover the secret key entries.