

# Securing the Open Softphone

## Kickoff Colloquium

**Wednesday, September 1<sup>st</sup>, 3:30 – 5:30pm**

**Photonics 210, 8 St. Mary's Street**

Or join us by video-conference at <http://met-meet.bu.edu>  
click *Join Meeting* then enter *softphone* for the room name

### Agenda

- Introduction of the group
- Big open research questions
- Educational mission and outreach

### Research Statement:

Mobile wireless devices are now turning into universal handsets: powerful sensor-rich software-controlled computing and communication devices. These "softphones" are increasingly entrusted with maintaining a users' electronic identity, calendars, financial data, and social networking in one device.

The increasing openness of softphones comes with equally large security issues and opportunities, some of which we are only beginning to understand. We proposed a multi-pronged research plan that methodically considers the security implications of the open softphone and focuses on identifying, understanding, and mitigating new security risks.

The project ultimately aims to understand how security problems associated with softphones and their networks are different from those of traditional computers and networks, and how to harness the unique capabilities of softphones for improved security.

This research project is supported by the NSF.

