

SUBJECT: M.S. Thesis Defense

BY: Dennis McMeekan

TIME: Friday, April 23, 2021, 3:30 pm – 4:30 pm

PLACE: <https://wiu.zoom.us/j/99087502468?pwd=QUIEU1hCdkdmcitnMWdJWWVZOG5wQT09>, Virtual

TITLE: Securing WebRTC

COMMITTEE: Dr. Binto George,
Dr. Nilanjan Sen,
Dr. Chunying Zhao

SUMMARY

Real-time communication between two individuals over a web application has become the norm for interaction. WebRTC provides this type of specification without the use of plug-ins or added installations. Being relatively new, not all security features have been examined. Our committee has targeted two specific security concerns, confidentiality violations and IP leaks.

Confidentiality violations involve altering a WebRTC specification to implement covert channels. And if WebRTC is susceptible to covert channels, this will then be mitigated. In relation to IP leaks, this is the idea that when using a WebRTC specification, the public IP address of a user will be available. This can be solved through implementation of a distributed hash table, which will be discussed and explained briefly.