Speakers:

- John Althouse
- Jeff Atkinson

Fingerprinting Encrypted Channels with Bro for High Fidelity Detection

Last year we open sourced JA3, a method for fingerprinting client applications over TLS, and we saw that it was good. This year we tried fingerprinting the server side of the encrypted communication with Bro, and it's even better. Fingerprinting both ends of the channel creates a unique TLS communication fingerprint between client and server making detection of TLS C2 channels in Bro exceedingly easy. I'll explain how in this talk.

What about non-TLS encrypted channels? The same principal can be applied. I'll talk about fingerprinting SSH clients and servers with Bro and what we've observed in our research. Are those SSH clients what they say they are? Maybe not.