Speaker: Fatema Bannat Wala, Security Engineer, University of Delaware

Is Weird really weird?

As we know that BRO produces lots of interesting log files based on the network activity. One of which is weird.log log file, in which Bro logs the interesting activity that is not categorized as normal according to the TCP/IP and protocol standards. Recently we started seeing lot of activity being logged as weird, and hence decided to look into it more to know what they mean and why are they getting logged as weird activity. This talk will present the research done on different weird notices that get flagged in the network traffic and whether they are really 'weird', or just a misconfigured application or misconfigured firewall rules, which is causing the weird patterns in the traffic. We used Bro's weird.log file to do different analysis and troubleshooting of the network and ended up classifying some of the weird notices as normal or interesting for our environment. Also, to compliment the talk, the presentation will talk about some interesting case studies about how we detected some recent security incidents using BRO and used BRO log analysis to paint the complete picture of the compromise and tell the story about what have happened.