Carnegie Mellon University, Heinz College
Network Situational Awareness

Course 95-855
Thursdays, 5:30-8:20
Hamburg Hall, 1003
Class mailing list:
95-855@lists.andrew.cmu.edu

Instructor: Sid Faber
Office Hours by Appointment
Email sfaber@cmu.edu
Class web site:
www.andrew.cmu.edu/course/95-855/
95-855.fabersl.com

Course Description

In the typical mid to large sized network, no single individual has the ability to touch all the systems which generate and consume network data. However, a single individual or group is often responsible for operating and securing the network. When you complete this course, you should be able to analyze mid- to large-scale networks to answer questions such as:

- Is my bandwidth increasing from business-related activity, or from non-work related activity?
- How will my business be impacted by implantation of more stringent security policy?
- Am I positioned to take advantage of cloud-based services?
- How will socio-political uprisings impact my network?

This course will survey Network Situational Awareness techniques with labs. The concept of network situational awareness is to develop a cogent set of observed network characteristics that will inform decision makers as to the wise course to take in defending the network (or, more colloquially, "Know your network. Know the Internet. Know how they work together"). The labs involve investigation of captured network flow information and analysis for useful observable characteristics, with the inclusion of non-flow information where useful.

Textbook

There is no textbook for this course. However, there are reading assignments posted on the course web site which must be completed before class.

Attendance and Participation

Your attendance and participation in class is critical to gaining an understanding of the material. Classes are designed to be interactive and often are most successful when they draw on challenges faced by students.

Grading

Grading policy will be based on your class participation and various homework and project assignments. Additional details will be provided once the data set has been evaluated; however, you can anticipate the flexibility to drive your contribution to the project in your area of interest.

20% Class participation. In addition to attending class, this grade includes participating in classroom discussions, the class mailing list, and demonstrating an interest in the subject material beyond just the references presented by the instructor.

40% Homework assignments. Assignments will be given regularly to prepare for the upcoming week's lecture and to stimulate in-class discussion.

40% Project assignments. Four projects lasting between two to four weeks will be assigned to solidify the concepts discussed in class:

- Packet Analysis
- Metadata Analysis
- Flow Analysis
- Building Situational Awareness

All student projects are expected to be the original product of individual in your group unless otherwise specified. This means that your submissions are expected to be in your own words and the product of your own effort and any detected copying will be considered plagiarism unless appropriate citations are given. Students are cautioned that much of the material available from Internet searches is of dubious quality in this area.

All submissions must be electronic by email to sfaber@cmu.edu. Late assignments will be penalized by 10% of the assignment grade. No submissions will be accepted for submission after graded assignments have been returned to the class.

Schedule of Classes

Date		***Topic***
1	Aug 30	Introduction and Current Events
2	Sep 6	Layer 3 Services
3	Sep 13	Layer 3 Services (2)
4	Sep 20	Layer 2 Addressing
5	Sep 27	Layer 2 Routing
6	Oct 4	Layer 2 Anomalies
7	Oct 11	Layer 1 Local Networks
8	Oct 18	Network Situational Awareness
9	Oct 25	Layer 1 Global Networks
10	Nov 1	Malicious Traffic
11	Nov 8	Enterprise Sensor Grids
12	Nov 15	Network Situational Awareness and Information Warfare
	Nov 22	*No Class – Thanksgiving Holiday*
13	Nov 29	Intelligence and Global Network Conflicts
14	Dec 6	The Network Operations Center