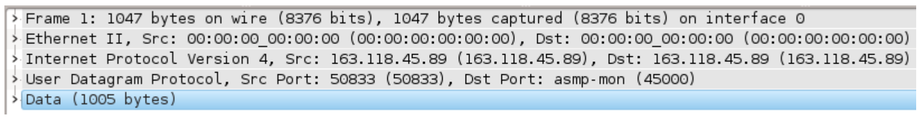
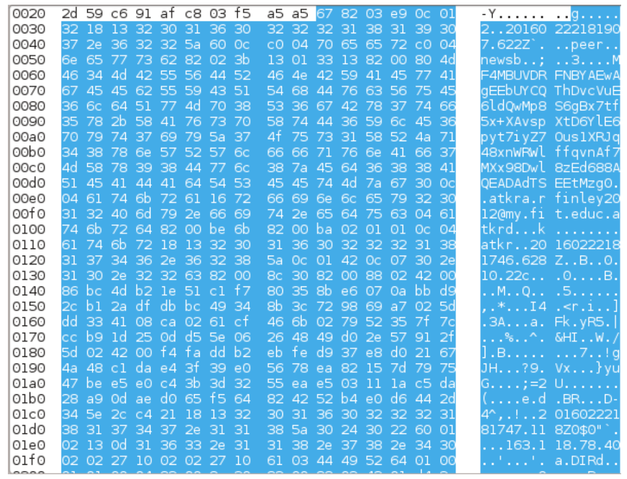
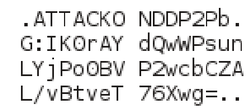
Denial Of Service on Direct Democracy Peer to Peer Protocol

Robert Finley **Brandi Busick** **Ben Mathew**

Faculty Advisor/s: Marius Silaghi , Dept. of Computer Science, Florida Institute of Technology







Abstract

The purpose of this project is to provide the first-ever implementation of a suspected vulnerability to the DDP2P app so that Dr. Silaghi's research students can understand the impact of a such a major vulnerability and take preventative measures. If the vulnerability is shown to be benign we shall present our findings as such. Our main project goal is to thoroughly research and conduct this case and present our findings.

Methods

Using the source code from the DDP2P application we have created an "Attacker" application, which will send out fake data IDs to the network. When other users request the data our attacker will not respond. We then use Wireshark to capture the information sent over the network to determine whether the attack is successful.

Attacker Agent

After the attacker agent infiltrates the DDP2P virtual network, it will need to scan the environment for potential targets. These targets will primarily be those user agents that openly broadcast their interests, friends, and groups. Using the information from the target, the attacker agent will send spoofed messages that pose as new/interesting information relevant to the target's interests. For our purposes though, we have created our own network of fake users to attack.

Tools

Wireshark:

We have to use this tool to collect detailed information about the Denial of Service attack on the virtual network. This will determine the effectiveness of the attack.

ASN1 Encoding:

Messages over the network are encoded using ASN-1 encoding protocol.

NORTHROP GRUMMAN

Engineering & Science Student Design Showcase at Florida Institute of Technology