

# 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

```
> Frame 1: 1047 bytes on wire (8376 bits), 1047 bytes captured (8376 bits) on interface 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 163.118.45.89 (163.118.45.89), Dst: 163.118.45.89 (163.118.45.89)
> User Datagram Protocol, Src Port: 50833 (50833), Dst Port: asmp-mon (45000)
> Data (1005 bytes)
```

```
0020 2d 59 c6 91 af c8 03 f5 a5 a5 67 82 03 e9 0c 01 -Y.....g....
0030 32 18 13 32 30 31 36 30 32 32 32 31 38 31 39 30 2..20160 22218190
0040 37 2e 36 32 32 5a 60 0c c0 04 70 65 65 72 c0 04 7.622Z' ..peer..
0050 6e 65 77 73 62 82 02 3b 13 01 33 13 82 00 80 4d newsb.; .3...M
0060 46 34 4d 42 55 56 44 52 46 4e 42 59 41 45 77 41 F4MBUVD R FNYAEWA
0070 67 45 45 62 55 59 43 51 54 68 44 76 63 56 75 45 gEEbUYCQ ThDvcVuE
0080 36 6c 64 51 77 4d 70 38 53 36 67 42 78 37 74 66 6ldQwM8 S6gBx7tF
0090 35 78 2b 58 41 76 73 70 58 74 44 36 59 6c 45 36 5x+XAvsp XtD6YlEe
00a0 70 79 74 37 69 79 5a 37 4f 75 73 31 58 52 4a 71 pyt7iyZ7 Ous1XRJg
00b0 34 38 78 6e 57 52 57 6c 66 66 71 76 6e 41 66 37 48xnwFwL ffqvnAf7
00c0 4d 58 78 39 38 44 77 6c 38 7a 45 64 36 38 38 41 Mxx98DwL 8zEd688A
00d0 51 45 41 44 41 64 54 53 45 45 74 4d 7a 67 30 0c QEADADTS EEtMzg0.
00e0 04 61 74 6b 72 61 16 72 66 69 6e 6c 65 79 32 30 .atkra.r finley20.
00f0 31 32 40 6d 79 2e 66 69 74 2e 65 64 75 63 04 61 l2omy.f1 t.educ.a
0100 74 6b 72 64 82 00 be 6b 82 00 ba 02 01 01 0c 04 tkrd..k .....
0110 61 74 6b 72 18 13 32 30 31 36 30 32 32 31 38 atkr..20 16022218
0120 31 37 34 36 2e 36 32 38 5a 0c 01 42 0c 07 30 2e 1746.628 Z..B..0.
0130 31 30 2e 32 32 63 82 00 8c 30 82 00 88 02 42 00 10.22c...o...B.
0140 86 bc 4d b2 1e 51 c1 f7 80 35 8b e6 07 0a bb d9 ..M..Q...5.....
0150 2c b1 2a df db bc 49 34 8b 3c 72 98 69 a7 02 5d ..*..I4 <r..l..l
0160 dd 33 41 08 ca 02 61 cf 46 6b 02 79 52 35 7f 7c .3A..a. Fk.yRS.l
0170 cc b9 1d 25 0d d5 5e 06 26 48 49 d0 2e 57 91 2f ..*..^..6HI..w./
0180 5d 02 42 00 f4 fa dd b2 eb fe d9 37 e8 d0 21 67 l.B.....7..lg
0190 4a 48 c1 da e4 3f 39 e0 56 78 ea 82 15 7d 79 75 JH..79. Vx...}yu
01a0 47 be e5 e0 c4 3b 3d 32 55 ea e5 03 11 1a c5 da G...;=2 U.....
01b0 28 a9 0d ae d0 65 f5 64 82 42 52 b4 e0 d6 44 2d (...e.d..BR..D.
01c0 34 5e 2c c4 21 18 13 32 30 31 36 30 32 32 32 31 47..l..2 01602221
01d0 38 31 37 34 37 2e 31 31 38 5a 30 24 30 22 60 01 81747.11 82040*
01e0 02 13 0d 31 36 33 2e 31 31 38 2e 37 38 2e 34 30 ...163.118.78.40
01f0 02 02 27 10 02 27 10 61 03 44 49 52 64 01 00 ..... a.DIR..
```

Name

Method

Initiator

Identity

```
.ATTACKO NDDP2Pb.
G:IKOrAY dQwWPSun
LYjPo0BV P2wcbCZA
L/vBtveT 76Xwg=..
```

## 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

