OSPF ROUTE INJECTION

PRESENTER: GARY MCCULLY

DATE: DECEMBER 8TH, 2021

MAIN IDEAS

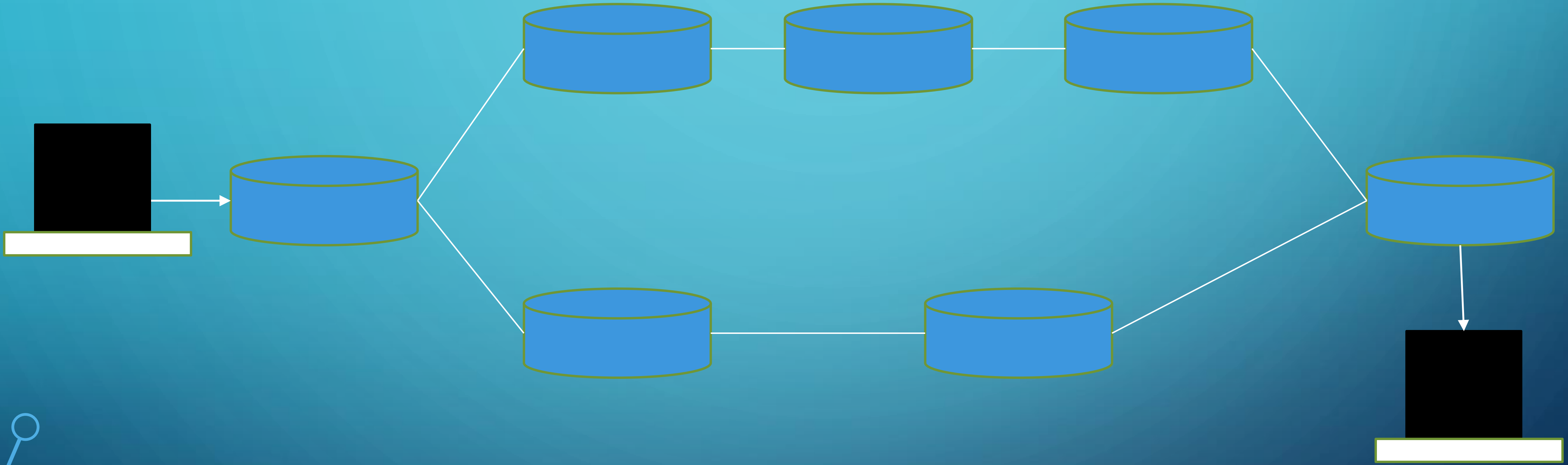
- Routers are used to move network packets across the network to their intended recipient. To ensure packets are routed through the most efficient path possible, protocols such as OSPF are used within large organizations. OSPF also enables networks to "self-heal" in the event that one of the routers goes down.

- In many cases, OSPF is misconfigured and traffic that should only be sent and received by other routers within the OSPF topology can be sent and received by other network segments. These segments may include segments used for end-user computing or segments used by the organization's servers.

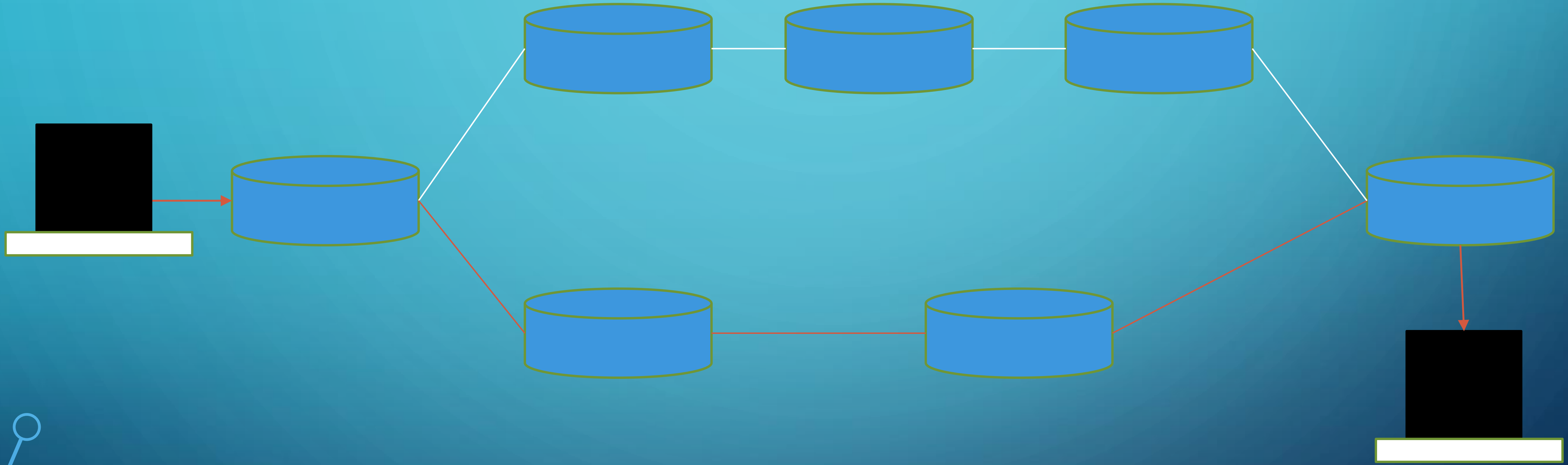
- Even when the servers used within the OSPF topology use authentication, it may be possible for an attacker to insert malicious routes within the network topology that can result in a DoS condition, enable an attacker to view sensitive information, or impersonate a different system.

OSPF INTRODUCTION (MAIN IDEAS 1)

THE PROBLEM

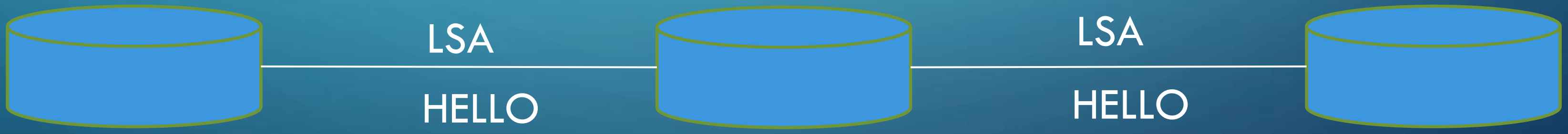


THE SOLUTION (OPEN SHORTEST PATH FIRST)



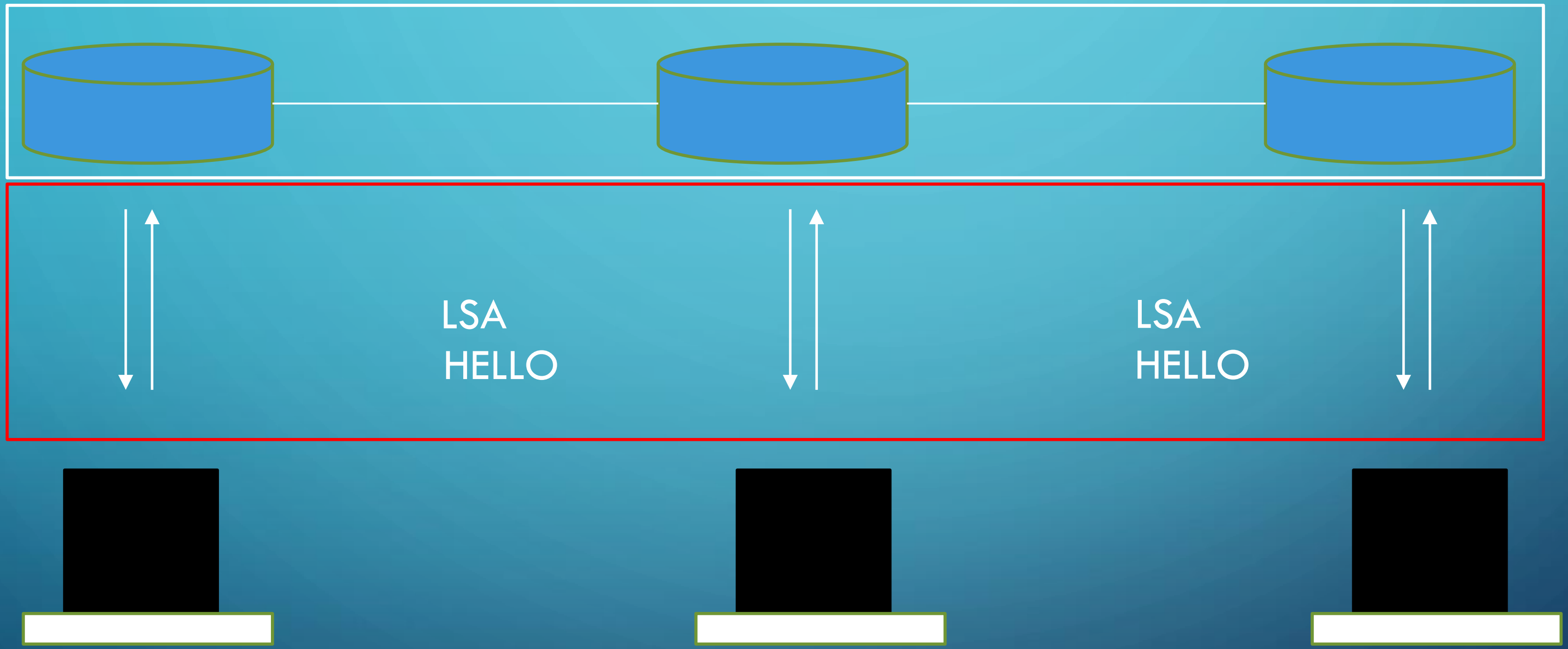
LINK STATE ADVERTISEMENTS (LSA) & HELLO PACKETS

- LSA
  - Sent between routers to share information
  - 8 Different LSA Types (Router, Network, etc.)
  - Type 1 (Router LSA)
    - Connected routers
    - Connected Networks
    - Etc.
  - Hello Packets
    - Discover and Maintain Neighbor Relationships



MISCONFIGURATIONS (MAIN IDEA 2)

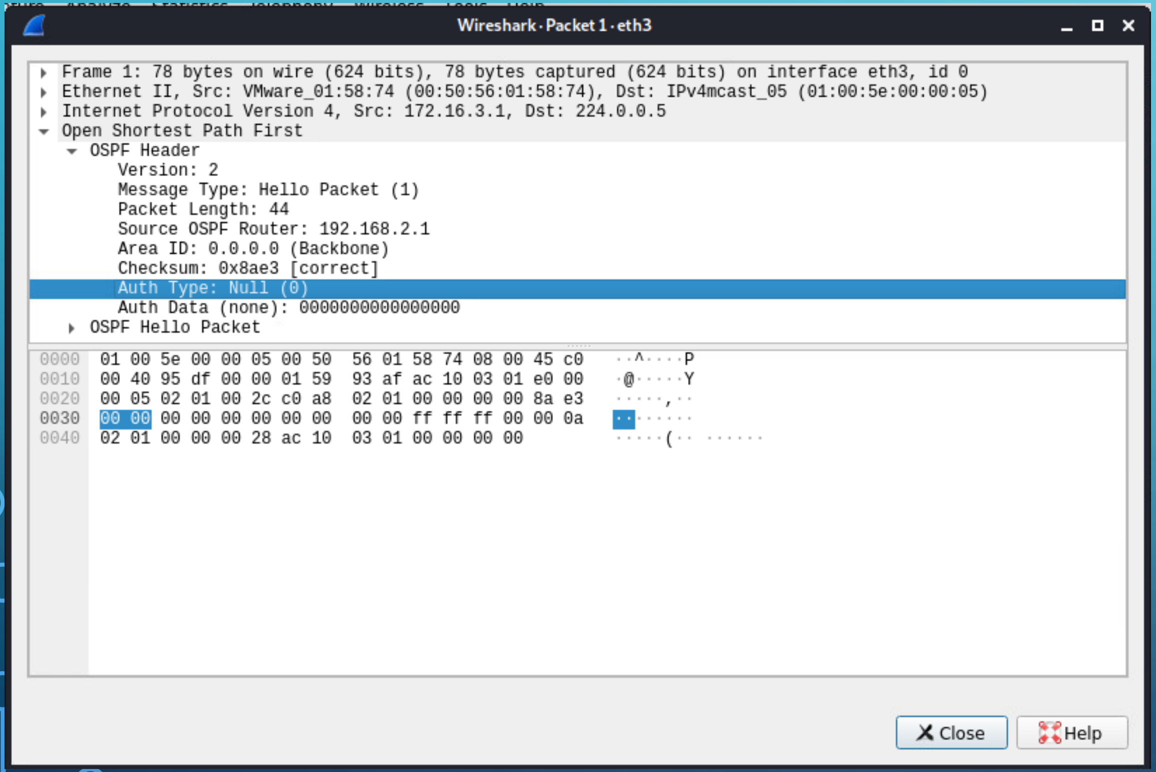
THE SOLUTION (OPEN SHORTEST PATH FIRST)



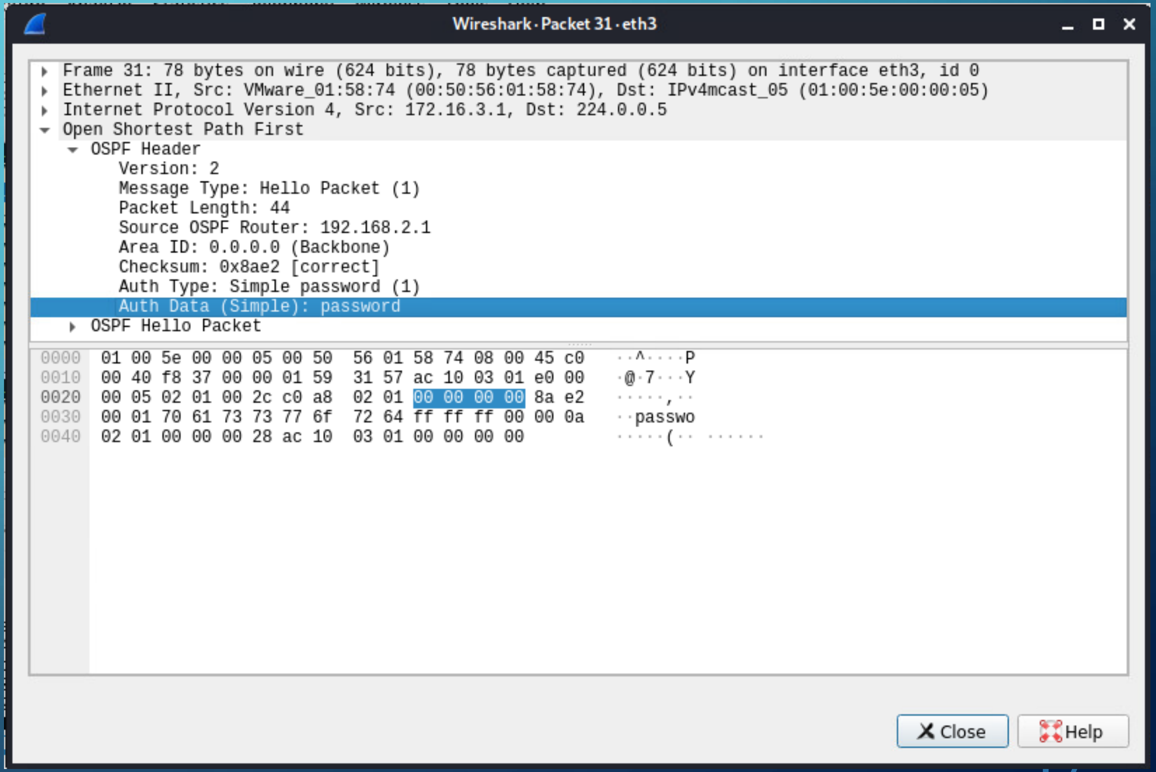
AUTHENTICATION ISSUES (MAIN IDEA 3)

SECURITY

- Type 1: No Authentication
- Type 2: Clear Text
- Type 3: Cryptographic (MD5)

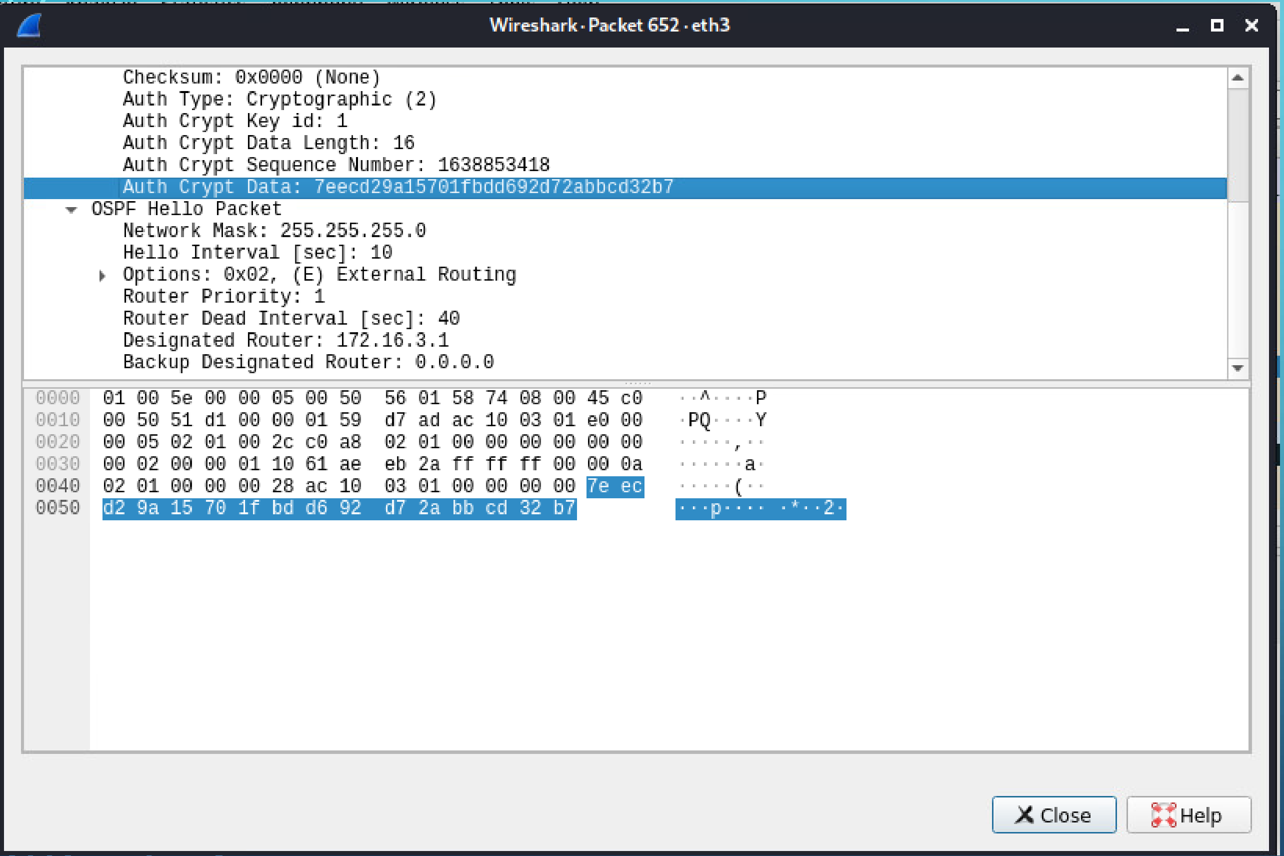


```
▸ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth3, id 0
▸ Ethernet II, Src: VMware_01:58:74 (00:50:56:01:58:74), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
▸ Internet Protocol Version 4, Src: 172.16.3.1, Dst: 224.0.0.5
▾ Open Shortest Path First
  ▾ OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 44
      Source OSPF Router: 192.168.2.1
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0x8ae3 [correct]
      Auth Type: Null (0)
      Auth Data (none): 0000000000000000
  ▸ OSPF Hello Packet

0000  01 00 5e 00 00 05 00 50  56 01 58 74 08 00 45 c0   ··^····P V·Xt··E·
0010  00 40 95 df 00 00 01 59  93 af ac 10 03 01 e0 00   ·@·····Y ········
0020  00 05 02 01 00 2c c0 a8  02 01 00 00 00 00 8a e3   ·····,·· ········
0030  00 00 00 00 00 00 00 00  00 00 ff ff ff 00 00 0a   ········ ········
0040  02 01 00 00 00 28 ac 10  03 01 00 00 00 00         ·····(·· ······
```



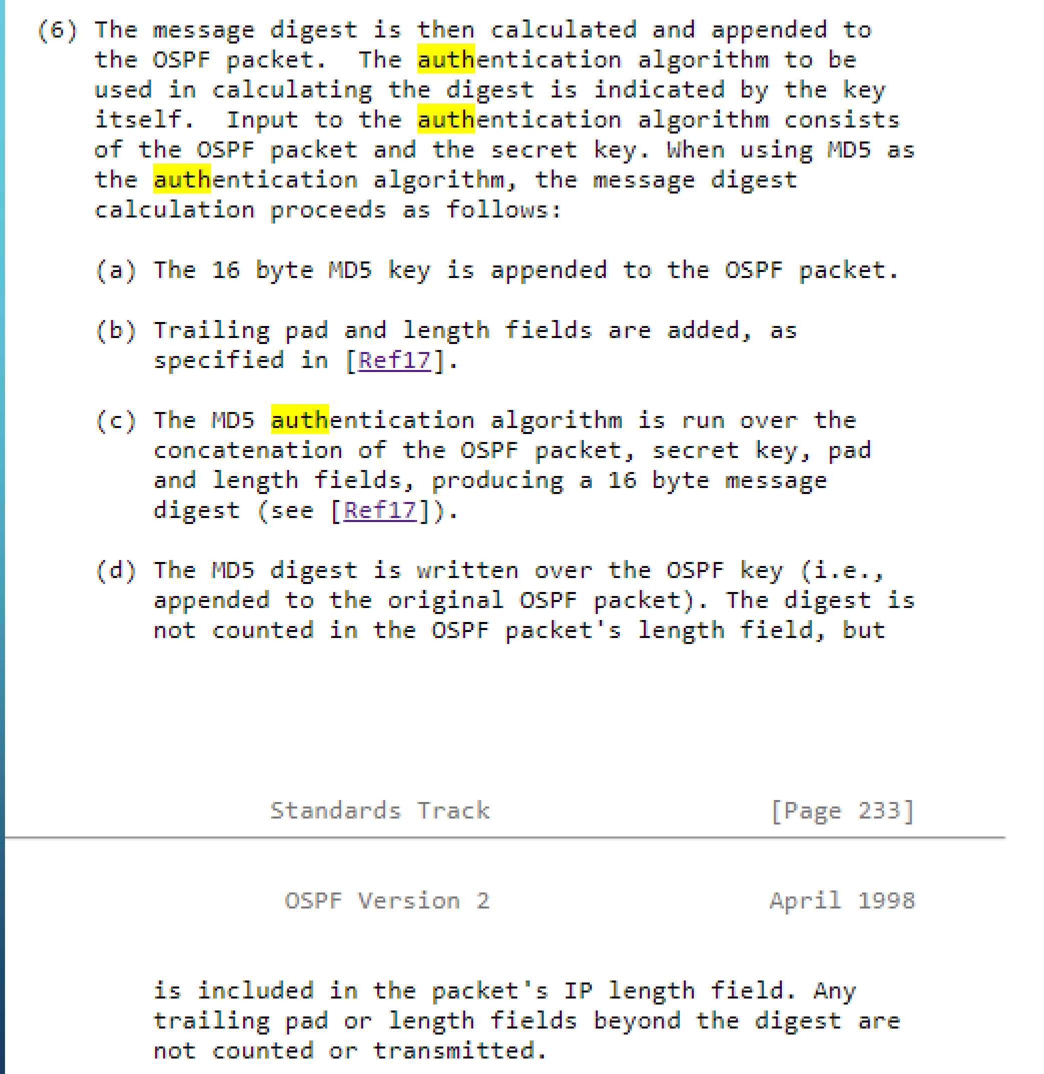
```
▸ Frame 31: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth3, id 0
▸ Ethernet II, Src: VMware_01:58:74 (00:50:56:01:58:74), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
▸ Internet Protocol Version 4, Src: 172.16.3.1, Dst: 224.0.0.5
▾ Open Shortest Path First
  ▾ OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 44
      Source OSPF Router: 192.168.2.1
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0x8ae2 [correct]
      Auth Type: Simple password (1)
      Auth Data (Simple): password
  ▸ OSPF Hello Packet

0000  01 00 5e 00 00 05 00 50  56 01 58 74 08 00 45 c0   ··^····P V·Xt··E·
0010  00 40 f8 37 00 00 01 59  31 57 ac 10 03 01 e0 00   ·@·7···Y 1W······
0020  00 05 02 01 00 2c c0 a8  02 01 00 00 00 00 8a e2   ·····,·· ········
0030  00 01 70 61 73 73 77 6f  72 64 ff ff ff 00 00 0a   ··passwo rd······
0040  02 01 00 00 00 28 ac 10  03 01 00 00 00 00         ·····(·· ······
```

SECURITY (TYPE 3)



```
        Checksum: 0x0000 (None)
        Auth Type: Cryptographic (2)
        Auth Crypt Key id: 1
        Auth Crypt Data Length: 16
        Auth Crypt Sequence Number: 1638853418
        Auth Crypt Data: 7eecd29a15701fbdd692d72abbcd32b7
    ▾ OSPF Hello Packet
        Network Mask: 255.255.255.0
        Hello Interval [sec]: 10
      ▸ Options: 0x02, (E) External Routing
        Router Priority: 1
        Router Dead Interval [sec]: 40
        Designated Router: 172.16.3.1
        Backup Designated Router: 0.0.0.0
```

```
0000  01 00 5e 00 00 05 00 50  56 01 58 74 08 00 45 c0   ··^····P
0010  00 50 51 d1 00 00 01 59  d7 ad ac 10 03 01 e0 00   ·PQ····Y
0020  00 05 02 01 00 2c c0 a8  02 01 00 00 00 00 00 00   ·····,··
0030  00 02 00 00 01 10 61 ae  eb 2a ff ff ff 00 00 0a   ······a·
0040  02 01 00 00 00 28 ac 10  03 01 00 00 00 00 7e ec   ·····(··
0050  d2 9a 15 70 1f bd d6 92  d7 2a bb cd 32 b7         ···p···· ·*··2·
```



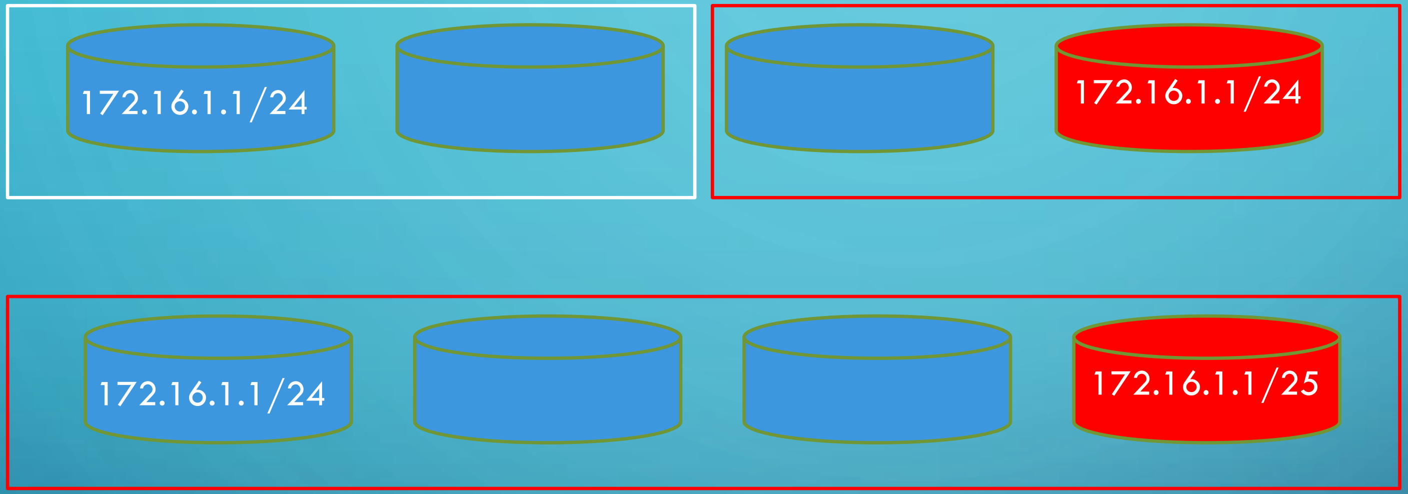
```
(6) The message digest is then calculated and appended to
    the OSPF packet.  The authentication algorithm to be
    used in calculating the digest is indicated by the key
    itself.  Input to the authentication algorithm consists
    of the OSPF packet and the secret key. When using MD5 as
    the authentication algorithm, the message digest
    calculation proceeds as follows:

    (a) The 16 byte MD5 key is appended to the OSPF packet.

    (b) Trailing pad and length fields are added, as
        specified in [Ref17].

    (c) The MD5 authentication algorithm is run over the
        concatenation of the OSPF packet, secret key, pad
        and length fields, producing a 16 byte message
        digest (see [Ref17]).

    (d) The MD5 digest is written over the OSPF key (i.e.,
        appended to the original OSPF packet). The digest is
        not counted in the OSPF packet's length field, but



              Standards Track                    [Page 233]

              OSPF Version 2                     April 1998


        is included in the packet's IP length field. Any
        trailing pad or length fields beyond the digest are
        not counted or transmitted.
```

OSPF ROUTE HIJACK WITH PFSENSE AND CAIN AND ABEL (DEMO)

WHY EXPLOIT WITH PFSENSE?

- Most Write-Ups use Loki
- Loki uses many deprecated packages
- OSPF traffic originating from PFSense may be considered less suspicious
- PFSense is used by many organizations and is actively maintained

DEMO LESSONS LEARNED



FUTURE DIRECTION

- New Tools Needed for OSPF Route Injection
- New Tools Needed for OSPF MD5 Cracking
- Can an “attack” plugin be created for pfSense?
- Create playbooks for bring your own infrastructure
- Router Priority Testing