Man-in-the-Middle and Denial-of-Service with ARP Poisoning

Uğurcan Arıkan - Alim Türkmen

24 December 2018

Contents

ARP Request

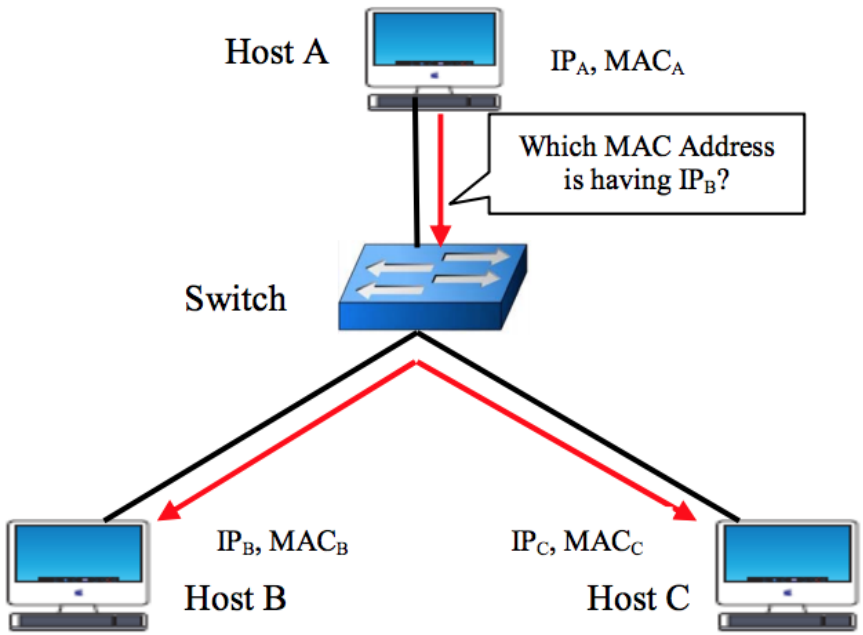


FIGURE – ARP Request

ARP Reply

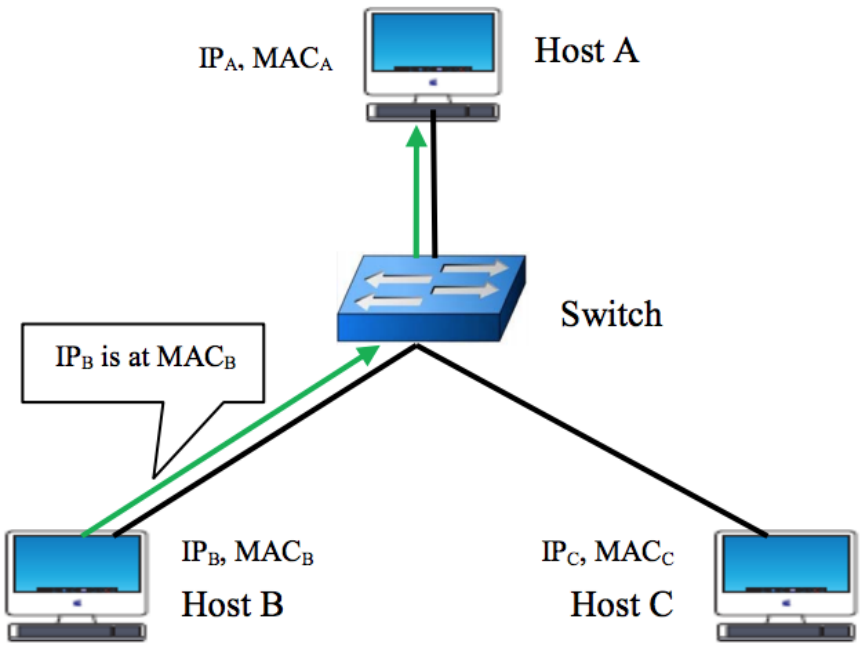
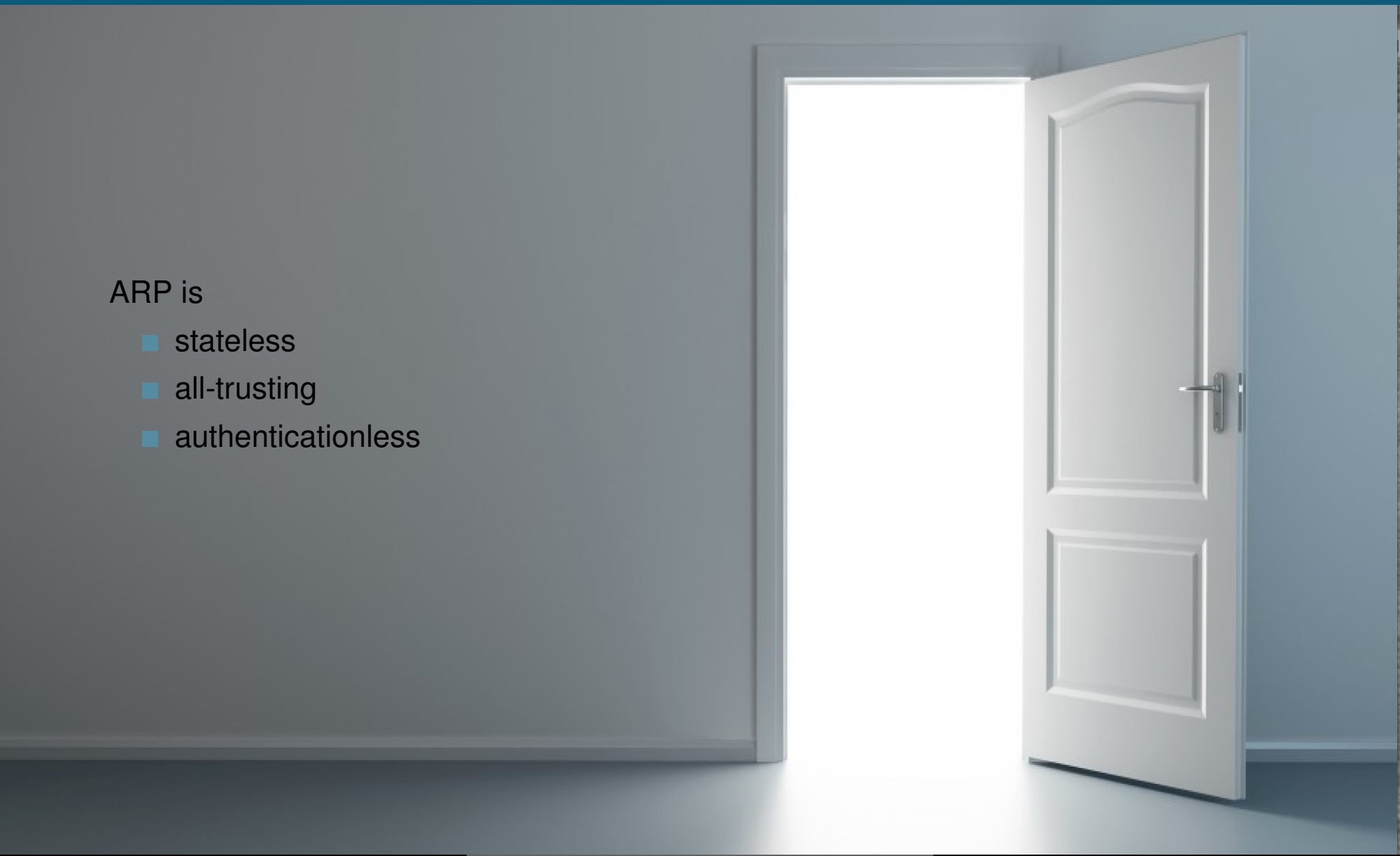


FIGURE – ARP Reply

ARP Weaknesses



ARP is

- stateless
- all-trusting
- authenticationless

ARP Poisoning

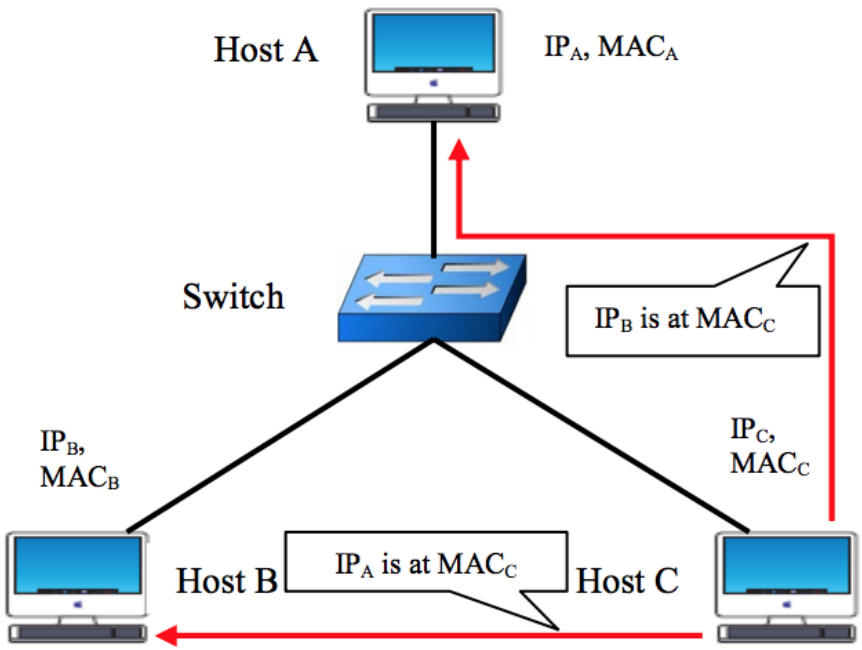


FIGURE – ARP Poisoning

After Poisoning

- Man-in-the-middle
- Denial-of-Service

Project Motivation

- Acquire people's private sensitive data
- **Vandalism**
- Using network resources more effectively

Network Security

```
###[ Ethernet ]###
  dst       = 6c:40:08:93:f8:ae
  src       = fc:4a:e9:de:ad:05
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 208
     id        = 61990
     flags     =
     frag      = 0
     ttl       = 245
     proto     = tcp
     chksum    = 0x660d
     src       = 216.58.212.3
     dst       = 192.168.0.13
     \options   \
###[ TCP ]###
        sport     = https
        dport     = 53095
        seq       = 2059526612
        ack       = 3192336098
        dataofs   = 8
        reserved  = 0
        flags     = PA
        window    = 240
        chksum    = 0xef57
        urgptr    = 0
        options   = [('NOP', None), ('NOP', None), ('Timestamp', (3974894282, 30113153))]
###[ Raw ]###
           load      = '\x16\x03\x03\x00d\x02\x00\x00`\x03\x03\\\x1f\xed\x82u\x88\xaa\xb1)\x9b\xe8\x92\xcdy\xc9\xb9\x83\xc
0\xc5\xb1h\xfe\x89\xd6\xb2\n\x9c<\x17\xdd\x177 \x01\x95\xf4\rG!\xd7:\xf7\xcdX\xb2\x9f\xac\t~\x8ep~x}J\xb7*N\x84!CP\x81\x13
\xe5\xc0+\x00\x00\x18\x00\x17\x00\x00\xff\x01\x00\x01\x00\x00\x0b\x00\x02\x01\x00\x00\x10\x00\x05\x00\x03\x02h2\x14\x03\x0
3\x00\x01\x01\x16\x03\x03\x00(\x00\x00\x00\x00\x00\x00\x00\x00\x07;\xf3\xc5]\t/\x82\x1f\xe6\xd0i\xa5vB\xfa\xef\xb2\x9f\x1c
\xde\xe7\x80!X\xa3\xf0\xd6?\xc4\x93\xfa'
```

FIGURE – Encrypted load

Network Security

```
###[ Ethernet ]###
  dst       = 6c:40:08:93:f8:ae
  src       = fc:4a:e9:de:ad:05
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x2
     len       = 1500
     id        = 32441
     flags     = DF
     frag      = 0
     ttl       = 244
     proto     = tcp
     chksum    = 0x99ef
     src       = 51.144.116.43
     dst       = 192.168.0.13
     \options   \
###[ TCP ]###
        sport     = http
        dport     = 53065
        seq       = 423157448
        ack       = 564087335
        dataofs   = 8
        reserved  = 0
        flags     = A
        window    = 1026
        chksum    = 0x1dad
        urgptr    = 0
        options   = [('NOP', None), ('NOP', None), ('Timestamp', (401541522, 30128794))]
###[ Raw ]###
           load      = '=\'div-gpt-ad-1508227432634-0\'>\n<script>\ngoogletag.cmd.push(function() { googletag.display(\'div-gpt-ad-1508227432634-0\')
; });\n</script>\n</div>\n<div class=\'display-block mb_10\'></div>\r\n                    </div>\r\n                    <div class="partialC
ontent" data-url="/rssbox/rssbox"></div>\r\n                    \r\n                    <!-- /300x250-->\r\n                    <div clas
s="cphsidebar">\r\n                    \r\n\r\n\r\n<script src="//media-cf.tr.beinsports.com/App_Themes/2011/js/bundle/ticker?v=5m4CaRrLSUMyW
f3FX_lmcqP3O29K1WbovxJhXl1pFWY1"></script>\r\n\r\n\r\n\r\n\r\n<script type="text/javascript">\r\n    $(document).ready(function() {\r\n        var interv
alId = setInterval(function() { RefreshLiveScoreTicker(); }, 60000);\r\n    });\r\n</script>\r\n<input type="hidden" id="hidden_videolig_actionUrl" v
alue="/_AjaxServices/VideoLeagueService" />\r\n<div id="ticker_container" clientidmode="Static" style=&#39;display:none;&#39;>\r\n</div>\r\n<script t
ype="text/x-jQuery-tmpl" id="ticker_template">\r\n    <a onclick="return false;" href="javascript:void(0);"\r\n        class="spr side_title">\r\n
```

FIGURE – Non-Encrypted load

Network Security

```
###[ DNS ]###
           id        = 9017
           qr        = 1
           opcode    = QUERY
           aa        = 0
           tc        = 0
           rd        = 1
           ra        = 1
           z         = 0
           ad        = 0
           cd        = 0
           rcode     = ok
           qdcount   = 1
           ancount   = 1
           nscount   = 0
           arcount   = 0
           \qd        \
            |###[ DNS Question Record ]###
            |  qname     = 'registration.boun.edu.tr.'
            |  qtype     = A
            |  qclass    = IN
           \an        \
            |###[ DNS Resource Record ]###
            |  rrname    = 'registration.boun.edu.tr.'
            |  type      = A
            |  rclass    = IN
            |  ttl       = 84838
            |  rdlen     = 4
            |  rdata     = '193.140.204.216'
```

Finding Host Name

```
finding all the hosts with mac addresses in the lan
192.168.4.0 at ff:ff:ff:ff:ff:ff
192.168.4.1 at 0:e0:b1:c2:c5:a6 as gateway
192.168.4.3 at 1c:15:1f:74:3c:17
192.168.4.7 at b8:63:4d:8:31:ed
192.168.4.12 at 54:26:96:cd:ae:dd
192.168.4.17 at f4:5c:89:c5:3f:9d
192.168.4.19 at d8:8f:76:79:52:2
192.168.4.21 at d4:38:9c:1a:d8:cb
192.168.4.28 at c8:3d:d4:83:65:9
192.168.4.30 at 8c:85:90:d8:93:89
192.168.4.34 at 88:e9:fe:83:36:1a
192.168.4.41 at e4:9a:79:b7:19:6f
192.168.4.51 at dc:74:a8:cb:43:75
192.168.4.52 at 68:d9:3c:52:9d:4e
192.168.4.57 at 74:e5:f9:34:82:b7
192.168.4.58 at 98:ca:33:97:3a:87
192.168.4.63 at f0:99:b6:5:f2:fc
192.168.4.65 at 4c:66:41:d0:9f:df
192.168.4.66 at 64:70:33:c2:79:5d
192.168.4.68 at 6c:40:8:93:f8:ae
192.168.4.69 at 6c:71:d9:a2:a2:39
192.168.4.70 at f4:60:e2:a5:10:6c
192.168.4.71 at e0:94:67:7f:10:34
192.168.4.73 at 78:88:6d:8d:ed:e0
192.168.4.74 at 7c:46:85:34:32:e7
192.168.4.75 at 60:3:8:9d:92:c4
192.168.4.76 at 80:e6:50:3:3d:26
192.168.4.77 at 2c:f0:ee:17:8a:1c
192.168.4.82 at 78:7b:8a:84:1e:ef
192.168.4.86 at 8:e6:89:eb:c4:a8
192.168.4.89 at a4:50:46:18:1d:5
192.168.4.91 at 40:a3:cc:87:53:2a
192.168.4.94 at f0:98:9d:9b:6a:73
192.168.4.95 at 6c:72:e7:8c:fa:b7
192.168.4.98 at ec:d0:9f:ed:b3:b9
192.168.4.99 at b4:b6:76:7d:e1:28
192.168.4.220 at 9c:b6:d0:e9:c8:39
```

FIGURE – Fishes in the sea

Tools Used

- **Python3**, obviously
- **Scapy**
- Wireshark
- Socket

Possible Enhancements

- Performing denial-of-service to LAN
- Finding host' usernames
- Filtering non-encrypted data

Conclusion

- Can perform denial-of-service
- Can perform man-in-the-middle, cannot decrypt data
- Questions ?