DHCP Security

Zaeem Israr, Leo Sterner, Alan Tang

A presentation for EECS4482 at York University, Fall 2019

Introduction

- **Introduction**
- Attacks
- Mitigations

- What?
- How?
- Why? (Benefits)

What is DHCP?

- Dynamic Host Configuration Protocol
- Replaced BOOTP
- Automatically assigns the following information to a host on the network
  - IP Address
  - Subnet Mask
  - Default Gateway
  - DNS Address
- Most routers have the ability to provide DHCP server support

How does DHCP work?

- Operates based on Client-Server Model

- Uses UDP
  - UDP Port 67 = server destination/source
  - UDP Port 68 = client destination/source

- Allocation Methods
  - Dynamic Allocation
  - Automatic Allocation
  - Manual Allocation

How does DHCP work?

- Four phases (DORA):
  - Server discovery
  - IP lease offer
  - IP lease request
  - IP lease acknowledgement

- Server Discovery = DHCPDISCOVER

Example DHCPDISCOVER message

Ethernet: source=sender's MAC; destination=FF:FF:FF:FF:FF:FF			
IP: source=0.0.0.0; destination=255.255.255.255 UDP: source port=68; destination port=67			
Octet 0	**Octet 1**	**Octet 2**	**Octet 3**
OP	**HTYPE**	**HLEN**	**HOPS**
0x01	0x01	0x06	0x00
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0x00000000			
SIADDR (Server IP address)			
0x00000000			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s, or overflow space for additional options; BOOTP legacy.			
Magic cookie			
0x63825363			
DHCP options			
0x350101 53: 1 (DHCP Discover)			
0x3204c0a80164 50: 192.168.1.100 requested			
0x370401030f06 55 (Parameter Request List): • 1 (Request Subnet Mask), • 3 (Router), • 15 (Domain Name), • 6 (Domain Name Server)			
0xff 255 (Endmark)			

DORA

IP Lease Offer = DHCPOFFER

DHCPOFFER message			
Ethernet: source=sender's MAC; destination=client mac address			
IP: source=192.168.1.1; destination=255.255.255.255 UDP: source port=67; destination port=68			
Octet 0	**Octet 1**	**Octet 2**	**Octet 3**
OP	**HTYPE**	**HLEN**	**HOPS**
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0xC0A80164 (192.168.1.100)			
SIADDR (Server IP address)			
0xC0A80101 (192.168.1.1)			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s; BOOTP legacy.			
Magic cookie			
0x63825363			
DHCP options			
53: 2 (DHCP Offer)			
1 (subnet mask): 255.255.255.0			
3 (Router): 192.168.1.1			
51 (IP address lease time): 86400s (1 day)			
54 (DHCP server): 192.168.1.1			
6 (DNS servers): • 9.7.10.15, • 9.7.10.16,			

IP Lease Request = DHCPREQUEST

DHCPREQUEST message			
Ethernet: source=sender's MAC; destination=FF:FF:FF:FF:FF:FF			
IP: source=0.0.0.0; destination=255.255.255.255;[a] UDP: source port=68; destination port=67			
Octet 0	**Octet 1**	**Octet 2**	**Octet 3**
OP	**HTYPE**	**HLEN**	**HOPS**
0x01	0x01	0x06	0x00
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0x00000000			
SIADDR (Server IP address)			
0xC0A80101 (192.168.1.1)			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s; BOOTP legacy.			
Magic cookie			
0x63825363			
DHCP options			
53: 3 (DHCP Request)			
50: 192.168.1.100 requested			
54 (DHCP server): 192.168.1.1			

DORA

IP Lease Acknowledgement = DHCPACK

DHCPACK message			
Ethernet: source=sender's MAC; destination=client's MAC			
IP: source=192.168.1.1; destination=255.255.255.255 UDP: source port=67; destination port=68			
Octet 0	**Octet 1**	**Octet 2**	**Octet 3**
OP	**HTYPE**	**HLEN**	**HOPS**
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0xC0A80164 (192.168.1.100)			
SIADDR (Server IP address)			
0xC0A80101 (192.168.1.1)			
GIADDR (Gateway IP address switched by relay)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s. BOOTP legacy			
Magic cookie			
0x63825363			
DHCP options			
53: 5 (DHCP ACK) or 6 (DHCP NAK)			
1 (subnet mask): 255.255.255.0			
3 (Router): 192.168.1.1			
51 (IP address lease time): 86400s (1 day)			
54 (DHCP server): 192.168.1.1			
6 (DNS servers): • 9.7.10.15, • 9.7.10.16,			

Options:

Code	Name	Length	Notes
0	Pad[13]:Section 3.1	0 octets	Can be used to pad other options so that they are aligned to the word boundary; is not followed by length byte
1	Subnet mask[13]:Section 3.3	4 octets	Must be sent before the router option (option 3) if both are included
2	Time offset[13]:Section 3.4	4 octets	
3	Router	Multiples of 4 octets	Available routers, should be listed in order of preference
4	Time server	Multiples of 4 octets	Available time servers to synchronise with, should be listed in order of preference
5	Name server	Multiples of 4 octets	Available IEN 116 name servers, should be listed in order of preference
6	Domain name server	Multiples of 4 octets	Available DNS servers, should be listed in order of preference
7	Log server	Multiples of 4 octets	Available log servers, should be listed in order of preference.
8	Cookie server	Multiples of 4 octets	*Cookie* in this case means "fortune cookie" or "quote of the day", a pithy or humorous anecdote often sent as part of a logon process on large computers; it has nothing to do with cookies sent by websites.
9	LPR Server	Multiples of 4 octets	
10	Impress server	Multiples of 4 octets	
11	Resource location server	Multiples of 4 octets	
12	Host name	Minimum of 1 octet	
13	Boot file size	2 octets	Length of the boot image in 4KiB blocks
14	Merit dump file	Minimum of 1 octet	Path where crash dumps should be stored
15	Domain name	Minimum of 1 octet	
16	Swap server	4 octets	
17	Root path	Minimum of 1 octet	
18	Extensions path	Minimum of 1 octet	
255	End	0 octets	Used to mark the end of the vendor option field

IP layer parameters per host[13]:Section 4

Code	Name	Length	Notes
19	IP forwarding enable/disable	1 octet	
20	Non-local source routing enable/disable	1 octet	
21	Policy filter	Multiples of 8 octets	
22	Maximum datagram reassembly size	2 octets	
23	Default IP time-to-live	1 octet	
24	Path MTU aging timeout	4 octets	
25	Path MTU plateau table	Multiples of 2 octets	

IP Layer Parameters per Interface[13]:Section 5

Code	Name	Length	Notes
26	Interface MTU	2 octets	
27	All subnets are local	1 octet	
28	Broadcast address	4 octets	
29	Perform mask discovery	1 octet	
30	Mask supplier	1 octet	
31	Perform router discovery	1 octet	
32	Router solicitation address	4 octets	
33	Static route	Multiples of 8 octets	A list of destination/router pairs

Link layer parameters per interface[13]:Section 6

Code	Name	Length	Notes
34	Trailer encapsulation option	1 octet	
35	ARP cache timeout	4 octets	
36	Ethernet encapsulation	1 octet	

TCP parameters[13]:Section 7

Code	Name	Length	Notes
37	TCP default TTL	1 octet	
38	TCP keepalive interval	4 octets	
39	TCP keepalive garbage	1 octet	

Application and service parameters[13]:Section 8

Code	Name	Length	Notes
40	Network information service domain	Minimum of 1 octet	
41	Network information servers	Multiples of 4 octets	
42	Network Time Protocol (NTP) servers	Multiples of 4 octets	
43	Vendor-specific information	Minimum of 1 octets	
44	NetBIOS over TCP/IP name server	Multiples of 4 octets	
45	NetBIOS over TCP/IP datagram Distribution Server	Multiples of 4 octets	
46	NetBIOS over TCP/IP node type	1 octet	
47	NetBIOS over TCP/IP scope	Minimum of 1 octet	
48	X Window System font server	Multiples of 4 octets	
49	X Window System display manager	Multiples of 4 octets	
64	Network Information Service+ domain	Minimum of 1 octet	
65	Network Information Service+ servers	Multiples of 4 octets	
68	Mobile IP home agent	Multiples of 4 octets	
69	Simple Mail Transfer Protocol (SMTP) server	Multiples of 4 octets	
70	Post Office Protocol (POP3) server	Multiples of 4 octets	
71	Network News Transfer Protocol (NNTP) server	Multiples of 4 octets	
72	Default World Wide Web (WWW) server	Multiples of 4 octets	
73	Default Finger protocol server	Multiples of 4 octets	
74	Default Internet Relay Chat (IRC) server	Multiples of 4 octets	
75	StreetTalk server	Multiples of 4 octets	
76	StreetTalk Directory Assistance (STDA) server	Multiples of 4 octets	

DHCP extensions[13]:Section 9

Code	Name	Length	Notes
50	Requested IP address	4 octets	
51	IP address lease time	4 octets	
52	Option overload	1 octet	
53	DHCP message type	1 octet	
54	Server identifier	4 octets	
55	Parameter request list	Minimum of 1 octet	
56	Message	Minimum of 1 octet	
57	Maximum DHCP message size	2 octets	
58	Renewal (T1) time value	4 octets	
59	Rebinding (T2) time value	4 octets	
60	Vendor class identifier	Minimum of 1 octet	

Benefits

- Accurate IP configuration
- Reduced IP address conflicts
- Automation of IP address administration
- Efficient change management

Attacks

- Introduction
- **Attacks**
- Mitigations

- Server Spoofing (MITM)
- Denial-of-Service
- Misc.

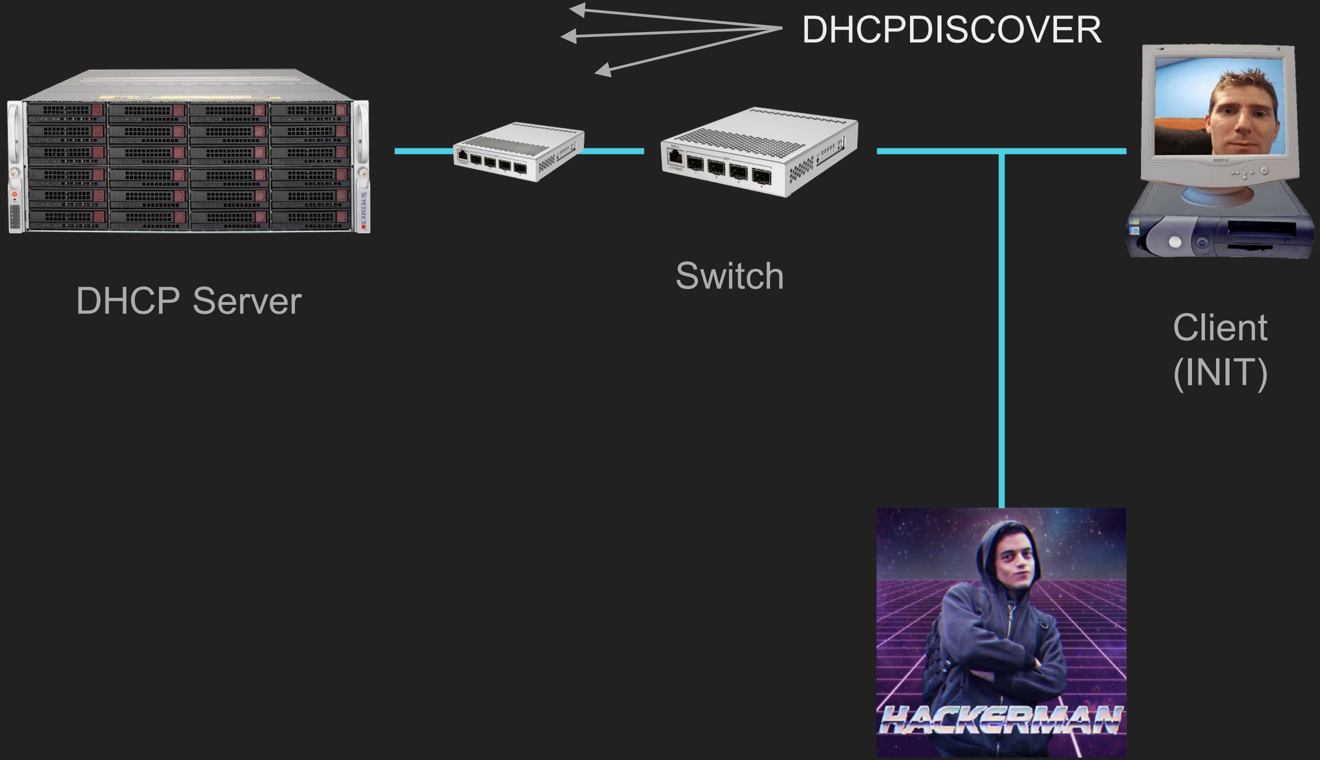
Server Spoofing

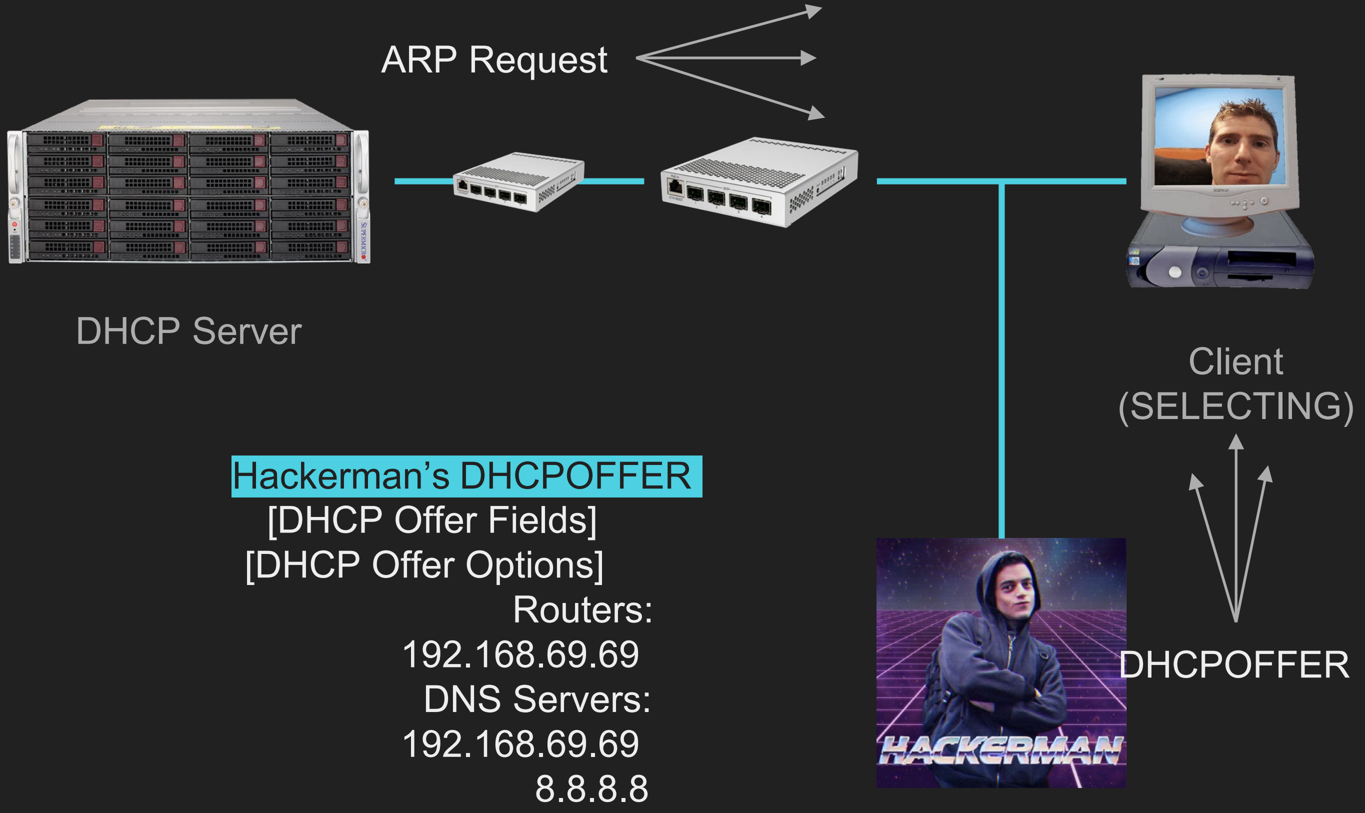
- Like IP, DHCP was not designed with security as a principle consideration
- There is no authentication built-in to the protocol
- An attacker can masquerade as a DHCP server
- This means attackers can misconfigure clients with attacker-controlled DNS servers or default gateways facilitating MITM

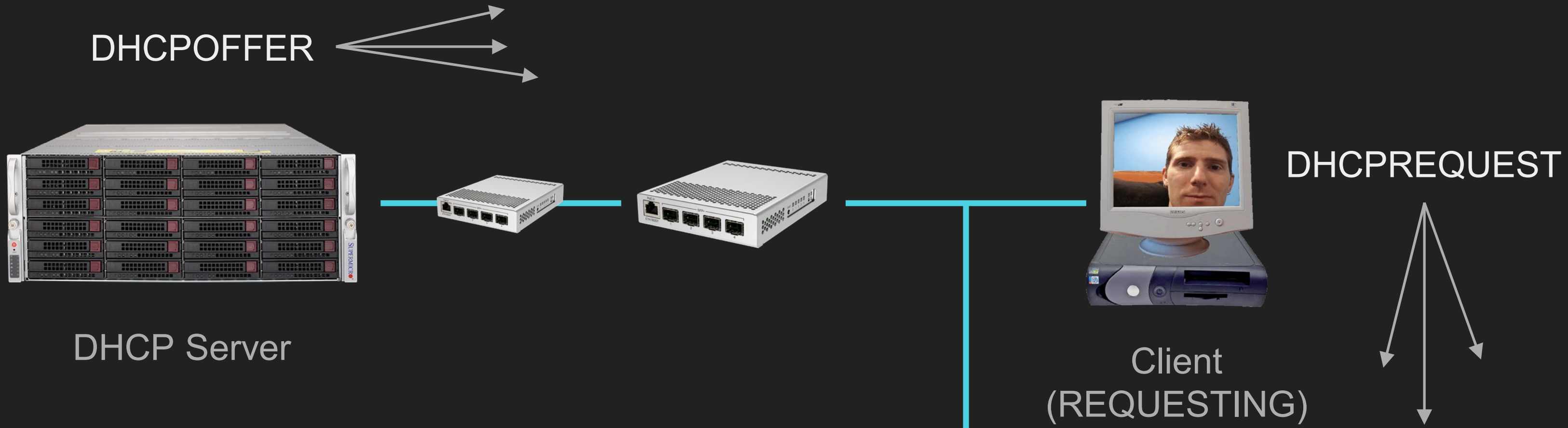
“the attacker’s rogue DHCP server races against the legitimate DHCP server: his answers must come first to the client otherwise they will most likely be ignored.”

-WhiteWinterWolf, security blogger

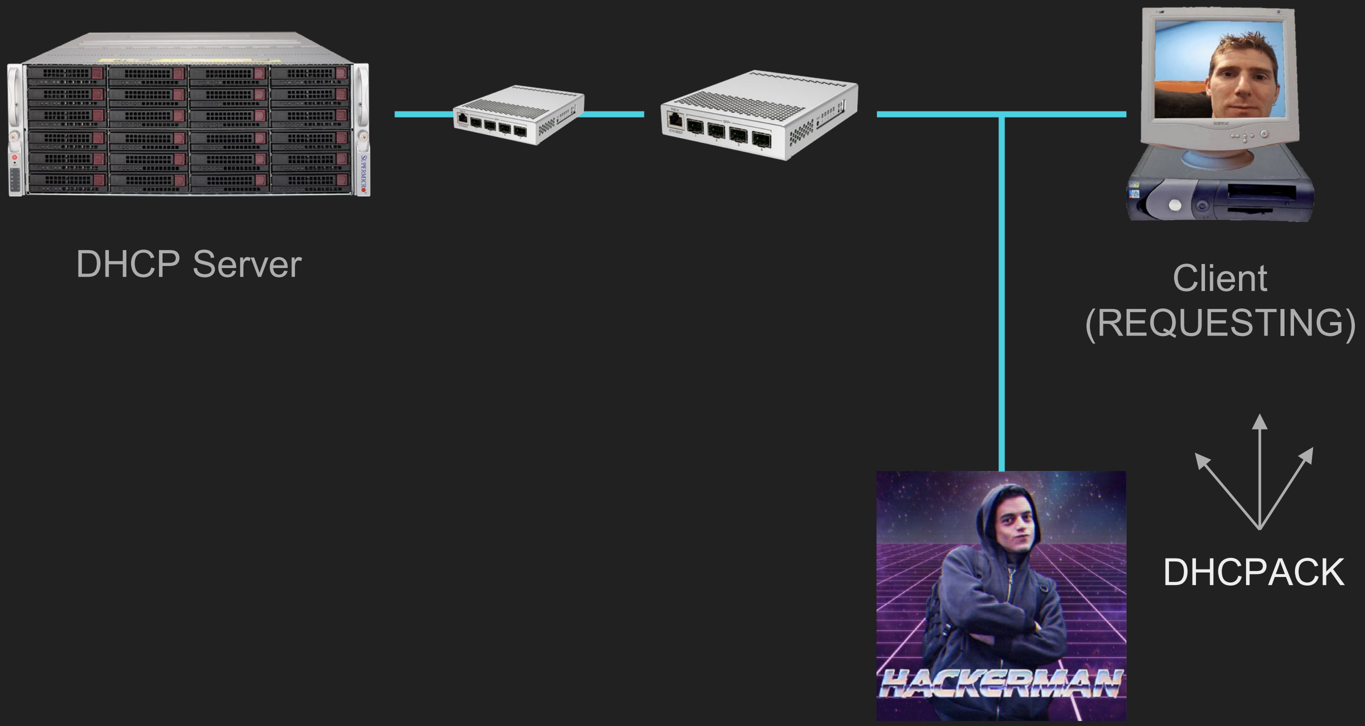
Spoofing

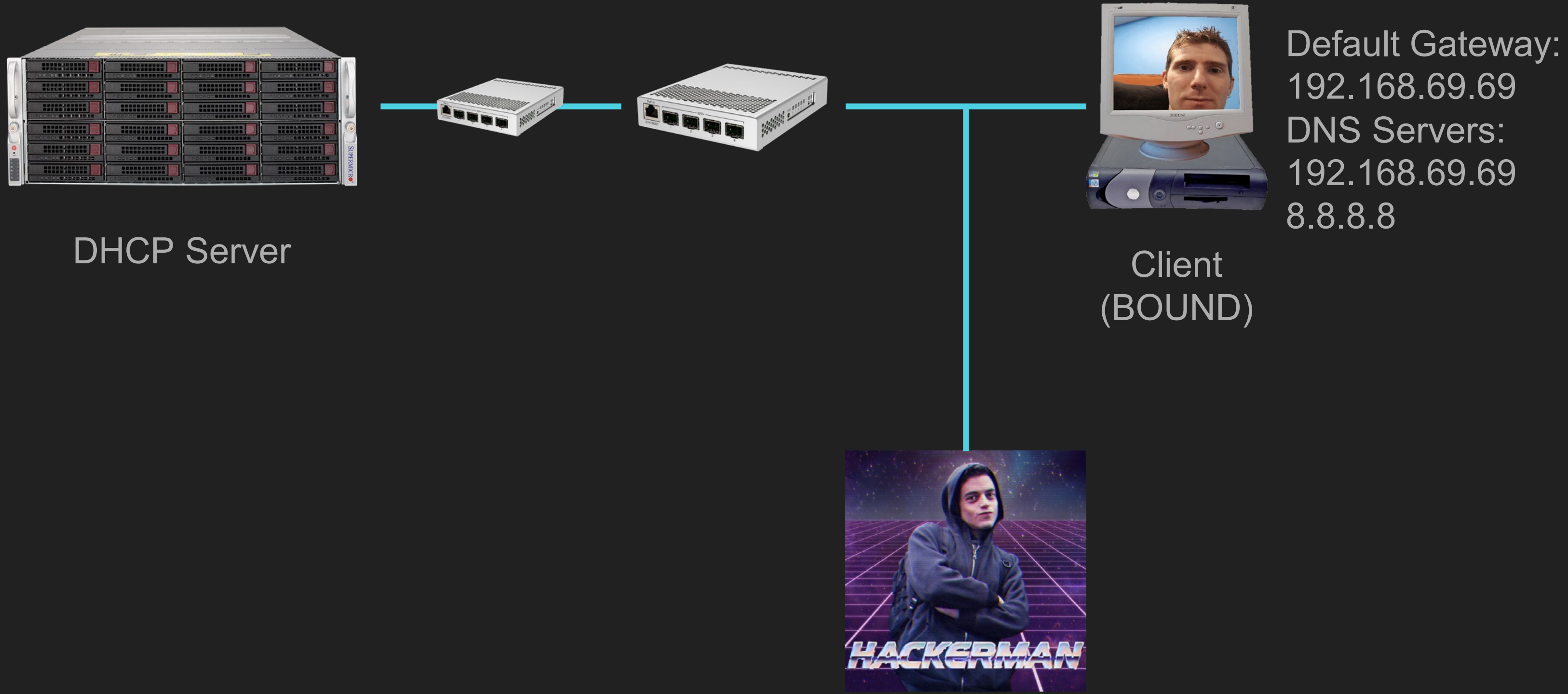



ARP Request
DHCP Server
Client
(SELECTING)
Hackerman's DHCPOFFER
[DHCP Offer Fields]
[DHCP Offer Options]
Routers:
192.168.69.69
DNS Servers:
192.168.69.69
8.8.8.8
HACKERMAN
DHCPOFFER



DHCP Server’s DHCPOFFER
[DHCP Offer Fields]
[DHCP Offer Options]
Routers:
192.168.69.2
DNS Servers:
8.8.8.8
8.8.8.4


DHCP Server
Client
(REQUESTING)
DHCPACK
HACKERMAN


DHCP Server
Client
(BOUND)
Default Gateway:
192.168.69.69
DNS Servers:
192.168.69.69
8.8.8.8
HACKERMAN

Server Spoofing

- Either DHCPOFFER or DHCPACK can be spoofed
- Spoofing DHCPOFFER requires the attacker to maintain legitimate leases on addresses or to choose addresses not in-use to avoid conflicts which may cause network problems
- Spoofing DHCPACK requires the attacker to impersonate the legitimate DHCP server, which in some scenarios (e.g. NIC not promiscuous), may cause the parameters to reset to their legitimate values upon renewal (renewals are unicast rather than broadcast)

Denial-of-Service (DHCP Flooding)

- This is an ordinary flood attack
- The attacker floods the network with DHCPDISCOVER messages
- This depletes resources from the DHCP server as it must check its address pool
- It may also amplify network traffic since it may send ARP requests to check if addresses in its pool are in-use

Denial-of-Service (DHCP Starvation)

- Lease so many IP addresses from the DHCP server's address pool that legitimate clients are starved of (cannot lease) IP addresses
- Requires both a DHCPDISCOVER and DHCPREQUEST from the attacker
- Attacker's messages are sent from randomized MAC addresses
- Does not work on wireless networks

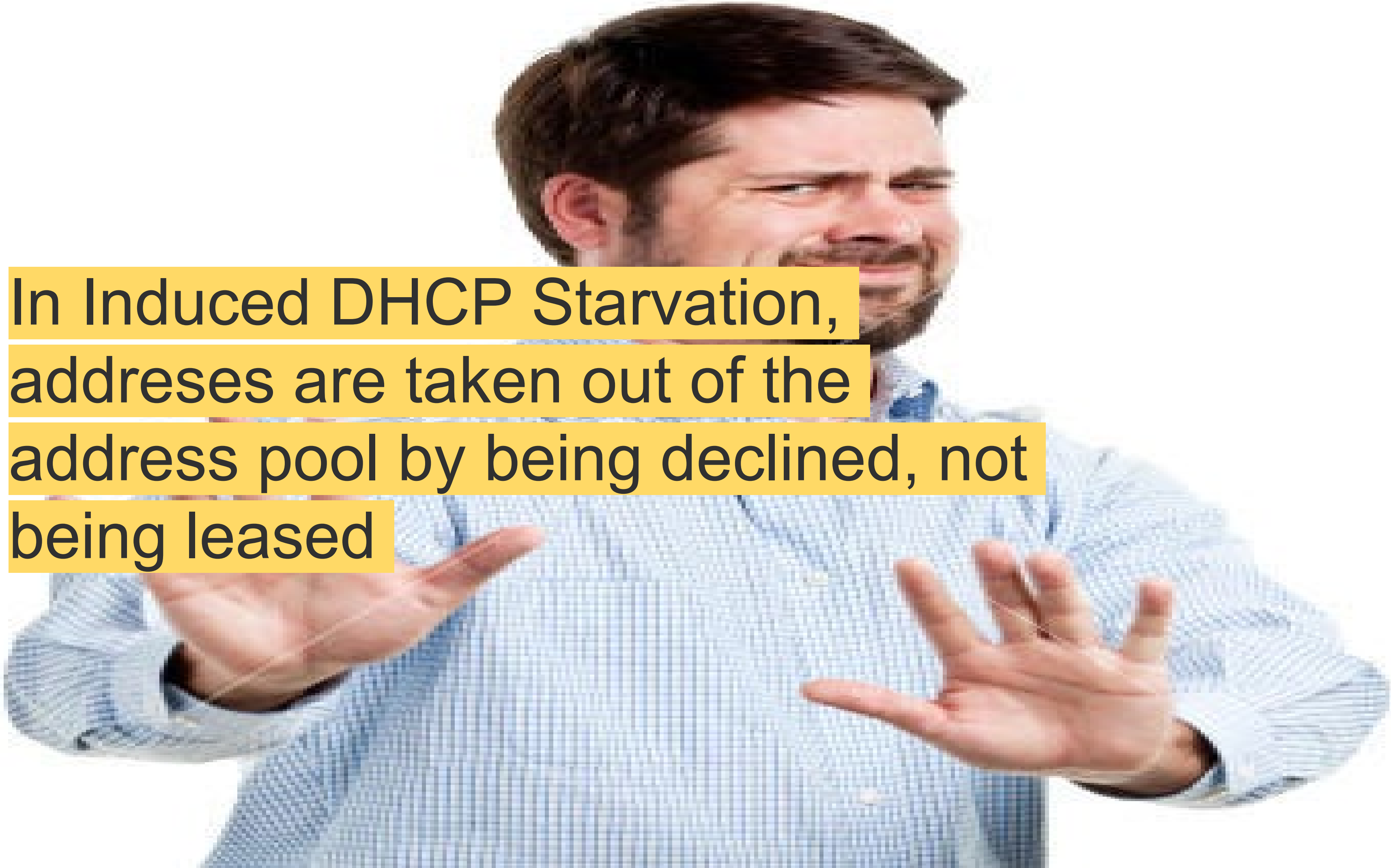
Wireless APs require an association with a client for traffic to be exchanged. This limits the number of spoofed MAC addresses to the number the AP can support.

Denial-of-Service (DHCP Starvation)

- Lease so many IP addresses from the DHCP server’s address pool that legitimate clients are starved of (cannot lease) IP addresses
- Requires both a DHCPDISCOVER and DHCPREQUEST from the attacker
- Attacker’s messages are sent from randomized MAC addresses
- Does not work on wireless networks
  - MAC addresses limited to the number of MAC addresses a wireless AP can support
  - Association phase is expensive
  - Spoofing the MAC address only on the application layer causes unicast DHCPOFFER replies to be destined for a non-existent MAC, and dropped

Denial-of-Service (Induced DHCP Starvation)

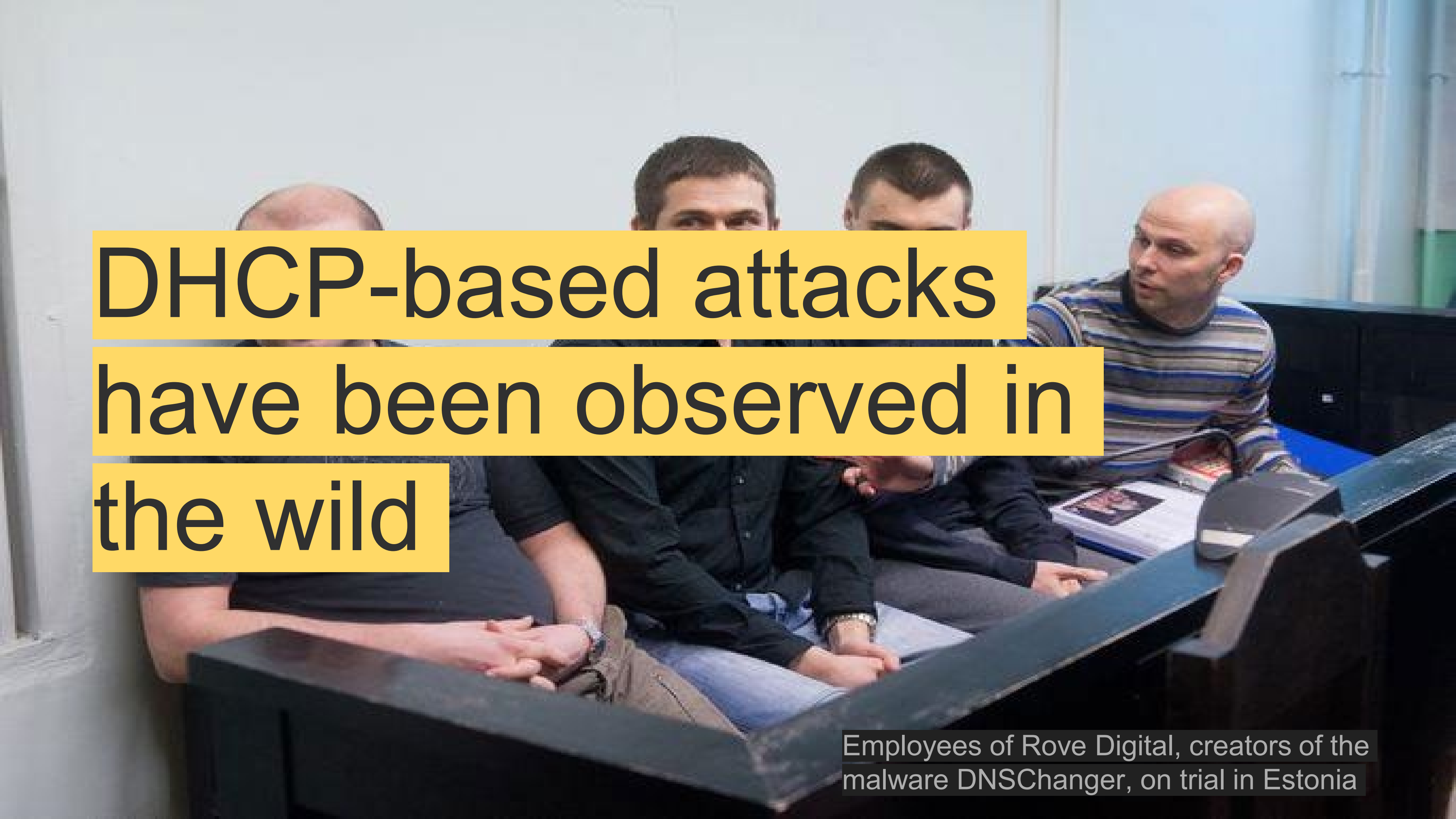
- Clients are required to check if an IP address is in-use via ARP requests after DHCPACK sent by server
- Attacker should listen for DHCP exchanges and reply to the relevant ARP requests
- This will cause the client to send a DHCPDECLINE
- Upon receipt of DHCPDECLINE, servers are required to remove the address from the address pool for its lease time
- More efficient than traditional starvation since only 1 message per offer is needed


In Induced DHCP Starvation, addreses are taken out of the address pool by being declined, not being leased

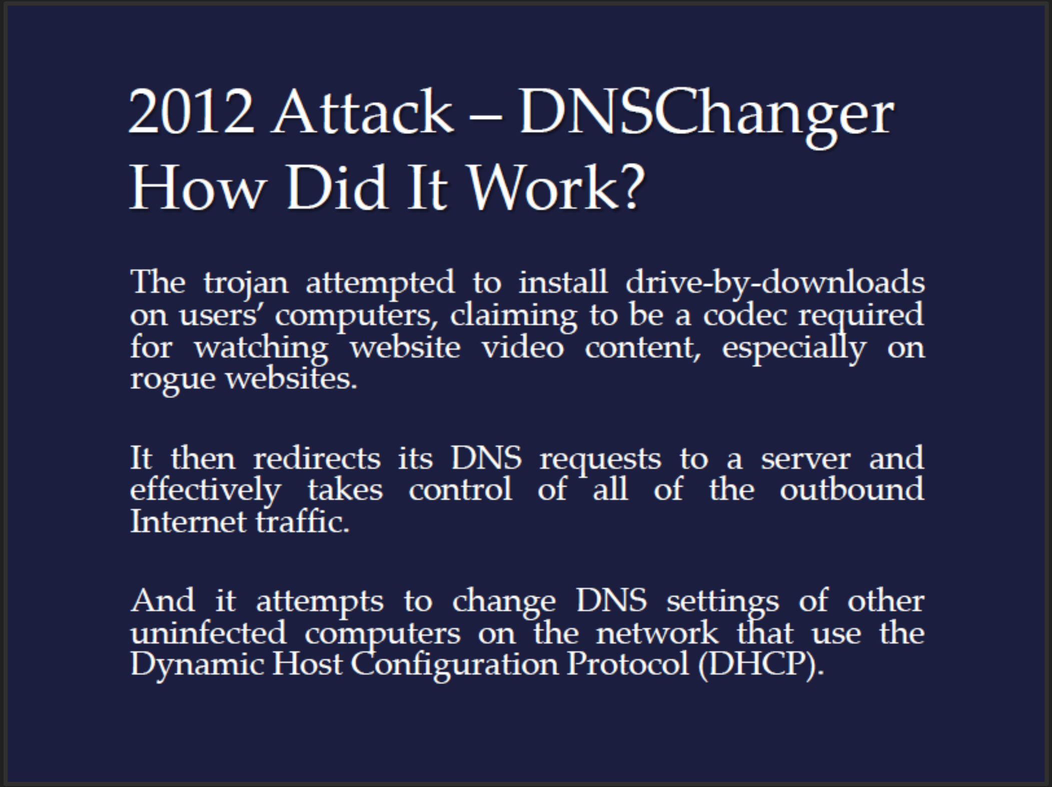
Miscellaneous Attacks

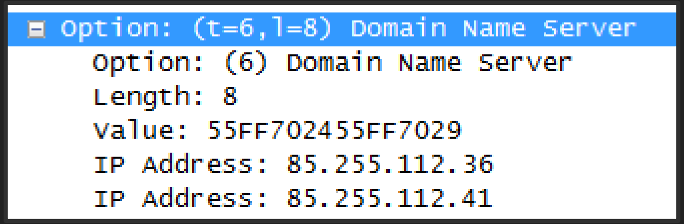
- Some believe that brittle implementations of DHCP may break if sent malformed packets (Singh et. al.)
- Implementation-specific vulnerabilities
  - CVE-2004-0460 Internet Software Consortium DHCP Daemon Buffer Overflow Vulnerability (widely-used on Linux)
  - CVE-2019-0626 Windows DHCP Server Remote Code Execution Vulnerability
- Theft of Service
  - DHCP has no built-in authentication
    - Current solutions are outside DHCP (e.g. DOCSIS BPI, captive portal)
    - “Protect the network”

DHCP-based attacks have been observed in the wild



Employees of Rove Digital, creators of the malware DNSChanger, on trial in Estonia





Top-left, right: Slides from EECS3482 presentation on DNS-based attacks in Fall 2014
Bottom-left: Details of a DHCP option field in Wireshark from a SANS write-up on DNSChanger malware. 85.255.112.0/20 has since been re-allocated.

Mitigations

- Introduction
- Attacks
- **Mitigations**

- A word on the security of the protocol itself
- DHCP Snooping
- DHCP Authentication
- DHCP Relay Agent Information Option
- Protect the network instead of the protocol

DHCP Security

- Old protocol, not defined with security in mind

RFC 2131 - Dynamic Host Configuration Protocol:

7. Security Considerations: "[...]Therefore, DHCP in its current form is **quite insecure**"

- Does not provide Authentication nor Data Integrity
  - Therefore, anyone on the network can pretend to be a DHCP server and provide malicious configuration, or pretend to be a DHCP client, and hold ressources intended for the client
- There are mitigations

DHCP Snooping (1/2)

Security measure implemented on a switch between the DHCP server and the clients

The switch acts like a “firewall” in regard to DHCP traffic

On the switch, interfaces connected to clients (or their network) are “untrusted” while the interface connected to the DHCP server (or its network) is “trusted”.

The switch drops DHCP traffic expected from the DHCP server when it arrives to an untrusted interface (prevent rogue DHCP server attack), and only forwards client DHCP traffic through the trusted interface.

DHCP Snooping (2/2)

Other features:

- Rate limiting for on every interface, to prevent DHCP starvation.
- Building and maintaining a database of hosts & leases information, to help determining if some DHCP traffic is bogus or legitimate.

DHCP Authentication

- (Also Known As RFC 3118 - Authentication for DHCP Messages)
- Allows clients and the DHCP server to send authentication information when exchanging messages using the DHCP protocol
- RFC does not give information on how to share the authentication keys
- Not widely adopted at all: DHCP is supposed to remove the need of manual configuration, but this RCF requires a shared secret.

DHCP Relay Agent Information Option

- (Also Known As RFC 3046 - DHCP Relay Agent Information Option)
- Implemented as an option of the DHCP protocol
- Middle-man (called “Agent” between hosts and DHCP server
- Agent forwards DHCP traffic and specify an agent-specific ID in the message
- The server keeps track of IDs to determine if traffic is bogus or not
- Trust placed on the agent rather than the client

Protect the network, not the DHCP server!

DHCP attacks always require the attacker to be on the DHCP server’s network (or subnet).

The easiest way to prevent such attacks is to prevent an attacker to be on the network in the first place!

Introducing IEEE 802.1X: “““EAP over LAN”””

(Extensible Authentication Protocol over Local Area Network)

Client can’t access network (and do not have an IP address) until authenticated.

Key Takeaways

Key Takeaways

- What are the stages of DHCP operation?
  - Discovery, Offer, Request, Acknowledgement
- Which stages of DHCP operation can be exploited for malicious purposes?
  - DHCP Flooding: Discovery
  - DHCP Spoofing: Offer, Acknowledgement
  - DHCP Starvation: Discovery, Request; Acknowledgement
- Why is DHCP so insecure?
  - It was not defined with security in-mind

References

References

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html

https://tools.ietf.org/html/rfc3046

https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

https://tools.ietf.org/html/rfc2131#page-43

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html

https://en.wikipedia.org/wiki/IEEE_802.1X

https://tools.ietf.org/html/rfc3580

https://www.networkworld.com/article/3299438/dhcp-defined-and-how-it-works.html

https://tools.ietf.org/html/rfc2131

N. Hubballi, et. al. "A closer look into DHCP starvation attack in wireless networks," Computers & Security, vol. 65, March, 2017

D. Bickram, et. al. "DNS Changer Attacks," from EECS3482 Intro. to Computer Security. YorkU, 2014.

References

B. Zdrnja, "Rogue DHCP servers," InfoSec Handlers Diary Blog, Dec, 04, 2008. [Online]. Available: http://isc.sans.org/diary.html?storyid=5434

WhiteWinterWolf, "DHCP exploitation guide", WhiteWinterWolf, Oct, 30, 2017. [Online]. Available: https://www.whitewinterwolf.com/posts/2017/10/30/dhcp-exploitation-guide/#fnref-ideal-world

T. Rooney, IP Address Management: Principles and Practice, Piscataway, New Jersey: Wiley-IEEE Press, 2011