Strathmore University
Faculty of Information Technology

Detecting Rogue DHCP and Man-in-the-Middle Controllers in Local Area Networks

Vitalis Gavole. O

Presented by
Vitalis G. O.

Introduction

Local Area Networks (LAN and WLAN):

- Provide fixed/portable point of attachment for end users to the network
  - Fixed Ethernet and WiFi

Dynamic Host Configuration Protocol (DHCP):

- Provides IP parameters to computers joining a network

Domain Naming System (DNS):

- Provides translation of computer names to IP addresses

Address Resolution Protocol (ARP):

- Provides mapping between IP addresses and MAC addresses

Introduction

Local Area Network Security Vulnerabilities

- IP hijacking (DoS)
  - Attacker assigns victim's IP address to alias interface in order to disrupt victim's communications (MS windows warns of duplicate IP detected and disables communications; Ethernet switch table Flaps btw attacker's and victims ports)
- ARP flooding (DoS)
  - Attacker sends many ARP requests to overwhelm victims with processing ARP messages – Slows victim's computer
- DHCP scope exhaustion (DoS)
  - Attacker creates many virtual network interfaces and requests an IP address for each hence depleting all IP addresses that DHCP server can issue to genuine computers – Genuine computers are locked out of network due to lack of IP addresses

Introduction

Local Area Network Security Vulnerabilities (Contd…)

- Smuff attack (DoS)
  - Attacker send ICMP echo (PING) requests to many proxy-attackers (also victims) using a false source IP address i.e. main victim's IP address requesting them to respond with a large payload
  - Victim is flooded with a lot of data in many PING responses
- Rogue Access Point (Man in Middle)
  - Attacker installs WiFi AP with SSID and WPA key of genuine institution's WiFi network
  - Victim's devices connect to attacker AP – Happens automatically due to WiFi handover
  - Attacker can intercept victim's communications

Introduction

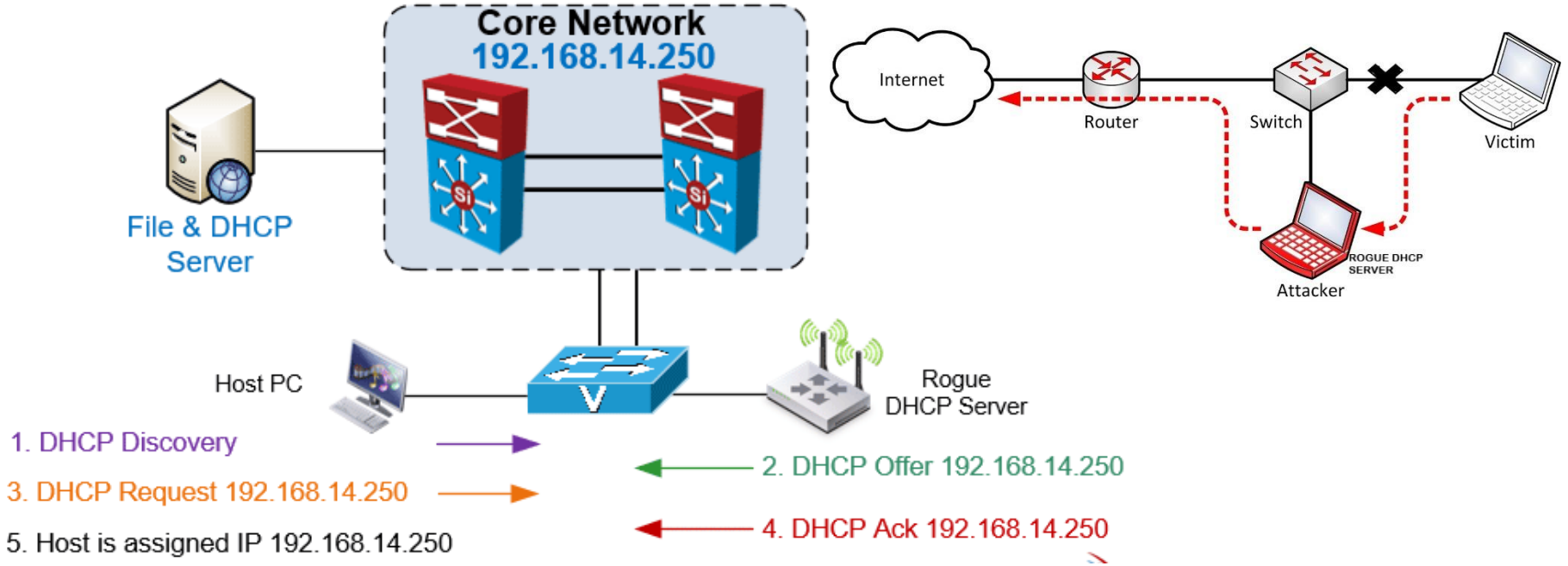
Local Area Network Security Vulnerabilities (Contd…)

- Rogue DHCP server
  - Addressed in this presentation
- ARP-Based Man-in-The-Middle (MiTM) controllers
  - Addressed in this presentation

Introduction

Rogue DHCP servers:

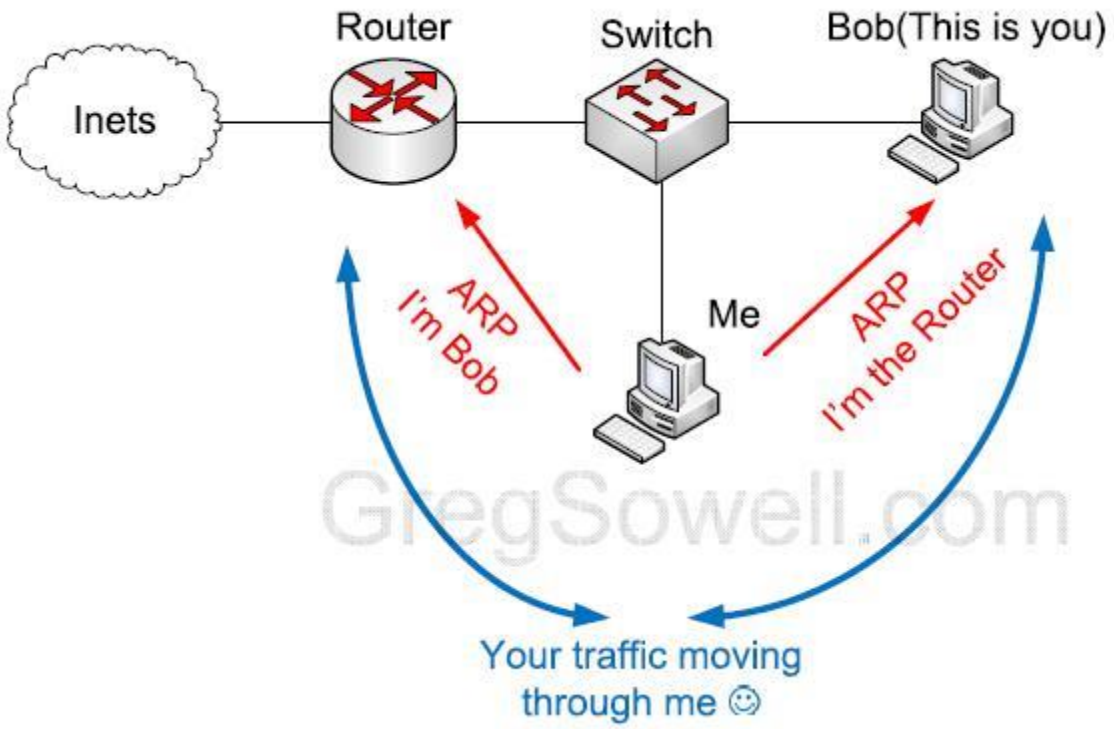
- DHCP server set up on a network by an attacker
- Issues rogue Router and DNS server addresses to joining computers



Introduction

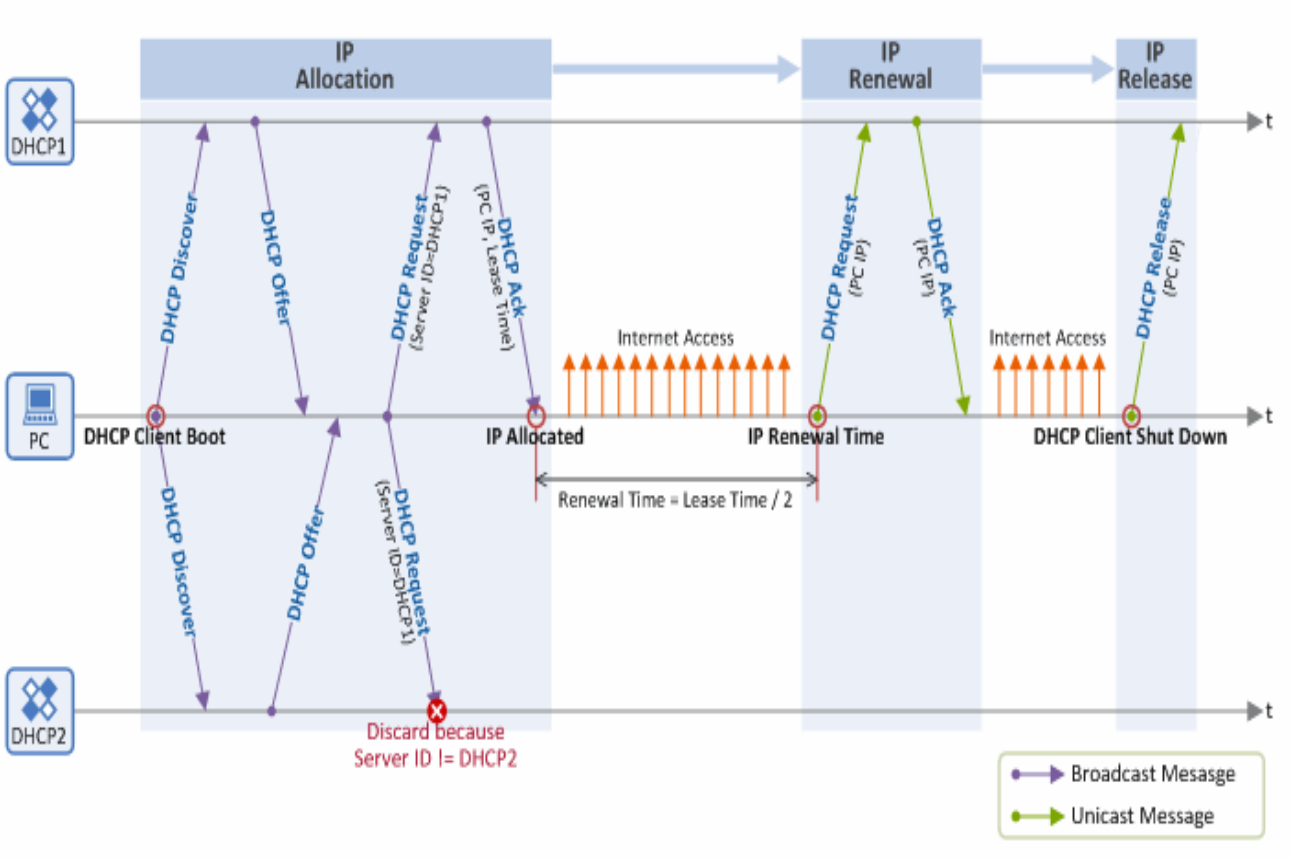
MiTM Controllers:

- User GARP to redirect victim and default router to MiTM server
- Can deploy Rogue DNS, or rogue default router
- Sniff unencrypted traffic



Introduction

DHCP



DHCP parameters:

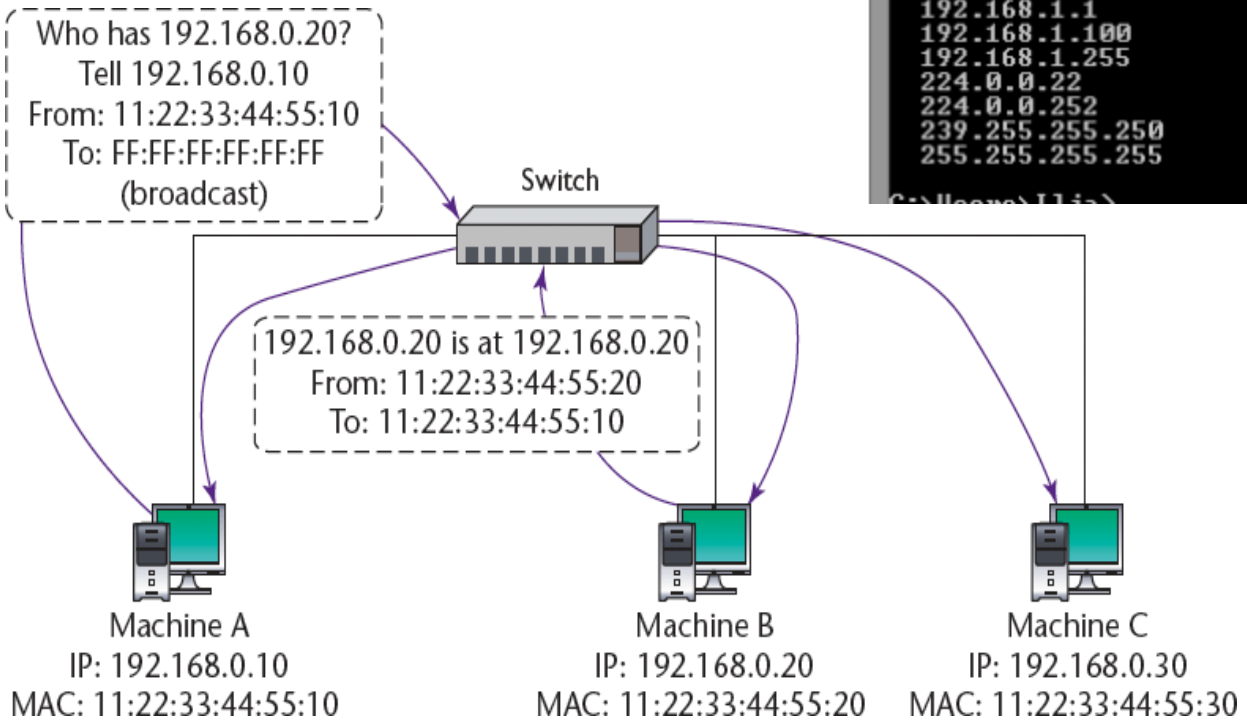
- IP address
- Subnet Mask
- Router (Default Gateway)
- Lease duration
- DHCP server
- DNS Servers

Introduction

Solicited ARP

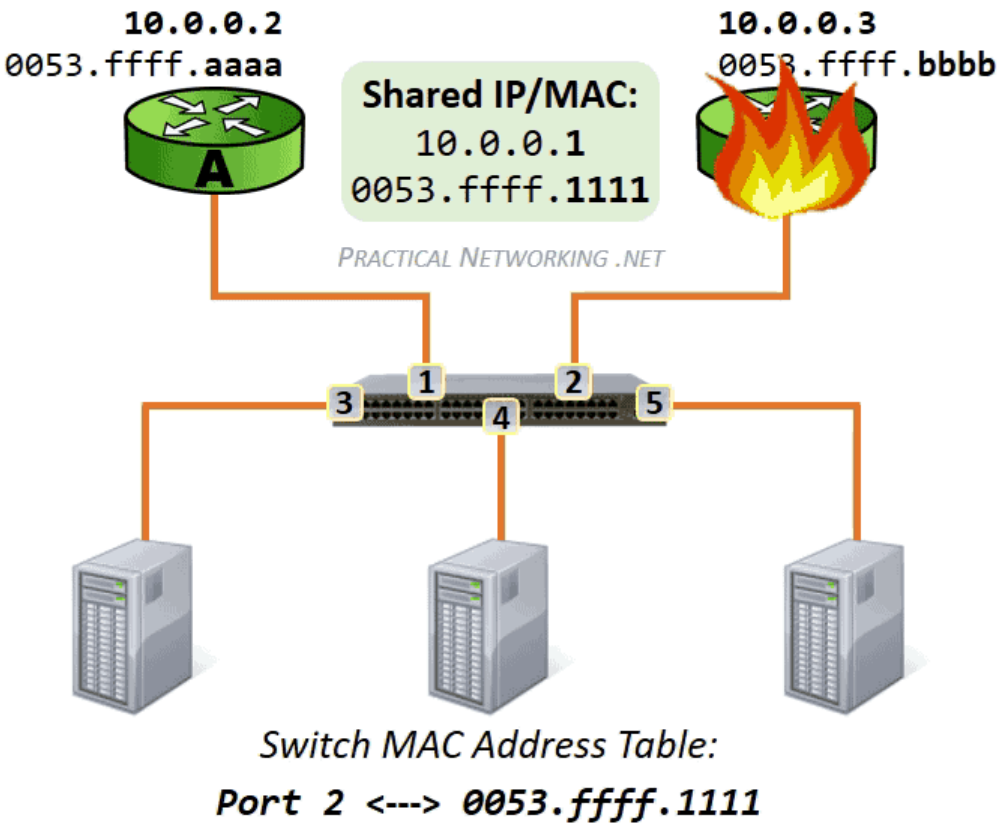
```
C:\Users\Ilja>arp -a

Interface: 192.168.1.101 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           00-23-69-ec-79-4d     dynamic
  192.168.1.100         74-d0-2b-a1-b3-11     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```



Introduction

Gratuitous ARP



- They can help detect IP conflicts
- Updating of other machines' ARP tables in Clustering
- Update switch tables
- Notify MAC address of new member of subnet

Related Works

- Authenticated DHCP – RFC 3118
- AP restriction of direction of DHCP responses
- Firewall restriction for outbound DNS requests from clients on subnet
- DNSSec

Proposed Approach

- IDS counts number of DHCP OFFERS for each DISCOVER
  - Flags extra messages
- IDS identifies suspicions DHCP options in ACK messages
  - Track rogue DHCP server on fixed LAN
  - Needs method to locate rogue server in WLAN
- Disable GARP on default router
- IDS detect GARP advertising router IP address
  - Track MiM controllers on fixed LAN
  - Needs method to locate MiM in WLAN

Experimental Details

- Will setup rogue DHCP server and GARP MiTM controllers on Strathmore University WiFi
  - Determine number of victim devices over different hours of day
  - Assess different exploits against victims
- Deploy IDS against Rogue DHCP server and GARP MiTM controllers
  - Evaluate effectiveness in detecting introduction of multiple rogue DHCP servers and MiTM controllers

Results and Analysis

- This is work in progress

Conclusions

- WLAN is popular in campuses: Colleges, Restaurants, airports
- All users are potential victims
- Detection and tracking of rogue DHCP servers and MiM controllers will improve security of these networks

Q and A?

?