July 30, 2018

PROTECTING PRINTERS FROM ROGUE DHCP SERVERS

HP INC

Protecting Printers from rogue DHCP servers

Abstract

In today’s world, securing devices from Malwares is a big concern. Even though IDS (Intrusion detection systems) are in place, it is hard to eliminate malwares completely in a network. A vulnerable device in a network can be attacked by a malware which can act as rogue DHCP server. It can move connected print device(s) out of network.

This paper proposes a solution to handle rogue DHCP server and protect printers from simulated DHCP servers by malwares or misbehaving DHCP servers. Our idea is to implement a mechanism in printers which will provide an ability to protect themselves from rogue server(s) present in network.

Problem Statement

Printer(s) acquire IP provided by DHCP server, when connected to network (Call flow of DHCP is explained in Appendix). Printer(s) don’t have the ability to verify the authenticity of the DHCP server(s).Rouge server may provide IP configuration (IP address, subnet-mask, default gateway etc) which will not be in-line with network devices’ configuration. If so, printer(s) acquire IP configuration in such a way that printer can’t be accessible for other devices in the network.

Prior Solutions

There are solutions available which needs alteration of DHCP protocol for embedding security credentials for the sake of authenticating DHCP server.

Solution

The proposed solution is based on validation of DHCP servers through certificates over SSL. The authentication will be carried out after the printer receives the DHCP-ACK packet (DHCP call flow is explained in Appendix-1). Once the printer receives the DHCP-ACK packet from the server, print device will not configure IP address on network interface, rather printer will validate the server’s authenticity (Call flow for authentication is given in Appendix -2). Once the authentication process is successful, the printer will configure IP address on network interface. If the server fails to authenticate, DHCP server will be treated as a rogue server and the printer will restart IP procurement process. Rogue server will be blacklisted in procurement process.

The broad sequence of operations would be as below:

1. Connect printer to network.
2. Printer sends DHCP- DISCOVER packet and receives one or more offers from DHCP server(s) via DHCP-OFFER packets. Printer selects one among multiple offers and sends DHCP-REQUEST to the corresponding server.
3. Once DHCP sever responds with DHCP-ACK, Printer needs to know whether the server is rouge or not, based on the authentication result.
4. The below flow of operations is used to validate authenticity of server

a) Printers receives DHCP-ACK packet from the DHCP server.
b) Instead of configuring IP address on the network interface, printer initiates certificate exchange using SSL with DHCP server.
c) For SSL certificate exchange, the same DHCP port can be used over TCP.
d) If SSL authentication is successful, print device will configure the IP address on the network interface.
e) If SSL authentication fails, Printer considers server as rouge and adds to blacklist for further IP procurement negotiation. The print device will restart IP configuration procurement process.

5. The operation flowchart of this solution is enunciated in Figure: 1 below.

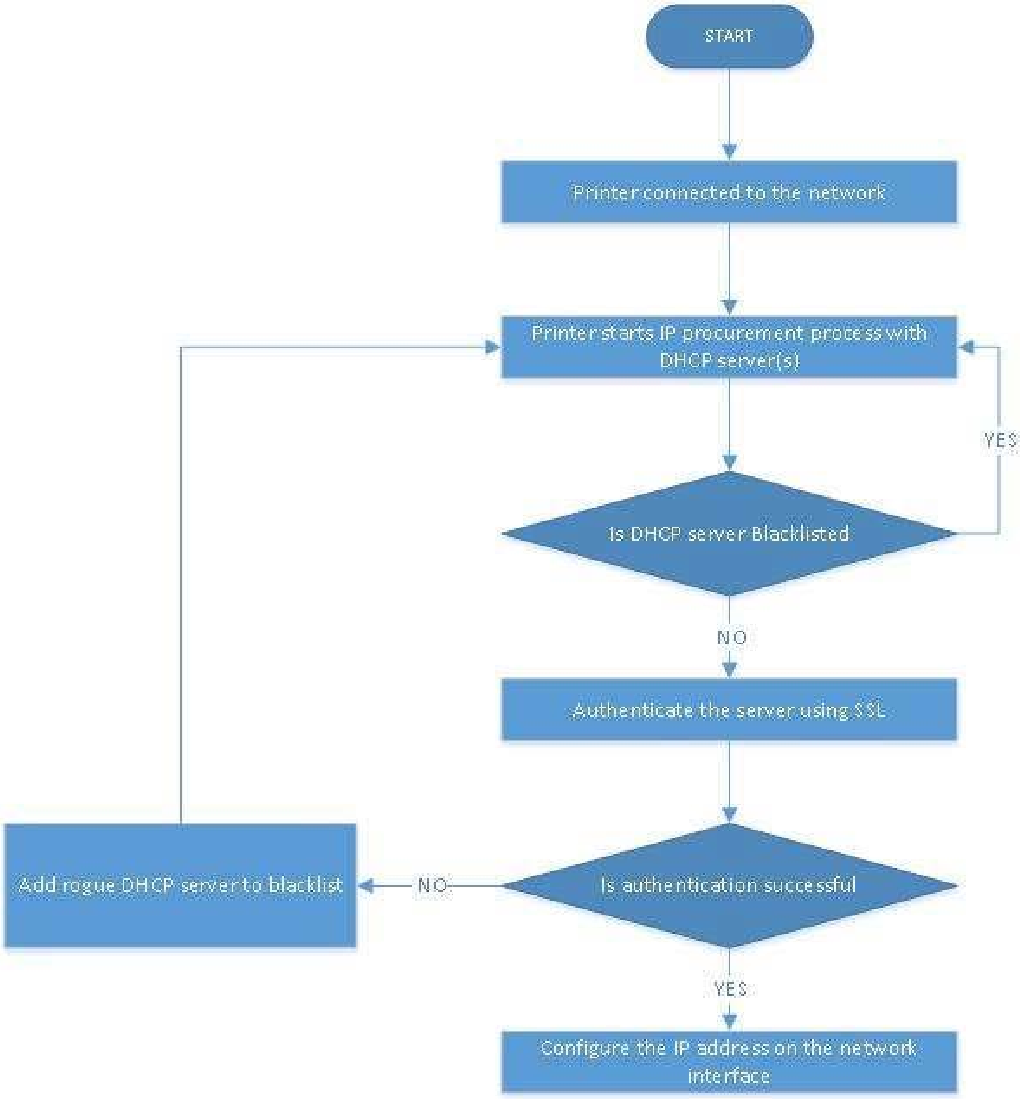

START
Printer connected to the network
Printer starts IP procurement process with DHCP server(s)
YES
Is DHCP server Blacklisted
NO
Authenticate the server using SSL
Add rogue DHCP server to blacklist
NO
Is authentication successful
YES
Configure the IP address on the network interface

Figure 1: Operational Flowchart

Advantages

This solution doesn't require any change in DHCP protocol.

Appendix-1

DHCP IP procurement call flow

1. DHCP-DISCOVER packet provides information about host with hostname, MAC address etc. and requests for IP, subnet mask, gateway etc. which are related to network configuration.
2. DHCP-OFFER Packet contains info regarding Options like FQDN, lease time, gateway, etc.
3. DHCP-REQUEST packet is same as DHCP-DISCOVER except it may contain offered IP address and printer needed info.
4. DHCP-ACK contains IP Address, lease time, gateway, DHCP server IP, FQDN, etc.

Figure 2 covers the DHCP call flow.

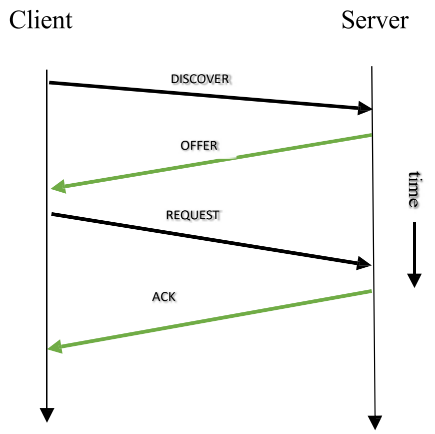


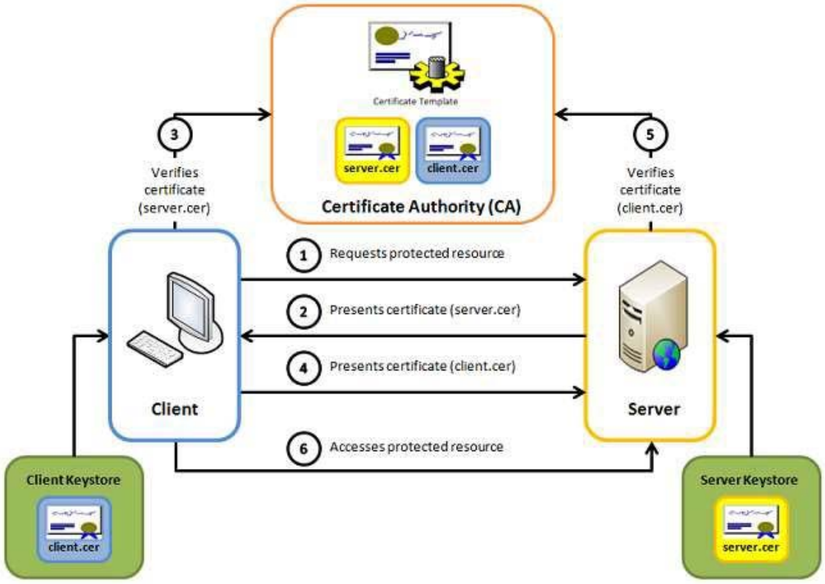
Figure 2 : DHCP call flow

Appendix-2

Mutual SSL authentication or certificate based mutual authentication refers to two parties authenticating each other through verifying the provided digital certificate so that both parties are assured of the others' identity. In technology terms, it refers to a client authenticating themselves to a server (website or server application) and that server also authenticating itself to the client through verifying the public key certificate/digital certificate issued by the trusted Certificate Authorities (CAs). From a high-level point of view, the process of authenticating and establishing an encrypted channel using certificate-based mutual authentication involves the following steps:

1. A client requests access to a protected resource.
2. The server presents its certificate to the client.
3. The client verifies the server's certificate.

4. If successful, the client sends its certificate to the server.
5. The server verifies the client's credentials.
6. If successful, the server grants access to the protected resource requested by the client.


Certificate Template
server.cer
client.cer
Certificate Authority (CA)
3
Verifies certificate (server.cer)
5
Verifies certificate (client.cer)
1 Requests protected resource
2 Presents certificate (server.cer)
4 Presents certificate (client.cer)
6 Accesses protected resource
Client
Server
Client Keystore
client.cer
Server Keystore
server.cer

Mutual SSL authentication / Certificate based mutual authentication

Disclosed by Yalamarthi Balaji, Sheelam Prathap Reddy, Rahul Sharma and Jasjiv Singh, HP Inc.