Global Information Assurance Certification Paper

Security problems with DNS (CNR)
George Sagos
November 27, 2000

This report will take a closer look at security issues with the DHCP protocol in general, but with the Cisco Network Registry (CNR) in mind as part of a secure DHCP solution.

BootP/DHCP History brief

BootP

BootP uses a server to allocate IP addresses, a fairly simple request/reply mechanism; it broadcasts requests to LAN segments, crosses routers with IP helper (bootp relay).

BootP server hands out IP addresses, and with diskless workstations, points to file servers with more setup info. This all results in no setup for users and more control for administrators.

One "problem" with bootp is that it requires maintaining of a list of matching Mac and IP addresses.

DHCP

Dynamic Host Configuration Protocol (DHCP) extends BootP capabilities significantly; easier administration, automated configuration…

You can Manually link the Mac address to the IP address like BootP, to make it *static*, or you can get a IP address *dynamically* leased from a pool of addresses from the DHCP server. In that case the IP address has an expiration date, and the host can return to the DHCP pool when expired.

Finally you can *automate* a static IP address by letting the host boot up and get a Dynamic IP address and then assign the IP address as a permanent (static) lease; i.e. Printers.

The pool, and lease times are configured on the server, both the server and the client keeps track of lease times. Basically it's the client that does all the work; request an addr., terminates a lease, renegotiate a lease at specific intervals.

Expired leases are re-allocated by the server.

How does DHCP work?

Here's a short overview of different DHCP packets and what a DHCP packet looks like.

1. DHCPdiscover: client broadcasts to locate available servers.
2. DHCPoffer: server respond with offer of configuration parameters
3. DHCPrequest:

   A: Client requesting offered parameters from one server and implicitly decline offers from all other servers.
   B: Client confirms previously allocated addr.
   C: Client extends a lease on an addr.

4. DHCPack: server responds with configuration parameters and IP addr.
5. DHCPnak: server rejects request from client; clients lease has expired
6. DHCPdecline: client found a problem with assigned addr.; addr. is already in use
7. DHCPinform: asking only for local configuration parameters
8. DHCPrelease: client returns assigned addr. Before lease expires or canceling remaining lease.

DHCP vulnerabilities

There are both outside and inside vulnerabilities with DHCP.

The server can be attacked in different ways; attackers can mess up your scopes, or take control over servers.

In CNR you should have at least 2 DHCP servers for redundancy, a primary and a secondary. They communicate with each other for different reasons; at start up, updates…

In CNR its on port 647 using UDP; transmitter responsible.

What if a "man in the middle" attack occurred, picking up all information from one server during an update.

On basic DHCP there is no security no authentication, any client can plug in and get DHCP information.

Some companies wants different level of access for different type of users i.e. IT people could have access and rights to some servers, and legal department to others and again financial or sales departments to others with different rights, witch can be hard to manage in dynamic environments.

How to secure DHCP

DHCP should definitely be firewalled from external hosts, as there is no reason an external host should be querying your DHCP server for IP addresses etc. In addition to this making it available to the outside world could result in an attacker starving the DHCP server of addresses assuming you use a dynamic pool(s) of addresses and learning about the structure of your internal network.

When I mention firewall, I don't mean a firewall box or firewall software straight out the box, but a firewall concept configured specifically for your network, that obeys companies' security policies.

Make sure that only plugs in the wall that is connected to hardware is "live", either by shutting down all inactive ports on the switch or physically removing the cables.

University of Massachusetts has a remedy AR (Action Request) based system where they are able to locate a port connecting an IP or Mac address:

Basically they look up the IP address in the DHCP server logs, search the switches CAM tables for MAC addresses, and then look up user records in an Oracle database using Remedy.

Boston collage is using CNR with some scripting to keep track of their DHCP service, something similar to the configuration bellow.

In this configuration is 2 DHCP servers one UNIX and one SUN both with CNR, one UNIX with LDAP database installed, and one with Oracle.

Here's what happens step by step:

1. Client boots and issues DHCP or BootP request. DHCP respons, given the client a "provisional" address. With the provisional address, no default gateway is given, and the client is told to use a "crippled" DNS server that can only resolve one server (www. Company.com)

2. Client opens a browser (with cookies enabled) and goes to www.company.com (Name resolution occurs from the crippled DNS server database.)

3. Web server on www.company.com recognizes that the client has a provisional IP address, and forwards the user to the activation page.

The activation servlet is run from the activation www page.

4. User types his username and PIN into the web page and hits enter.

This sends the username/PIN data securely (using https) to the servlet.

5. Servlet receives the username and PIN information from the client and verifies the data against an LDAP database.

6. If the username/PIN is a valid combination, servlet receives information about the user (address, status, phone number, etc.) from LDAP. If the username/PIN is an invalid combination, the servelet tells the user that the username and/or PIN was incorrect.

7. The servlet determines the operating system and IP address of the client machine. (Servlet can determine O/S from the browser being used on the client.)

8. Servlet contacts DHCP server and asks for the MAC address of the client using the provisional IP address, and DHCP server responds to the request.

9. The client-class is created on DHCP server based on the "persontype" LDAP field (determined in step 6). For example, company persontypes could include IT dept., Finacial dept., guest or other dept. (The client-class is an indicator as to which scope a DHCP lease should be granted from. The default is a the client-class for the provisional scope. Once a MAC address has been activated a "real" client-class is created.)

10. The user's ID, position, activation date, client-class, and operating system type are written to an Oracle database by the servlet.

11. The running servlet displays user information (from the Oracle database) and computer information (the MAC and IP address of the client) in the client's browser and the user is told to reboot.

12. Client reboots and issues a DHCP or BootP request DHCP server responds to the request, giving the client an address out of the appropriate DHCP scope (as decided by the client-class created in step 9), the address of the default gateway, and the addresses of the "real" DNS servers.

13. DHCP server tells primary DNS server to create a Dynamic DNS entry for the client (DNS entries are created when DHCP leases are issued).

14. A zone transfer occurs (at a configurable interval) to update secondary DNS servers.

Also some scripting have to done to Get the MAC from the IP (step 8 above) and create the client-class entry (step 9 above). The rest is taken care of by CNR.

Sources & references:

http://www.dhcp.org

http://www.isoc.org/hmp/paper/127/html/paper.html
R. Droms. DHCP protocol rfc 1531/1541/2131

http://www.lopht.com/advisories/rdp.txt

http://www.bc.edu

http://www.usenix.org/sage/sysadmins/sage-members-archive/1997/msgoo165.html

http://www.cisco.com/univercd/cc/td/doc/product/rtmgmt/ciscoasu/nr/nr50/relnot/relnot50.htm

http://www.umass.edu

http://www.remedy.com

http://www.sans.org
SANS Network Sedurity 2000, Technical Conference Day 1, Free Reign Children, Scott Conti, Umass.

http://www.rfs-editor.org