Network Working Group
INTERNET-DRAFT
Category: Informational
Expires: December 15, 2006

R. Hibbs
Richard Barr Hibbs, P.E.
C. Smith
C & C Catering
B. Volz
Cisco Systems, Inc.
M. Zohar
IBM T. J. Watson Research Center
June 13, 2006

Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Threat Analysis

<draft-ietf-dhc-v4-threat-analysis-03.txt>
Saved: Tuesday, June 13, 2006, 12:56:25

Intellectual Property Rights

Status of this Memo

Abstract

DHCPv4 (RFC 2131) is a stable, widely used protocol for configuration of host systems in a TCP/IPv4 network. It did not provide for authentication of clients and servers, nor did it provide for data confidentiality. This is reflected in the original "Security Considerations" section of RFC 2131, which identifies a few threats and leaves development of any defenses against those threats to future work. In about 1995, DHCP security began to attract attention from the Internet community, eventually resulting in the publication of RFC 3118 in 2001. Although RFC 3118 was a mandatory prerequisite for the DHCPv4 Reconfigure Extension, RFC 3203, it has had no known usage by any commercial or private implementation since its adoption. The DHC Working Group adopted a work item for 2003 to review and modify or replace RFC 3118 to afford a workable, easily deployed security mechanism for DHCPv4. This memo provides a threat analysis of the Dynamic Host Configuration Protocol for Ipv4 (DHCPv4) for use both as RFC 2131 advances from Draft Standard to Full Standard and to support our chartered work improving the acceptance and deployment of RFC 3118.

Table of Contents

1 Introduction

DHCPv4 as defined in [RFC1541] and [RFC2131] does not provide any form of communication security, confidentiality, data integrity, or peer entity authentication.

A design team was formed at IETF-55 in Atlanta in November 2002 to look at DHCPv4 and [RFC3118] to document security requirements for DHCPv4. [RFC3118] defines the current security mechanisms for

DHCPv4.

Unfortunately, RFC 3118 has neither been implemented nor deployed to date. There is widespread feeling that its current restriction to manual keying of clients limits its deployment. The DHC Working Group seeks to rectify this situation by defining security mechanisms for DHCPv4 that have better deployment properties.

1.1 Issues for Consideration

Specific issues to be considered include:

- Improved key management and scalability.
- Security for messages passed between relay agents and servers.
- The increased usage of DHCPv4 on insecure (e.g., wireless) and public LANs.
- The need for clients to be able to authenticate servers, without simultaneously requiring client authentication by the server.
- Does use of the Relay Agent Information Option imply the need for authenticated messages between DHCP servers and relay agents?

1.2 Exclusions

Excluded from our analysis are:

- Securing messages between relay agents and servers: work is already underway on this, see [RFC4030] and [relay-ipsec].
- DHCP Reconfigure Extension (FORCERENEW) [RFC3203]: the authors believe it is appropriate to put the onus to provide the analysis on those who are interested in moving that work forward. [Editor's note: despite repeated calls on the DHC Working Group mailing list to identify even a single implementation of FORCERENEW, we are unable to put forward an example of its use.]
- DHCP Failover Protocol, as defined in [failover]: the server-to-server protocol used differs significantly from DHCP, and there has been no recent work on the [failover] draft.
- DHCP-DNS Interaction, as defined in [fqdn]: securing communication between DHCP servers and DNS servers is a DNS

update security issue and therefore out of scope for the DHC working group.

- O DHCPv6, as defined in [RFC3315]: while we believe that authentication techniques developed for DHCPv4 would generally be applicable to DHCPv6, there are fundamental differences between the two protocols and RFC 3118 specifies DHCPv4-style message and options formats, so we have chosen to concentrate on DHCPv4.

- O DHCP Lease Query, as defined in [RFC4388]: because of lack of maturity.

2 Use of Key Words

The key words "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3 Applicability

3.1 Assumptions

This document assumes that the reader is familiar with both the base DHCPv4 protocol as defined in [RFC2131] and the DHCPv4 authentication extension as defined in [RFC3118], and does not attempt to provide a tutorial on either.

3.2 Scope of this Memo

This document confines its analysis to DHCPv4, as defined in [RFC2131] and [RFC2132] and DHCP Authentication, as defined in [RFC3118].

4 General threats to DHCPv4

These are the classes of threats to the base DHCPv4 protocol. Not all of these are DHCP-specific, nor can all the concerns listed be addressed by DHCP authentication.

4.1 Denial-of-Service Attacks

4.1.1 Refusal to Configure Clients

A rogue DHCP server can refuse to configure clients by responding with either partial information (i.e., missing the IP address, yet containing other information), or a non-routable (or otherwise bad) IP address, or the server may respond to DHCPDISCOVER messages (with

DHCPOFFER messages) but then ignore the subsequent client DHCPREQUEST messages. This may cause a client to repeatedly fail to be configured, though clients could take steps to ensure that they subsequently ignore such servers for some time.

4.1.2 Impersonating Clients

A rogue client can impersonate a client or many clients, by using another client's client identifier (client identifier option) and/or

hardware address (chaddr) or by generating these identifiers. This may be done to:

- Obtain addresses when hardware address or client identifier restrictions (lists) are configured into the site's server through some mechanism not described in RFC 2131. Some sites may use such a mechanism to restrict the clients that are allowed addresses. A rogue client listens to DHCPv4 traffic and captures a few chaddrs or client identifiers and starts using them.

- Simulate many clients to consume all available addresses. The rogue client may either hold on to these addresses (until the leases expire) or decline the addresses (by sending a DHCPDECLINE) in the hopes that the server will remove the declined address from use for a longer period.

- Create havoc on the subnet by injecting fake messages on behalf of other clients, prematurely releasing (DHCPRELEASE) or declining (DHCPDECLINE) their addresses. A rogue client listens to DHCPv4 traffic and gleams client identity and address information and uses this information to inject fake messages.

4.1.3 Flooding

A rogue client can flood the network with (near-) continuous DHCPv4 request messages thereby consuming processing resources and network bandwidth.

We mention this attack only for completeness, as there is little or nothing that a DHCP server can do to prevent such an attack and the client could just as well send messages of other protocols, so we will not discuss it further.

4.2 Client Misconfiguration

Rogue servers may give out bad configuration information (such as fake gateways or DNS servers), or relay agents or other network elements may alter packets between a client and server, to cause the client to be misconfigured, or potentially worse cause future man-in-the-middle attacks. This category is usually part of another attack, be it theft of service, business espionage, or business interruption including denial of service.

4.3 Theft of Network Service

By "theft of network service", we mean the taking of an unused address for network access or the use of an assigned address not belonging to the client, in contrast with "client masquerading" (Section 2.1.2) which refers specifically to the use of a legitimate client's chaddr or client identifier.

Instantiation of an unauthorized client for purposes of using network resources or services is only partially preventable using client-server authentication techniques. We mention this attack only for completeness, as there is little or nothing a DHCP server itself can do to prevent such an attack. Additional host and

application security is required to prevent theft of service, and such layer 5 and higher functions are declared out of scope for this analysis.

4.4 Packet Insertion, Deletion, or Modification

If a client (or server or relay agent) is known to crash or shut down when invalid packets of some type are sent, this could be simply another type of denial of service attack. Likewise, simply deleting certain packet types (DHCPREQUEST to renew or rebind a lease) would eventually result in client lease expiration, a denial of service attack. A rogue relay agent or other host would typically use packet insertion and deletion to interrupt service. In a different vein, the modification of packets in the DHCP exchange may be used to facilitate many different types of attacks on either client or server. For example, a DHCPACK could be modified to a DHCPNAK, thereby denying the client a lease.

5 Weaknesses of RFC 3118

An authentication mechanism for DHCPv4 protocol messages was developed in RFC 3118, proposing two basic authentication mechanisms and the means for extending the repertoire of methods as needed. The configuration token method (protocol 0) relies on exchanging clear-text authentication tokens between unconfigured DHCPv4 clients and DHCPv4 servers. It is also vulnerable to message interception. Delayed authentication (protocol 1) focuses on solving the intradomain authentication problem where the out-of-band exchange of a shared secret is feasible.

5.1 Key Exposure

The configuration token protocol, protocol 0, utilizes clear-text authentication tokens (i.e., passwords), providing only weak entity authentication and no message authentication. This protocol is vulnerable to interception and provides only the most rudimentary protection against inadvertently instantiated DHCP servers. It also leaks the key before knowing whether the server supports protocol 0.

5.2 Key Distribution

Both protocols 0 and 1 suffer from the lack of a means to easily, quickly, and reliably distribute authentication tokens used in the protocols. In many environments, some existing key distribution mechanism is presumed to be trusted and reliable, with strong administrative procedures and a security-conscious user population in place, leaving only the selection and specification of an appropriate cryptographic algorithm as a concern of the protocol designer.

Relying on such out-of-band methods to distribute and manage tens or hundreds of thousands of tokens is a significant barrier to the widespread implementation of either protocol 0 or 1.

Key distribution presents a significant system management challenge that is in marked contrast with DHCP itself, a protocol that has been successfully deployed in environments that make few demands or

assumptions. If we are to hope for similarly successful deployment of authentication for DHCP, a means for mitigating (if not eliminating) these difficulties must be offered.

5.3 Replay attacks

Since the configuration token protocol, protocol 0, passes a clear-text authentication token, the token would be visible to any host on the same subnet. Delayed authentication, protocol 1, is not susceptible to replay attacks since it contains a nonce value generated by the source and a message authentication code (MAC) which provides both message and entity authentication.

5.4 Protocol Agreement Difficulties

An a priori agreement is presumed to have taken place between client and server on the authentication protocol to use. No mechanism is provided to allow for the discovery of supported protocols, nor is there a facility for negotiation. The only way to express non-support of a protocol is by failing to respond.

5.5 DHCPv4 Relay Agents Excluded

[RFC3118] is defined exclusively for client-server communication. The role of relay agents has expanded somewhat from their earliest definition to include a DHCP option carrying relay agent information via sub-options [RFC3046]. An authentication sub-option for the relay agent information option has been defined by [RFC4030], though it only defines a single protocol, symmetrical shared-secret keys, to protect the contents of the messages between DHCP relay agents and servers. Work-in-progress to protect the interaction between relay agents and servers using IPSEC [relay-ipsec] seems to have halted, with no recent work.

5.6 Unanticipated Infrastructure Changes

Rapid commit, defined by [RFC4039], specifies how a two-message exchange between client and server can dramatically decrease the elapsed time for address assignment, a feature becoming significant as more and more highly mobile devices desire an abbreviated address assignment phase for short duration communications.

While a two-message exchange by itself does not affect the overall security of the communications, it has two side effects. First, the delayed authentication protocol simply cannot be used as the DHCPOFFER message required to return a nonce value to the client is not present. Second, as noted by the authors of [RFC4039], without authentication it is considerably more likely to consume addresses, increasing the risk of one type of denial of service attack.

CableLabs client configuration [RFC3495] adds another two-tier option to the DHCPv4 options list, defining an initial set of sub-options for passing configuration information specific to CableLabs VoIP and possible future services. Although several of the sub-options contain potentially sensitive information regarding Kerberos tickets to be used by cable modems and media terminal adapters. The option specification does not require used of DHCP authentication,

although it would seem to be necessary. The authors of this memo do not wish to go so far as to recommend that DHCP authentication be a requirement for any or all DHCP options, but the CableLabs client configuration option will likely not be the last option that could benefit from a robust, workable authentication implementation.

Passive duplicate address detection [p-dad] is a relatively new proposal to replace the use of ICMPECHO and ARP messages by DHCP clients and servers to improve the duplicate address detection process by passively listening to message traffic and developing a table of matches between chaddr, DHCP client identifier, and IP address that would be periodically transmitted to interested DHCP servers. The presence of an entry for a particular IP address would signify that it is known to be in use, so a DHCP server could exclude the address from its pool of addresses available for assignment.

The address usage collector (AUC) defined by [p-dad] does not use the DHCP client-server protocol, nor does it function by actively handling DHCP messages, so its implementation would not affect authenticated DHCP messages. However, DHC Working Group discussion of the [p-dad] draft raised the point that the AUC must capture the client identifiers used in DHCP message exchanges. If DHCP authentication were enabled, an AUC of necessity would be required to have the same authentication configuration data (protocol, algorithm, and key) as the clients and servers, certainly a consideration for scalability and risk assessment.

6 DHCPv4 Security Requirements

DHCPv4 was developed in an era when computers were primarily used in business and university environments. Security was either not a concern or was addressed by controlling physical access stemming from the belief that intrusion into critical systems was most likely to come from an external source. Now, with wireless access points and ubiquitous networking, physical access control mechanisms are no longer sufficient, and security and privacy issues are a major concern.

6.1 Environments

The following environments can be expected for DHCPv4 implementations:

- Network size, from a few hosts to hundreds of thousands of hosts.
- Network topology, from a single subnet to Class-A networks.
- Network location, from a single room to international dispersion.
- Wired, broadcast wireless, and directional wireless media.
- Movement between different media and networks.

6.2 Capabilities

The following are essential elements of DHCPv4 security:

1. Clients MUST be able to authenticate servers (to prevent misconfigured clients and assure that the correct servers are being contacted).
2. Servers MUST be able to authenticate clients (use of hardware addresses and client-IDs provides no real security but is all that is easily possible today). Better mechanisms are needed for servers to identify clients to whom they will offer service (to prevent IP address pool depletion, for example).
3. Administrators MUST be able to choose between four authentication paradigms:
   a. No authentication required.
   b. Mutual authentication required.
   c. Client authenticates server.
   d. Server authenticates client.
4. Integrity of DHCP packet exchanges MUST be assured.

Not all capabilities may be needed or desired in all situations.

6.3 Musings on the Key Distribution Problem

The authors believe that only by addressing scalability issues with key distribution can RFC 3118 achieve wide deployment. While it is not our intention to describe solutions in this document, we admit that we find several models used today by browsers and secure web servers as well as token-based user authentication schemes such as the RSA SecureID token to be attractive. Trusted root certificates are distributed with the client implementation (web browser); users have the ability to extend the certificates that they will accept, install their own certificates (should client identification be required), and choose which certificate to present to servers requesting the client's identity. Security tokens that combine a secure seed value with the current time of day using a cryptographic algorithm to produce effectively a random one-time pad are relatively inexpensive and widely available.

Analogously, DHCPv4 servers could make use of certificates just as web servers do, while DHCPv4 clients could be distributed with appropriate certificate authority certificates (trust anchors). Self-signed certificates are, of course, a possibility should an organization wish full control over its domain of trust.

Should this path be pursued, we believe that certificate revocation will be a major problem to confront, just as it is in the browser/web server environment today. Revocation of client certificates (which we believe would occur, on the whole, much more

frequently than revocation of server certificates) would require only ordinary care in certificate validation by the DHCP server.

Revocation of server certificates is more complex because of the difficulty updating client configurations, as well as the inability of clients to rely on certificate revocation lists while in the process of performing IP address and configuration management.

Using a security token device today is mostly to identify a person requesting access to a private resource. Key fobs, USB dongles, or wallet cards are in the possession of a user, and in conjunction with a user name, password, and possibly other information confirms two of the three classic dimensions of provable identity (something you know--user name and password, something you have--the security token, and something you are--biometrics typically satisfy this

dimension.)

We envision a security token becoming part of the host system's hardware complement in the near future, such that the token then becomes not a user identity validator, but a host system validator. It is common today to have a system service tag or serial number that is machine-readable. Some hardware configurations include processors with readable serial numbers as well. What we lack is a secure means to generate a cryptographically random key that cannot be easily defeated by software or component swapping.

Either of these approaches offers a simple way to avoid the classic key distribution problem, though neither is totally without cost. Somehow, somewhere, a token's identifiers (seed and algorithm) must be recorded by the DHCP and other interested servers, or the certificate infrastructure must be in place. We see no way to eliminate administrative issues associated with security, but we can see an end to passwords written on a sticky note.

An interesting Internet-Draft by Alper Yegin et al. [eap-auth] proposed the use of EAP for DHCP authentication using the delayed method. Their draft required modifications to several components of an AAA solution, but illustrated how delayed authentication could be "bootstrapped" using tools at our disposal.

That idea is also suggested by [RFC4014] Ralph Droms and John Schnizlein, who define a DHCP option code for RADIUS information provided by an NAS, similar to the mechanism in [eap-auth]. These two documents taken together may provide a third solution to the key distribution problem.

6.4 Data Confidentiality

Data Confidentiality was not provided for in the original DHCP protocol as defined in RFC 2131 or any of the subsequent RFCs. Historically, DHCP was mainly used to assign IP addresses and return configuration options such as the local gateway and DNS information.

Over time the DHCP protocol has evolved, deployments are extending beyond physically secure intranets to public networks in hotspots, cafes, airports, and at home over broadband. We are seeing an accompanying proliferation of new configuration options.

DHCP has, in fact, become so successful that it is now used to transport a great deal of configuration data that could be obtained in a variety of other ways. It is certainly possible that a client or server will wish to reveal some of these data only to a properly authenticated peer.

6.4.1 "Public" Data in DHCP Packets

We assume that any information that may be gleaned directly from the network using, for example, Ethernet promiscuous mode is not confidential. It could be argued that over time more and more communication will be switched, encrypted, or secured at the physical layer, so that less information could easily be gleaned from the network traffic.

Taking encryption into consideration, the IP packet payload might be encrypted, but not the IP header itself since it is required for packet routing. As a result, none of the IP header fields are confidential. IP addresses included in the header are therefore not confidential. Similarly, the hardware addresses are also not confidential.

Although the IP packet payload (which would include the UDP or TCP header) might normally be encrypted, some protocols have made explicit decisions not to encrypt their exchanges, declaring their data public. DNS is such a protocol [dns-threats]. Thus, we may also treat DNS domain and server information as public.

Commonly used routing protocols such as BGP [RFC1771], RIP [RFC1721], and router discovery [RFC1256] also normally send advertisements in the clear and we therefore extend our treatment of public DHCP data to routing information.

6.4.2 Protecting Data in DHCP Options

Some DHCP options (e.g., relay agent options, [RFC3046]) or option families (site or vendor options) admit no analysis because the data carried by them may be of unknown sensitivity. Users must do their own analysis of confidentiality.

Should some data require confidentiality, it may be possible to exploit the "public" data above to allow a two-step configuration process in which sufficient client configuration is first obtained by the normal DHCPDISCOVER/OFFER/REQUEST/ACK exchange, and private data subsequently transmitted over a secure communications channel (such as IPsec) using DHCPINFORM.

6.5 Host versus User Authentication

[RFC3118] is concerned specifically with DHCP clients and servers authenticating themselves to each other if required by an

administrative domain. This is not the same thing as authenticating users for establishing their Identity, access rights, permissions, or other matters relating to what they can view or do once connected to the network.

6.5.1 Why do we make this distinction?

Host authentication provides only assurance that the hosts connecting to a network are recognized. This may be for several reasons, including:

- Requirement to restrict network access from "foreign" hosts to ensure consistent technical support or meet other regulatory requirements such as double-insulation or non-sparking.

- Requirement to restrict network access from "unsecured" (for instance, non-TEMPEST compliant) hosts in a high security network.

- Requirement to restrict network access from unknown hosts whose identity has not been recorded by existing administrative procedures, saving troubleshooting and administrative effort.

User authentication focuses on the individual users of a host system, seeking to uniquely identify someone to establish their rights to view, print, add, alter, delete, edit, modify, copy, or manipulate any data maintained by an organization, run software programs, or affect changes in the environment. This may be for such reasons as:

- Requirement to be compliant with regulations such as HIPAA, SOX, and GLBA designed to safeguard and protect confidentiality and various reporting requirements.

- Requirement to maintain reasonable controls over access to certain critical systems such as utility power grids, water and sewage treatment plants, the network infrastructure itself, and life safety systems of all sorts.

- Requirement to maintain administrative controls over certain sensitive information such as trade secrets and personnel data

6.5.2 Is one mechanism sufficient?

Full discussion of this question is beyond the scope of this memo, but the simple answer is, "probably not." This has a significant implication for the claims of certain techniques such as "sandboxing" of unverified users, restricting their network access to a user registration web site until their identity has been established. Simply put, limiting network access is not DHCP authentication, although it does represent a very workable approach to user authentication in many cases.

Recall that a user can be identified by "something they know," "something they have," and "something they are." While the same could be said to be true of host systems, the authors point out that while we do not pretend to understand all of the ways that future developers might imbue hosts with the tools to independently create attacks on our infrastructure, we will assert that users will be the greatest risk for some time still.

DHCP Authentication addresses only host authentication from the belief that other, existing mechanisms such as IPSEC, SSL, and VPN

can protect the content of communications, with Identity Management and other technologies can protect applications and data.

A properly authenticated host could still launch a denial of service attack, corrupt sensitive data, or wreak other havoc, which underscores our point that host and user authentication are different.

A well-secured network needs both.

7 IANA Considerations

None known.

8 Security Considerations

This entire memo presents a threat analysis of the DHCPv4 protocol.

9 Acknowledgements

This document is the result of work undertaken the by DHCP working group, beginning at the 55th IETF meeting in Atlanta. The authors would also like to acknowledge contributions from others not

directly involved in writing this memo, including John Beatty and Vipul Gupta of Sun Microsystems, Ralph Droms of Cisco Systems, Bernard Aboba of Microsoft, and Mark Stapp of Cisco Systems for their careful reviews and helpful suggestions.

10 References

10.1 Normative References

[RFC1256] Deering, S., "ICMP Router Discovery Messages," RFC 1256, September 1991.

[RFC1541] Droms, R., "Dynamic Host Configuration Protocol," RFC 1541, October 1993.

[RFC1721] Malkin, G., "RIP Version 2 Protocol Analysis," RFC 1721, November 1994.

[RFC1771] Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4)," RFC 1771, March 1995.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol," RFC 2131, March 1997.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option," RFC 3046, January 2001.

[RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages," RFC 3118, June 2001.

[RFC4014] Droms, R. and J. Schnizlein, " Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option," RFC 4014, February 2005.

10.2 Informative References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3," RFC 2026, BCP 9, October 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3203] T'Joens, Y., C. Hublet and P. De Schrijver, "DHCP Reconfigure Extension," RFC 3203, December 2001.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," RFC 3315, July 2003.

[RFC3495] Beser, B. and P. Duffy, "Dynamic Host Configuration Protocol (DHCP) Option for CableLabs Client Configuration," RFC 3495, March 2003.

[RFC3594] Duffy, P., PacketCable Security Ticket Control Sub-Option for the DHCP CableLabs Client Configuration (CCC) Option"," RFC 3594, September 2003.

[RFC3978] Bradner, S., "IETF Rights in Contributions," RFC 3978, BCP 78, March 2005.

[RFC3979] Bradner, S., "Intellectual Property Rights in IETF Technology," RFC 3979, BCP 79, March 2005.

[RFC4030] Stapp, M. and T. Lemon, "The Authentication Suboption for the DHCP Relay Agent Option," draft-ietf-dhc-auth-suboption-03), RFC 4030, March 2005.

[RFC4039] Park, S., P. Kim and B. Volz, "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)," RFC 4039, March 2005.

[RFC4388] Woundy, R., and Kinnear, K., "Dynamic Host Configuration Protocol (DHCP) Leasequery," February 2006.

[dns-threats] Atkins, D. and R. Austein, "Threat Analysis Of The Domain Name System," draft-ietf-dnsext-dns-threats-07 (work in progress), April 2004.

[draft2223bis] Reynolds, J. and R. Braden, "Instructions to Request for Comments (RFC) Authors," draft-rfc-editor-rfc2223bis-08.txt (work in progress), August 2004.

[eap-auth] Yegin, A., H. Tschofenig and D. Forsberg, "Bootstrapping RFC3118 Delayed DHCP Authentication Using EAP-based Network Access Authentication," draft-yegin-eap-boot-rfc3118-02, (work in progress), March 2006.

[failover] Droms, R. and K. Kinnear, "DHCP Failover Protocol," draft-ietf-dhc-failover-12 (work in progress), December 2003. [Editor's note: at the time of publication of this memo, the Failover Internet-Draft has expired.]

[fqdn] Stapp, M., Volz, B., and Y. Rekhter, "The DHCP Client FQDN Option," draft-ietf-dhc-fqdn-option-13 (work in progress), March 2006.

[p-dad] Forte, A., S. Shin and H. Schulzrinne, "Passive Duplicate Address Detection for Dynamic Host Configuration Protocol (DHCP)," draft-forte-dhc-passive-dad-02 (work-in-progress), June 2006.

[relay-ipsec] Droms, R., "Authentication of DHCP Relay Agent Options Using Ipsec," draft-ietf-dhc-relay-agent-ipsec-02 (work in progress), May 2005. [Editor's note: at the time of publication of this memo, the Relay IPSEC Internet-Draft has expired.]

Authors' Addresses

Richard Barr Hibbs
Richard Barr Hibbs, P.E.
952 Sanchez Street
San Francisco, California 94114-3362
USA

Phone: +1 415 648 3920
Fax: +1 415 648 9017
E-Mail: rbhibbs@pacbell.net

Carl Smith
C & C Catering
1121 Holly Street
Alameda, California 94502
USA

E-Mail: islandia@alumni.ucsd.edu

Bernard Volz
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, Massachusetts 01719
USA

Phone: +1 978 936 0382
E-Mail: volz@cisco.com

Mimi Zohar
IBM T. J. Watson Research Center
19 Skyline Drive
Hawthorne, New York 10532-2134
USA

Phone: +1 914 784 7606
E-Mail: zohar@us.ibm.com

Full Copyright Statement

Intellectual Property

rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

APPENDIX: NOTES

This appendix will be removed in its entirety before the memo goes to Working Group Last Call.

ISSUES LIST

This section summarizes issues raised in this memo that require resolution by the DHC Working Group.

1. Because of the specific exception for inclusion of the Relay Agent Information Option [RFC3046] in cases where it does not fit in the main payload portion of a DHCP response packet, should the use of DHCP Authentication be mandated in place of the Relay Agent Authentication suboption?

2. Does the CableLabs Client Configuration option [RFC3495] require the use of DHCP Authentication to protect sensitive information about Kerberos domains and keys?

3. Should the DHC Working Group promote the development of a new authentication protocol based on the use of certificates?

4. Should the DHC Working Group solicit an update from the authors of the EAP-based authentication protocol [eap-auth] and develop it as a new authentication protocol?

5. Should the DHC Working Group promote the development of a new authentication protocol based on hardware security tokens?

CHANGE LOG

This section summarizes the changes made to this memo as it has evolved.

"-01" Draft

No significant changes were made from initial ("-0") version:

- Updated author information.

- Removed unused references.

- Added the Change Log section.

"-02" Draft

The following changes were made:

- Updated author information.

- Added text to 1.3 to exclude security for messages passed between relay agents and servers, as there are two Internet-Drafts on this subject.

- Reworded several sections in section 2.

- Revised and renamed section 2.1.2. Now includes more attacks.
- Revised section 2.1.3.
- Minor revisions to section 3, 3.2, and 3.2.
- Other minor insertions, deletions, and modifications based on comments from Bernard Aboba and Mark Stapp and to otherwise improve the document.

"-03" Draft

The draft was updated, correcting minor spelling, grammatical, and typographical errors, and modified in the following ways:

- Removed Section 8, "Change Log," to APPENDIX and added an issues list section.
- Replaced all Internet-Draft boilerplate with the most current versions.
- Renumbered document sections.
- Updated author information.
- Updated references for I-Ds advanced to RFCs.
- Added normative and informative references.
- Added discussion of Relay Agents (section 3.5.)
- Added section 3.6, discussing the side effects of infrastruture changes from the Rapid Commit and CableLabs configuration options, and the newly proposed Address Usage Collector (AUC) for passive duplicate address detection.
- Expanded section 4.3, "Musings on the Key Distribution Problem" to include description of hardware-based key generation tokens.
- Added section 4.5, "Host versus User Authentication," to help clarify the problem [RFC3118] is intended to address.
- Added discussion of the RADIUS-based authentication proposal described in [RFC4014].

- Added discussion of the EAP-based authentication protocol proposed by A. Yegin et al.

- Inserted Intellectual Property Rights statement on first page.

- Performed general spelling, grammar, and typography update of entire memo text.

- Reviewed all drafts used as references, updated as necessary.