DHCPにおけるメッセージ認証機能の実装と評価

上山 晴久†, 小林 和真‡, 山口 英†

†奈良先端科学技術大学院大学
‡倉敷芸術科学大学/奈良先端科学技術大学院大学

概要

ホストの接続を自動化するDHCPでは、クライアントやサーバの認証について全く考慮されていない。これに対し、IETFではDHCPにおいて認証を行なう方法が提案されているが、この方法には曖昧な点がありそのまま実装することはできない。そこで、本稿ではDHCPにおける認証の必要性を議論し、実装方法を明確にしたDMA(DHCP Message Authentication)方式を提案する。また、この方式を用いて認証機能を持つDHCPを実装し、その有効性を示す。

Implementation and Evaluation of the authentication mechanism for DHCP.

Haruhisa Kamiyama†, Kazumasa Kobayashi‡, Suguru Yamaguchi†

†Nara Institute of Science and Technology
‡Kurashiki University of Science and the Arts/Nara Institute of Science and Technology

Abstract

DHCP does not support the mechanism with which clients and servers authenticate each other. At IETF, the authentication mechanism for DHCP has been proposed as Draft, but it has some vague points, so the authentication mechanism cannot be realize just as described. This Paper discusses the need for the authentication mechanism for DHCP, proposes the DMA(DHCP Message Authentication) method as its improved mechanism. This paper also presents the implement of the DHCP with the authentication mechanism based on the DMA, and shows its availability.

1 はじめに

コンピュータ関連技術の発展に伴ない、小型軽量で持ち運び可能なノート型コンピュータ(移動ホストと呼ぶ)が普及している。移動ホストは利用者とともに移動し、様々なネットワークに接続される。

ネットワークに接続するホストがIPアドレスや経路などの情報を獲得するためのプロトコルであるDHCP(Dynamic Host Configuration Protocol)[1][2]は、移動ホストなどで広く利用されている。

しかし、現在のDHCPはセキュリティについて全く考慮されていない。ネットワークに接続

しようとする全てのクライアントの要求に対してIPアドレスの割当てを行なうため、誰にでもアクセスを許してしまう。また悪意を持ったサーバが不正な情報を配布し、クライアントやそのネットワークを混乱させることもできる。

これに対してIETFではDHCPメッセージにDHCP認証オプションを付加することでサーバやクライアントの認証を行なう方法[3]が提案されているが、現在はDraftであり記述内容に曖昧な点があるため、このままでは実装を行なうことはできない。

本稿では、IETFで提案されている方法における曖昧な点を指摘し、実装方法を明確にしたDMA(DHCP Message Authentication)方式を提案する。また、この方式を実装することでDHCPメッセージ認証機能を実現し、評価を行なう。

2 DHCPにおけるセキュリティ

2.1 DHCPの概要

インターネットにコンピュータを接続する際に必要となる作業の自動化を行なうための機構としてDHCPが広く利用されている。DHCPは、クライアントサーバ方式であり、サーバがネットワークに接続されたクライアントとDHCPメッセージの交換を行なうことで資源を割り当て、設定情報の配送を行なうためのプロトコルである。

2.2 DHCPにおける認証の必要性

DHCPは元来ディスクレスワークステーションなどに資源を割り当てるためのプロトコルであり、これらの装置にはパスワードなどを用いた認証機構の導入が困難なことからセキュリティについては全く考慮されていない。このため以下のような問題が生じる可能性がある。

DHCPクライアントの認証を行なわない場合

DHCPクライアントの認証を行なわない場合、どのクライアントからの要求に対してもDHCPサーバはIPアドレスの割り当てを行なう。このため、次のような問題が生じる。

- 無線LANを用いた環境や大学の講義室のような場所で、ネットワークを不正に利用することができる。
- 悪意を持ったクライアントが、サーバが割り当て可能な全てのIPアドレスを要求し、正当な利用者への割り当てを不可能にすることができる。

DHCPサーバの認証を行なわない場合

DHCPサーバの認証を行なわない場合、クライアントは不当なサーバからの情報を区別できない。このため、次のような問題が生じる。

- 悪意を持ったサーバが重複したIPアドレスを割り当てたり、不正な設定情報を配布することで、ネットワークを混乱させることができる。
- 悪意を持ったサーバが、クライアントが設定情報要求の際に発行するDHCPREQUESTメッセージに対して、それを拒否するDHCPNAKメッセージを送信し、クライアントのネットワーク利用を不可能にすることができる。

これらの問題を解決するため、DHCPにおいて、クライアントとサーバが互いを認証する機能を実現する必要がある。

2.3 IETFで提案されている認証方式

現在、IETFではInternet Draft "Authentication for DHCP Messages"[3]として、DHCPメッセージ認証機能を提供する方式が提案されている。

この方式では、DHCPオプションの1つとして認証情報を交換するためのDHCP認証オプションの定義と、プロトコル0およびプロトコル1の2つのプロトコルが定義されている。

プロトコル0では、認証情報として認証トークンと呼ばれるパスワードなどの文字列を用い

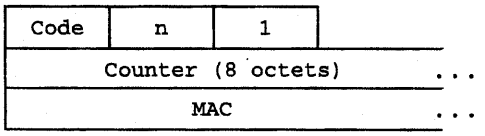

図 1: プロトコル 1 を使用する場合の DHCP 認証オプションのフォーマット

る認証が定義されている。しかし、認証トークンは暗号化されずそのまま送信されるため、十分な安全性を確保することはできない。

プロトコル 1 では、次のことが定義されている。

- 認証情報として MAC(Message Authentication Code) と呼ばれるデジタル署名とカウンタを用いること。
- MAC の計算には暗号化ハッシュ関数として MD5[4] を利用した HMAC[5] を用いること。
- MAC の計算で利用する鍵は共有鍵を用いること。
- MAC を利用した認証手順。
- カウンタを利用したリプレイ攻撃の防止方法。
- 認証に失敗した DHCP メッセージは破棄すること。

プロトコル 1 ではまた、MAC の計算に使用する鍵の管理方法について議論がなされている。また、鍵生成のアイデアとして、クライアントの識別子とサーバのマスター鍵から鍵を作成する方法が付録で紹介されている。

プロトコル 1 での認証手順は次のとおりである (図 2)。

1. 送信者は秘密鍵を用いて MAC を計算する。
2. 送信者はカウンタとして現在時間などの単調増加の値を設定する。

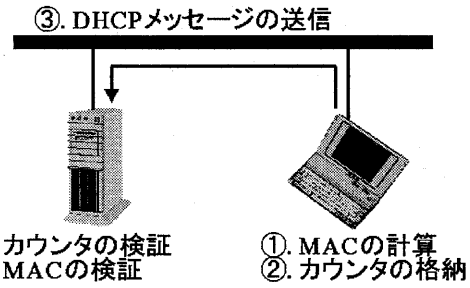

図 2: 認証手順

3. DHCP 認証オプションを含む DHCP メッセージを送信する。
4. メッセージの受信者は、カウンタの確認を行なう。ある送信者からのメッセージのカウンタが以前に同じ送信者から送られてきたメッセージに含まれるカウンタより小さいか等しい値であるとき、認証は失敗する
5. 受信者は MAC の計算をして、DHCP 認証オプションに含まれる送信者が計算した MAC と一致するか確認する。

3 DMA 方式の提案

前節で説明した IETF での提案は、曖昧な点があるためそのまま実装することはできない。本稿では、その点を指摘し、実装方法を明確にした DMA 方式を提案する。

DMA 方式では、IETF で提案されている 2 つのプロトコルを利用する。このうち、プロトコル 0 はそのまま実装可能である。ここでは、IETF での提案のプロトコル 1 における曖昧な点について議論し、DMA 方式で採用する方法について述べる。

3.1 MAC の計算対象

IETF での提案では、MAC の計算対象についての定義がなされていない。

MAC の計算に DHCP メッセージ全体を利用すれば DHCP メッセージの安全性を確保するこ

とが可能となる。そこで、DMA方式ではMACの計算対象はDHCPメッセージ全体とする。

また、MACの計算の際にDHCP認証オプションを含むか記述されていないが、DMA方式では含むこととする。MACフィールドは0で埋めておく。

3.2 プロトコル1におけるDHCP認証オプションの長さ

IETFでの提案では、プロトコル1におけるDHCP認証オプションの長さが定義されていない。プロトコル1のMACの計算にはHMAC-MD5を用いることが定義されており、HMAC-MD5で計算されるMACの長さは16オクテットである。これよりプロトコル1におけるDHCP認証オプションの長さはプロトコルとカウンタのフィールドを加えた25オクテットと定義できる。

3.3 鍵管理

この節では、クライアントとサーバの鍵の管理と利用の方法について述べる。

3.3.1 鍵の管理方法

DHCPメッセージ認証での利用が想定される鍵の管理方法として次の方法が考えられる。

1. 各クライアントは鍵を持っており、サーバでは正当なクライアントの鍵が管理される。

2. 各サーバは自身の鍵を持っており、正当なクライアントに対してその鍵を配布する。

3. 1対のクライアントとサーバで1つの鍵が作成され、両者で管理される。

これらの方法について考察する。

1では、鍵の作成、管理の容易さに加え、各サーバへのアクセスに同じ鍵を利用できる利点があるが、鍵の漏洩に対しては全てのサーバでの鍵の置き換えが必要となる。

2では、鍵の作成、管理が容易であるが、サーバは各クライアントを識別できないため、後に特定のクライアントからのアクセスを拒否することが不可能であり、鍵の漏洩に対しては全ての正当なクライアントに対して鍵を再配布する必要がある。

3では、サーバは新たなクライアントに対して鍵を生成する必要があるが、クライアントの識別が可能であり、鍵の漏洩にも鍵を使用しているサーバとクライアントで鍵を再生成すればよい利点がある。

DHCPメッセージ認証における鍵の管理方法では、次の点が重要となる。

- 特定のクライアントからのアクセスを拒否することが可能であること。
- 鍵の漏洩への対処が容易であること。

そこで、DMA方式では鍵の管理方法に3を使用する。

3.3.2 クライアントの識別

サーバでは複数のクライアントの鍵を管理しているため、受信したDHCPメッセージを送信したクライアントの識別が必要となる。そこで、DMA方式ではクライアントの識別子をDHCPオプションを利用して配送し、クライアントの識別を行なう。

クライアントの識別子は、サーバが管理しているクライアント間で重複してはいけない。接続するDHCPサーバが異なるときクライアントの識別子は異なっていてもよい。

DMA方式では、サーバが管理しているクライアント間で重複しない任意の文字列を識別子として用いる。

3.3.3 鍵の生成

IETFでの提案の中で述べられている共有鍵の生成方法では、クライアントとサーバの共有鍵は、暗号化ハッシュ関数H、クライアントをユニークに識別するための識別子 $ClientID$、マスター鍵 MK として、

$$\mathrm{H}(MK, ClientID)$$

で計算される。マスター鍵はサーバが管理している鍵で、各サーバに1つずつ用意されている。

この方法では、あるサーバで同一のクライアントの識別子に対して同一の鍵が生成されるため、鍵の漏洩などで鍵を再生成するためには、クライアントの識別子を変更する必要がある。そこで、DMA 方式では鍵を生成する度に異なる要素 r を使用して、

$$\mathrm{H}(MK, ClientID, r)$$

の計算結果を用いる。

ハッシュ関数としては MD5 を用いる。*ClientID* には前節で述べたクライアント識別子を利用する。

3.3.4 鍵の選択

複数のサーバの鍵を管理するクライアントは接続するネットワークに応じて鍵を選択する必要がある。

この方法として、DHCP メッセージ交換で自動的に選択する方法と、クライアントの利用者が手動で指定する方法が考えられる。

自動的に選択する方法

サーバの識別子を自動的に獲得してサーバの選択するを行なう。サーバの識別子は、DHCPOFFER メッセージなどで配送され、このメッセージを受信することで獲得が可能である。

IETF での提案の中では、認証を行なうメッセージの種類は定義されていない。そこで、DHCPDISCOVER メッセージの認証を行なわないことで、サーバの選択を次の手順で行なう。

1. クライアントは DHCPDISCOVER メッセージをその識別子を含めて送信する。

2. DHCPDISCOVER メッセージを受けとったサーバが、送信したクライアントの鍵を管理しているなら DHCPOFFER メッセージを送信する。その際 DHCP 認証オプションも付加する。

3. DHCPOFFER メッセージを受信したクライアントは、そのサーバの識別子を入手したため、そのサーバの鍵で認証を行なう。もし認証が成功すれば、後のメッセージ交換にはその鍵を使用する。

この方法では、正当でないクライアントが正当なクライアントの識別子を含む DHCPDISCOVER メッセージを送信することで、DHCPOFFER メッセージを受けとることが可能となる問題がある。

手動で指定する方法

クライアントの利用者が手動で指定する方法では、DHCPDISCOVER メッセージを含む全てのメッセージにおける認証を行なう利点がある。

しかし、手動で指定する方法では、DHCP においてサーバの IP アドレスなどの知識なしで利用できる利点を無駄にしてしまう。

そこで、DMA 方式では自動的にサーバを選択する方法を利用する。

4 実装と評価

本稿では、DMA 方式を実装することにより、DHCP メッセージ認証機能を実現した。

4.1 実装

実装は、C 言語を用いて BSD/OS 上で WIDE 版 DHCP(dhcp-1.4.0p1) に改造を加えることで行なった。サーバは約 800 行、クライアントは約 650 行追加した。

送信側での DHCP 認証オプションの処理は、DHCP メッセージが完成してから行ない、受信側では DHCP メッセージの処理を開始する直前に行なった。

プロトコル 1 で利用するカウンタの値には、BSD/OS で提供されている gettimeofday 関数で得られる現在時刻を用い、受信側ではカウンタの値は timeval 構造体で参照した。timeval 構造体は 2 つの 4 オクテットのロング型整数から

なる。これを利用することで8オクテットのカウンタの比較を容易に行なうことができる。

また、サーバのマスター鍵を作成するプログラム、サーバとクライアントの共有鍵を作成するプログラムも提供した。

4.2 評価

4.2.1 動作確認

ネットワーク上にDMA方式で実装したクライアントとサーバを用意し、以下の実験を行ない実際に認証を行なっていることを確認した。

- DHCP認証オプションを含まないDHCPメッセージを受信したサーバはそのメッセージを破棄した。
- DHCP認証オプションにクライアントの共有鍵以外で計算したMACを付加したDHCPメッセージを受信したサーバはそのメッセージを破棄した。
- 正当な鍵を利用し計算したMACを付加したDHCPメッセージを受け取ったサーバはそのメッセージを処理し、適切なDHCPメッセージを返信した。

クライアントにおいても同様の動作確認を行なった。このことから、認証機能は実現できたと言える。

4.2.2 安全性

DMA方式では、送信するDHCPメッセージごとにHMACで計算したMACにより認証を行なっている。そのため、認証の強度はHMACの強度に依存する。

DMA方式では、共有鍵が漏洩した場合その鍵を無効にすることで安全性を保っている。しかし、この方式では鍵の漏洩を検出する方法は提供していない。そのため、漏洩した鍵によるアクセスの検出は、利用者に委ねられる。

5 まとめ

本稿ではIETFで提案されているDHCPメッセージ認証機能の曖昧な点を指摘し、実装方法を明確にしたDMA方式を提案した。この方式により、DHCPを利用する環境でのサーバ、クライアント認証を実現することができた。

また、IETFではリレーエージェント認証の必要性についても議論されている[6]。今後は、DMA方式のリレーエージェントへの拡張についても検討したい。また、現在のDMA方式では鍵の交換や更新については考慮していない。これについても今後検討する必要がある。

参考文献

[1] R. Droms: "Dynamic Host Configuration Protocol", RFC 2131 (1997).

[2] S. Alexander, R. Droms: "DHCP Options and BOOTP Vendor Extensions", RFC 2132 (1997).

[3] R. Droms 編: "Authentication for DHCP Messages", Internet Draft (1997).

[4] R. Rivest: "The MD5 Message-Digest Algorithm", RFC 1321 (1992).

[5] H. Krawczyk,M. Bellare, R.Canetti: "HMAC: Keyed-Hashing for Message Authentication", RFC 2104 (1997).

[6] O. Gudmundsson: "Security Architecture for DHCP", Internet Draft (1997).