3ZA-7

IPヘッダへの利用者認証フィールド埋め込み型認証システムの改良

加藤　央　　安井　浩之　　吉野　邦生

東京都市大学

1. はじめに

コンピュータのインターネット接続が一般的になり，大学の図書館や食堂など不特定多数が利用可能な場にも，簡単にネットワークへ接続できる環境が整っている．このような環境を用いることでネットワーク接続の利便性が向上する反面，使用が許可されていないユーザによる不正利用や，悪意のあるユーザによる盗聴などセキュリティの問題が浮上している．

このような問題に対して我々はAIPS(Authenticated IP System)[1]を提案・開発してきた．しかし，AIPSには認証の手法や強度に脆弱性が残っている．

本報告ではAIPSの脆弱性を解決するための改良とその安全性について述べる．

2. AIPS

2.1 概要

AIPSは特定多数のユーザが利用する情報コンセント環境を想定したユーザ認証システムで，図1で示すようなIPv4のクラスC規模(/24)ネットワーク(以下，認証ネットワーク)を対象とする．ユーザ認証はゲートウェイ上で動作する認証サーバプログラム(以下，認証サーバ)と，持込端末上で動作する認証クライアントプログラム(以下，認証クライアント)により実現している．

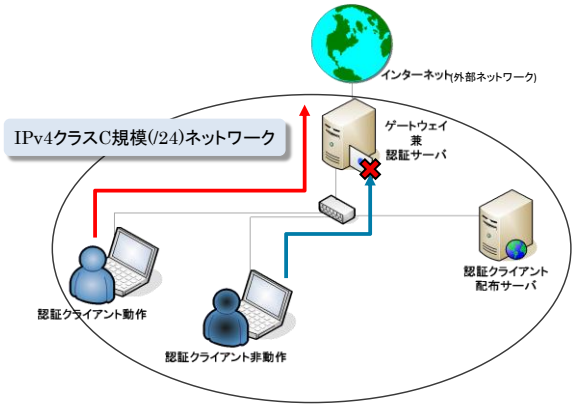

図1 AIPSのシステム構成

Improvement of LAN System with User-Authenticator Embedded into IP Header
Hiroshi Kato, Hiroyuki Yasui, Kunio Yoshino
Tokyo City University

認証ネットワークを利用するユーザは事前にユーザIDと接続用パスワードを認証サーバに登録している必要があり，認証サーバ・認証クライアントは登録したユーザIDと接続用パスワードをもとに認証情報を生成・照合を行う．正規でないユーザや認証クライアントの動作していない持込端末から送信されるIPパケットはその認証情報を用いてゲートウェイ兼認証サーバで破棄する．

2.2 特徴

AIPSの特徴はIPヘッダに認証情報を埋め込む点である．対象とする情報コンセントは/24ネットワークであることから，送信元IPアドレスの上位24bitはそのネットワーク内部で同一であり，冗長である．これを利用し，IPヘッダの冗長な部分に認証情報を埋め込む．これによりIPパケット長を変えることなく通信ができるので，フラグメントを起こすことなくEthernetのパケットサイズを十分に活用することができる．

認証ネットワーク内を流れるパケットのIPヘッダは図2のようになる．

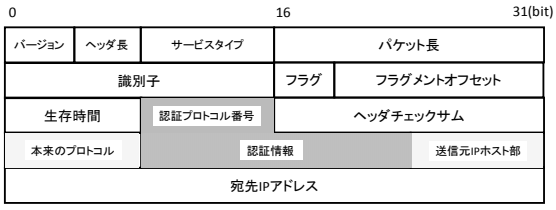

図2 AIPSでのIPヘッダ

認証までの流れはまず，認証クライアントはDHCPサーバよりIPアドレスが割り振られた後，認証サーバにユーザIDとIPアドレスを告知する．それに対し認証サーバはユーザIDとIPアドレスの対応を格納し，認証クライアント宛にリプレイアタック対策のワンタイムパスワード(OTP)を発行する(この通信をファーストコンタクトと呼ぶ)．ファーストコンタクト後，認証クライアントはOTP・接続用パスワード・IPペイロード部から認証情報を生成してIPヘッダに埋め込み，外部に向けて通信を開始する．認証サーバはIPパケットに対し認証を行い，正規の認証情報であればIPヘッダを復元して外部ネットワークに送信する．

2.3 問題点

AIPS における問題点としてリプレイアタックや DoS 攻撃の危険性が挙げられる．AIPS では 2.2 で述べたようにリプレイアタック対策として OTP を認証情報生成時に使用しているが，この OTP の有効期限内であれば同一の認証情報を利用して認証を行うため，リプレイアタックの危険性は残っている．また，パスワードを解析する手段として総当たりで認証を試すブルートフォースアタックが存在する．一般的な認証システムで有効とされている認証情報の bit 長は 64bit 以上[2]であり，16bit の認証情報を用いている AIPS は 65,536 通りしか認証情報を表現することができずブルートフォースアタックで通信が成立してしまう確率が高い．その対策として複数回認証が失敗するとその IP アドレスからのアクセスを遮断する仕様となっているが，悪意のあるユーザが正規ユーザになりすまし，故意に認証を複数回失敗することで DoS 攻撃が成立してしまう．

3. AIPS の改良点

3.1 認証情報の拡張

これまでの AIPS は図 2 の様に改変された IP ヘッダを通常の IP ヘッダへ復元する時，送信元 IP アドレスの下位 8bit の送信元 IP ホスト部を使用している．そこで，ファーストコンタクト時に送信元 MAC アドレス・ユーザ ID・IP アドレスと後述するカウンタを関連付け，認証時に送られてきたパケットの送信元 MAC アドレスを基に，IP アドレスを復元する．このように，MAC アドレスを復元に使用することで，送信元 IP アドレスホスト部を含めた 24bit に認証情報を拡張する．さらに，フラグメント時に使用する IP ヘッダの識別子フィールド(16bit)を利用することで 40bit まで拡張する．

3.2 認証手法の改良

改良した認証までの流れを図 3 に示す．

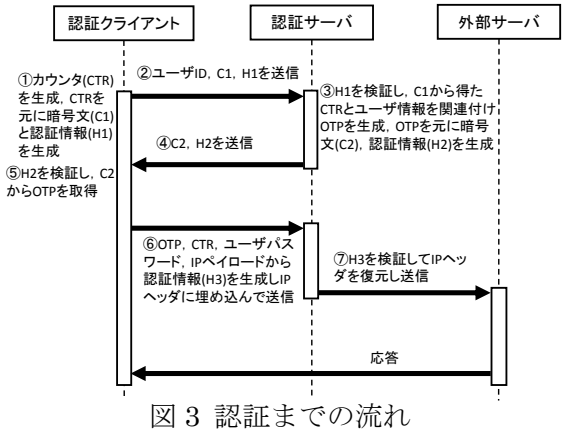

図 3 認証までの流れ

従来の認証手法では，OTP にリプレイアタックの危険性が残っている．そこで，2.2 で述べた 3 種類のデータに加えて，認証情報の生成毎に変化するカウンタ(CTR)を使用しリプレイアタックの危険性を軽減するように改良する．具体的にはファーストコンタクト時に認証クライアント・サーバ間で CTR を同期させておき，パケットを送受信する毎にインクリメントして認証情報の生成に使用する．同期方法は，認証クライアント側で CTR を生成・暗号化(C1)し，C1 に対する認証情報(H1)を生成して C1・H1・ユーザ ID を接続要求として送信する(図 3 中の①，②)．CTR を受け取った認証サーバは OTP に対する暗号文 C2 と，C2 に対する認証情報(H2)を返答する(図③中の③，④)．C2，H2 を受け取った認証クライアントは OTP・CTR・ユーザパスワード・IP ペイロード部を基に認証情報(H3)を生成し IP ヘッダに埋め込んで送信する(図 3 中の⑥)．これを受け取った認証サーバは検証後，MAC アドレスを基に IP ヘッダを復元して外部サーバに送信する．

4. 安全性について

前述の通り CTR はパケット毎に変化するため，リプレイアタックに強い認証手法であると言えると共に，IP アドレスや MAC アドレスの偽装を検出し警告を促すことが可能となる．さらに，認証情報を 40bit に拡張することで認証失敗許容回数を増やすことが可能となり DoS 攻撃が成立する前に管理者が対処することができる．

AIPS の認証情報生成には HMAC[3]を採用している．HMAC の出力 MAC 値の切捨てについて，リストガイド[2]で 32bit 以上と定められており，条件を満たしている．

5. まとめ

本報告では AIPS の脆弱性を解決するための認証手法の改良について示した．今後は本システムの実験・テストを行い，安全性評価をした上でより実運用に近いシステム実装を目指す．

参考文献

[1] 安井浩之　松山実：“IP パケット認証ゲートウェイシステム AIPS” 情報処理学会論文誌 Vol.47 No.7 pp.2614-2622 (2008)
[2] 2008 年度版リストガイド(メッセージ認証コード) 独立行政法人情報通信研究機構 (2009)
[3] M. Bellare, R. Canetti and H .Krawczyk "Keying Hash Functions for Message Authentication" CRYPTO'96 pp1-15, (1996)