

IP ヘッダへの利用者認証フィールド埋め込みによる認証システム

5H-01

川内 拓行 安井 浩之 松山 実

武蔵工業大学

1. はじめに

近年利用されている情報コンセントの多くは利用者認証機能を持たない DHCP により IP アドレスがノードに配布されるため、正式に許可を得ていない者の不正な利用を許してしまう。また専用のハードウェアを組み合わせた利用者認証機構も存在するが、既存の情報コンセントシステムに組み込むにはコストがかかる。本稿では認証機能を備えていない既存の情報コンセントシステムを有効活用した、ソフトウェアによる認証システムの実現を目指す。

前回の報告[1]では認証システムの概要について述べたが、ここでは詳細な設計ならびに測定について記す。

2. 認証システム

本システムはクライアントから発信される IP パケットに特別な認証フィールドを埋め込むことにより利用者認証を行う[2]。認証は送信する IP パケットのデータ部を用いてハッシュ化するため、仮にデータを第三者に改竄された場合でもその IP パケットは認証されないで安全性が確保される。またクライアントで受信する IP パケットに対しては加工を行わない。認証の対象となるネットワークは認証クライアント、認証サーバから構成される。それぞれの機能を図 1, 2 に示す。

各ノードで IP パケットの捕捉[3]を行うため、パケットキャプチャライブラリ pcap を用いる。

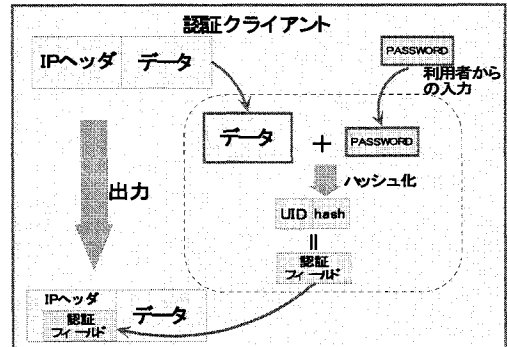


図 1 認証クライアントプロセス

認証クライアント動作手順

- 1 クライアントで生成した送信パケットを pcap で捕捉
- 2 パケットデータと利用者 Password をハッシュ化
- 3 ハッシュ値と UID(UserID)より認証フィールド生成
- 4 送信パケットに認証フィールドを埋め込む
- 5 認証サーバへ送信

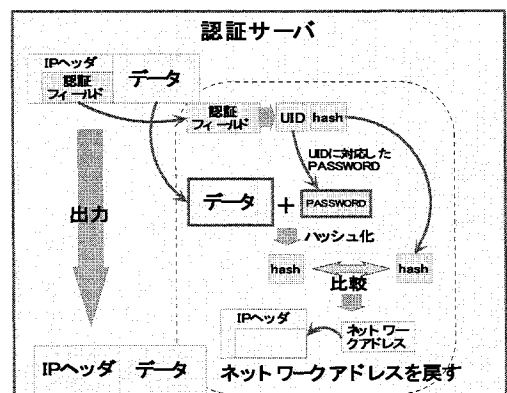


図 2 認証サーバプロセス

Authentication system with user-authentication-field embedded into IP-header.

Takuyuki Kawauchi, Hiroyuki Yasui,

Minoru Matsuyama.

Musashi Institute of Technology.

認証サーバ動作手順

- 1 受信パケットを認証サーバで捕捉
- 2 認証フィールドから UID とハッシュ値を取得
- 3 UID に対応した Password と IP パケットデータ部を合成しハッシュ化
- 4 生成したハッシュ値と受信ハッシュ値で比較
- 5 認証時にネットワークアドレスを正規に戻す
- 6 パケットを送信

4. パフォーマンス測定

認証機能を付加することによるネットワークトラフィックへの影響について測定を行うため、FTP 転送速度を測定する。実験は認証クライアント、認証サーバ、FTP サーバのノードから構成(図 3 参照)し、外部から影響を受けないよう独立したネットワークで行う。認証フィールド有り、無し状態で PUT と GET の速度、パケット数を計測し、パフォーマンス低下の度合を測定する。

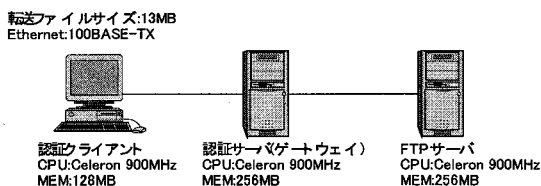


図 3 認証実験ネットワーク構成

5. 結果と考察

測定結果を表 1 に示す。認証有りで PUT した場合、認証クライアントから転送する IP パケット量に比例して認証フィールド生成の計算を行うため、通常のファイル転送と比較するとパフォーマンスが著しく低下するが、GET では受信する IP パケットの確認応答を返すのみなので低下は少ない。ネットワークに流れる IP パケットは pcap の特性により、認証フィールドを付加する前の形式も発信されてしまう。しかし認証サーバでブロックするため外部に流れることはない。

GET 時におけるパフォーマンスの低下は 17.6%

になり、一般的にクライアントにおけるデータフローは受信量が送信量より多いことを考慮すると実用の可能性があるといえるが、現状では認証速度に時間がかかり過ぎているので、パケットキャプチャを変更し、通過 IP パケットを減少させることによりパフォーマンスの向上が期待できる。

表 1 トラフィック測定結果

	認証無し	認証有り
転送速度 GET 時[MB/S]	11.27	9.28
転送速度 PUT 時[MB/S]	11.27	1.12
送受信パケット数 GET 時[個]	14472	28108
送受信パケット数 PUT 時[個]	14472	102788

6. おわりに

本稿では、情報コンセント環境における認証問題に関して、利用者認証システムの設計及びネットワークパフォーマンス測定について述べた。本利用者認証システムは IPsec[3]と似た技術を用いるが今後の課題として、クライアントが多数になった場合に認証サーバの認証処理速度にどの程度影響するかの実験を行う必要がある。また本システムは UNIX で実験されているが、汎用性を向上させるために Windows 等の OS でも稼動するようシステムを構築する。以上の課題を克服し、パフォーマンスを向上させ、更なるシステムの改善を目指す。

参考文献

- [1] 川内拓行, 安井浩之, 松山実, 徳山則秀: "IP ヘッダへの利用者認証フィールド埋め込みによる認証システム", 情報処理学会, 第 63 回全国大会, 講演論文集(3), pp. 539-540, 2001
- [2] 徳山則秀: "ネットワーク利用における認証機構の実装", 平成 12 年卒業論文, 武蔵工業大学工学部
- [3] 馬場 達也: "マスタリング IPsec", pp. 1-121, 2001 株式会社オライリー・ジャパン