零知識証明技術のコンピュータ間認証への適用

5T−2

小林 信博, 岡本 隆司, 桜井 幸一

三菱電機(株) 情報電子研究所

1 はじめに

コンピュータネットワークの発達により、ネットワークに接続されたマシン間の相互サービス利用が不可欠なものとなってきている。これに伴い、不正利用を防止する為のより安全性の高いコンピュータ間認証方式が必要とされている。しかし、従来から多用されている秘密情報をコンピュータ間で交換する認証方式では、ネットワークを盗聴された場合に秘密情報を盗まれる恐れがあった。一方、近年注目を集めている暗号方式に、秘密情報を漏らさずに秘密情報を知っていることを相手に納得させるという零知識証明技術(Zero-Knowledge Interactive Proof [Z-KIP])[1]がある。そこで、一般的なコンピュータ間通信手段の一つであるUNIXシステム[1]のtelnetコマンドを選び、零知識証明技術を認証部分に適用したZ-KIP telnetを開発した。本稿では、零知識証明技術のコンピュータ間認証への適用について、今回開発したZ-KIP telnetを基に述べる。

2 零知識証明技術

零知識証明とは、零知識対話証明 或は零知識会話型証明と呼ばれ、証明者が秘密の情報を明かすことなく、検証者と対話を行いながらその秘密を知っていることを検証者に対して証明する方法である。具体例として図1に示すように、サービス利用側である証明者をA、サービス提供側である検証者をBとし、証明者Aが持っている情報をsとすると、A固有の情報sをBに呈示することなく、"sを持っているので確かにAである"ことを何らかの情報交換により確認させることである[2]。

図1: 零知識証明技術

以下に、一実現方法として今回適用したFiat-Shamir法[3]を説明する。

まず、予め素数p、p-1以下の素数q、$N \equiv p \times q$を定めておく。証明者Aは秘密の数sを任意に選び、

$$I \equiv s^2 \ mod \ N \tag{1}$$

を計算する。Aはsを秘密に保ち、公開情報としてI, Nを検証者Bに伝送しておく。この上で、以下の情報交換を行なう。

1. Aは乱数rを選び、

$$R \equiv r^2 \ mod \ N \tag{2}$$

を計算し、Bに伝送する。

2. Bは2進数$e = 0$ or 1をランダムに選び、Aに伝送する。
3. Aはeを受信し、もし$e = 0$ならば、

$$V \equiv r \ mod \ N \tag{3}$$

をBに伝送する。もし$e = 1$ならば、

$$V \equiv (r \times s) \ mod \ N \tag{4}$$

をBに伝送する。
4. Bは$e = 0$の場合には、

$$V^2 \ mod \ N \equiv R \tag{5}$$

を検査し、$e = 1$の場合には

$$V^2 \ mod \ N \equiv (R \times I) \ mod \ N \tag{6}$$

を検査する。
5. 検査式が成立しないときは、Aでないことが確認されたので終了する。成立する時は1.〜4.までを繰り返すごとにAであることの信頼性が高くなる。

なお、2.においてBが常に$e = 1$を伝送すると仮定した場合、予めVを決定しそこからRを逆算することによってAに"なりすます"ことが可能である。従ってこれを防ぐ為に、eをランダムに選び伝送している。

3 コンピュータ間認証への適用

3.1 従来のコンピュータ間認証

従来のコンピュータ間認証では、サービスを利用するマシンAとサービスを提供するマシンBとの間でAの正当性を証明する為に、秘密情報であるパスワードをネットワークを介してAからBへ送るという方法がよく用いられていた。また、今回選んだUNIXシステムのtelnetコマンドの場合では、このパスワードがネットワーク上を暗号化されずにそのままの形で送られていた。従って、悪意を持った第三者Cが、ネットワークを盗聴しパスワードを入手することが可能であり、安全面からみて問題があった。

3.2 零知識証明を適用した認証

一方、コンピュータ間の認証に零知識証明技術を適用することにより、Aは直接パスワードを送ることなく、Bに対してパスワードを知っていることを証明することができる。まず、今回開発したZ-KIP telnetの概要を図2に示す。

ユーザーは、事前に秘密情報であるパスワードsを任意に決定する。そして、式(1)からIを算出し、I, Nを公開情報として予めデータベースに登録しておく。認証

An Application of Zero-knowledge Interactive Proof for Computer Authentication

Nobuhiro KOBAYASHI, Takashi OKAMOTO, Kouichi SAKURAI
Mitsubishi Electric Corp.

[1]UNIXオペレーティングシステムは、UNIXシステムラボラトリーズ社が開発し、ライセンスしています。

を行なう場合は、ユーザーがパスワード s を入力することによって、サービス利用側のAとサービス提供側のBの間で零知識証明の情報のやりとりが行なわれる。サービス提供側のBは、公開情報データベースから I, N を取り出し、これらとサービス利用者と交換した情報とを用いてAの認証を行なう。

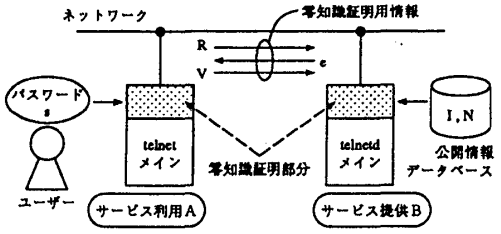

図 2: 適用例概要（ＵＮＩＸの telnet コマンド）

3.3 認証の高速化

零知識証明技術における対話式の情報交換では、1回の検査を行なう為に3回の情報交換を行なう必要がある。従って、検査を l 回繰り返すと、合計の通信回数 N は $3\times l$ 回となる。また今回の場合、検査1回に要するデータ量は合計 513 [bit] であるので、この検査を l 回繰り返すとすると、全データ量 S は、$513\times l$ [bit] となる。さて、安全性を高める為には検査回数を増やすべきであるが、これによりユーザーの操作性が低下することは避けなければならない。また、一般に同じ量の情報を送る場合、分割回数が多いほどオーバーヘッドが増加し、通信速度の低下という結果を招いてしまう。そこで、検査回数を増やしつつ認証の高速化を図る為に、データを l 回分まとめてパラレルに交換し、通信回数を減らす方法を採用した [3]。具体的には、図3の右に示すようにデータを交換する。左には比較として、3回の通信を l 回繰り返すシリアル版の情報交換を示す。

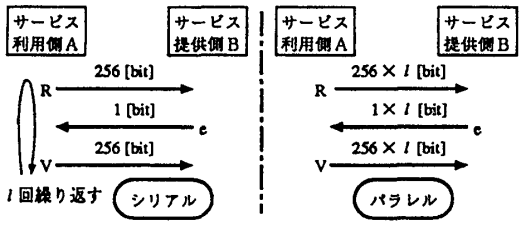

図 3: 情報交換の高速化

このように、パラレル版の情報交換を行なうことによって、検査 l 回分のデータを3回の通信によって交換できる。従って、情報交換のオーバーヘッドが減少し、認証に要する時間が短縮される。なお、パラレル版においても安全性に関しては同等である。

4 評価

4.1 安全性

今回、零知識証明技術を適用したZ-KIP telnet を開発し、直接パスワードを示す必要のないコンピュータ間の認証を実現した。これにより、従来の認証方式のように盗聴されたデータからパスワードが解読されるという危険性を排除することができた。

また、総当りによる検査の擦り抜けに対しても十分な安全性を確保することができた。1回の検査を秘密情報 s を知らない第三者が擦り抜ける確率は、手順3．でBから送られてくる e を当てることと等しいので $\frac{1}{2}$ である。一方、Z-KIP telnet では検査回数 l を 50 回に設定しているので、第三者が検査を擦り抜ける確率は $(\frac{1}{2})^{50}$ と極めて低い値になっている。更にこの検査回数を増やすことによって、安全性を高めることが容易に可能である。

4.2 通信性能

零知識証明技術をコンピュータ間認証に適用する場合に、大量の情報交換による処理速度の低下を招く恐れがあるが、今回の方式では、パラレルに情報を送ることによって認証の高速化を実現した。高速化前（シリアル版）と高速化後（パラレル版）の認証時間の比較を表1に示す。測定は、三菱電機(株)製ＥＷＳ ME-250 (CPU:68030 25[MHz], OS: ＵＮＩＸ SYSTEM V/68 Release R3V4) 2台の間で行なった。測定プログラムは、Ｃ言語とアセンブラ言語で記述し、通信には TCP/IP 通信方式を用いた。また、ネットワークには Ethernet(10[Mbps]) を使用し、誤差を除く為に同じ測定を 50 回行なった。

表 1: 通信速度の比較

	シリアル	パラレル
通信時間 [sec/50 回]	500.217	9.767
平均通信時間 [sec]	10.004	0.195

以上の結果より、情報交換をパラレル化することによって、認証に要する通信時間が大幅に短縮されていることが確認できた。

5 おわりに

より安全性の高いコンピュータ間認証を実現するため零知識証明技術に注目し、ＵＮＩＸシステムの telnet コマンドにこれを適用した Z-KIP telnet を開発した。Z-KIP telnet は、認証を行なう際にパスワードをネットワークを介して送る必要がない為、盗聴等によってパスワードを盗まれることがない。また盗聴したデータからもとのデータを算出することや、偶然によって検査を擦り抜けることも、数学的にほぼ不可能であることが証明されているので、この点についても安全である。従って、零知識証明技術を今後様々なコンピュータ間認証へ応用していくことにより、安全性の向上が期待できる。

参考文献

[1] 小山，”ゼロ知識対話証明の原理と課題”，情報処理第32巻第6号，pp643-653，(1991)

[2] 辻井，笠原，”暗号と情報セキュリティ”，昭晃堂，pp142-147，(1990)

[3] 太田，藤岡，”ゼロ知識証明の応用”，情報処理第32巻第6号，pp654-662，(1991)