5M－5

インターネットにおけるクレジット決済システム
3．クレジットカード会社用システム

川副 博、中山恭與、工藤道治

日本アイ・ビー・エム株式会社 東京基礎研究所

1. はじめに

筆者らのグループではインターネットでのクレジットカード払いのお買物システムを開発した。このシステムのクレジットカード会社システムについて報告する。

2. インターネット

インターネットで使われるプロトコルIP, TCPはデータの暗号化を行わない。通信経路上のネットワークを観測できる計算機はパケットの中身を読むことができる(図 1）。この覗き見は通信経路のネットワーク上の計算機でしかできない。従って、インターネット・バックボーン上の計算機の管理を厳格にしておけば覗き見は現実的でないと感じられるかもしれない。しかし、この覗き見を使った事件が実際に発生した[1]。

3. お買い物

日常的で誰もが行っている「お買物」は次の４つのステップから成り立っている。

1. 望みの物を探す。
2. お金を払う。
3. 物を受け取る。
4. アフターサービスを受ける。

これらのステップを介して行う方法をパソコン通信の場合とインターネットとの場合とについて表１に示す。インターネットの場合、買い手と売り手とは別の国の者であることがあるので、支払いは国際的に通用するものでなければならなく、クレジットカード払いが適している。クレジットカード払いの通信販売（電話注文、郵便注文）では有効なクレジットカードの番号を伝えれば買物ができる。

インターネットでクレジットカード番号を送ると覗き見され、悪用される可能性がある。

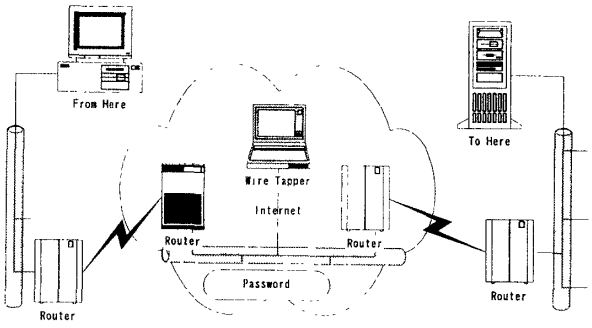

図 1：Packets on Internet are monitable.

4. クレジットカード払い専用プロトコル

本システムではクレジットカード払い専用プロトコルとしてiKP[2]を使った。このプロトコルでは買い手、売り手、クレジットカード会社の三者がそれぞれ公開鍵暗号システムの鍵対、公開鍵証明書を持つ。買い手のクレジットカード番号はクレジット

表 1．Shopping on BBS and Internet

	ＢＢＳ	インターネット
探す	メニュー	WWW
払う	クレジットカード、代金引き換え、現金書留、郵便・銀行振り込み	クレジットカード
受け取る	宅配便	宅配便
アフターサービス	電子メール	電子メール WWW

Payment By Credit Card on the Internet :
3. A System for Credit Card Company
Hiroshi KAWAZOE
Tokyo Research Laboratory, IBM Japan
Shimotsuruma 1623-14, Yamato, 242, JAPAN

カード会社の公開鍵を使って、買い手が暗号化して送る。 後の（注文した、しないなどの）紛争を避けるために、買い手、売り手はそれぞれ注文内容のハッシュに電子署名したものをクレジットカード会社に送る。 クレジットカード会社は買い手、売り手の署名を確認し、次に、両者が注文内容で合意していることを確認する。 その後、暗号化されて送られてきた買い手のクレジットカード番号を平文化する。与信確認、売り上げ処理を行い、その結果に電子署名をして売り手にかえす。

5. 問題点

クレジットカード番号はネットワーク上での覗き見、売り手の不正使用を防止するためにクレジットカード会社の公開鍵で暗号化する。悪意のある買い手が、他人のクレジットカード番号を使い、買い手本人の署名鍵で注文のハッシュに署名する。すると、買い手本人の署名鍵を使っているので、クレジットカード会社での買い手の署名の検査、公開鍵証明書の検査は通る。与信確認、売り上げ処理は他人のクレジットカードに対して行われる。 つまり、他人のクレジットカードで買物ができてしまう。本システムではクレジットカードの番号、署名鍵などを IC カードに格納しているので、このようなことは行い難い。 しかし、IC カードを使っていないシステムでは簡単に行える。本システムでも予防処置としてこの問題に対する対策を講じた。

6. 解決策

この問題はクレジットカード番号と買い手の公開鍵証明書との対応を行っていないので発生する。これらの対応をクレジットカード会社で行えばよい。買い手の公開鍵証明書は買物毎に買い手から売り手を経由してクレジットカード会社に送られる。公開鍵証明書のシリアル番号とクレジットカードとの対応表をクレジットカード会社で持つと、表の大きさはクレジットカード会社の発行済みクレジットカードの枚数のオーダーとなる。 (実験の間は１０００程度のある程度の数字で収まるだろうが、本番運用時にはこのオーダーとなる。）この方法は実際的ではない。

公開鍵証明書にクレジットカードの番号を入れればクレジットカード会社で公開鍵証明書と暗号化されて送られて来たクレジットカード番号とを照合できる。しかし、この方法では、公開鍵証明書内のクレジットカード番号を覗き見されたり、売り手により不正使用される可能性がある。

本システムでは買い手の公開鍵証明書にクレジットカード番号のハッシュ値をいれておくことにした。クレジットカード会社では暗号化されて送られてきたクレジットカード番号を復号し、ハッシュし、その値と送られてきた買い手の公開鍵証明書内のクレジットカード番号のハッシュ値とを比較する。

クレジットカードの番号は１０進１６桁程度であり、そのうち、４桁はクレジットカード会社固有の値になる。 従って10^{12}の総当たりを行うとハッシュ値が公開鍵証明書の値となるクレジットカードの番号が見つかる。本システムはクレジットカードの番号にクレジットカード会社、公開鍵証明書発行者だけが知る文字列を付け加えてハッシュすることにより、この総当たりによるクレジットカード番号の発見を避けた。

参考文献

[1] “ca-94:01:on going network monitoring attacks.”, file://ftp.cert.org/pub/cert_advisories/CA-94:01.ongoing.network.monitoring.attacks.

[2] M. Bellare, J.A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Sterner, G. Tsudik, and M. Waidner, "iKP - a family of secure electronic payment protocols," Workshop on Electronic Commerce, pp. 1-21, USENIX, 1995