6.915 Computer and Network Security	Fall Term, 1995

Lecture 16 : November 2, 1995

Lecturer: Ron Rivest *Scribe: Joe Bank*

1 Outline

The topic covered today was payment schemes over the Internet. The lecture first discussed the basics of electronic payment schemes, and then focused on the a particular credit card payment scheme proposed in the paper *iKP - A Family of Secure Electronic Payment Protocols*, which was handed out in class as Handout 27.

2 Payment Schemes

There are two major categories of payment schemes over the Internet:

- **Macro Payments.** These are for payments that are on the order of dollars. Examples of macro payment schemes are Internet use of credit cards, and electronic cash proposals. These schemes can afford to use fairly computational cryptography.
- **Micro Payments.** These are for payments that are on the order of fractions of cents. Micro payment schemes are intended to be used for activities such as charging for each access of a web page. Since each transaction is processing so little money, high security is not as much of an issue, and highly computational schemes are less desirable.

This weeks lecture discusses a particular macro payment scheme. A lecture on micro payment schemes was promised for next week.

It is desirable to model macro payment schemes on the Internet on current real world schemes. This helps the scheme gain acceptance and helps development since current models are well established. The three main "Real World" payment schemes in use are checks, credit cards and cash. Currently proposed electronic schemes have similarities to these three real world counterparts.

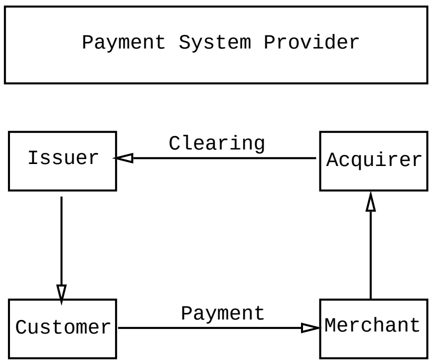
3 *i*KP

*i*KP (i-Key-Protocol) is actually a family of protocols (1KP, 2KP, and 3KP) designed to allow electronic payment over the internet using credit cards. The *i*KP protocol is a public-key based scheme. The variable i in the scheme indicates the number of parties who have keys.

It is an important to note that *i*KP is intended to model the current credit card-based transactions systems. Thus, the proposal does not attempt to address issues such as anonymity.

3.1 Parties Involved

The different parties involved in the payment system are shown in Figure 1.



The main parties involved directly in the *i*KP protocol are the Customer, the Merchant and the Acquirer. The basic model is that the Customer and Merchant agree on a transaction, then payment information is given from the Customer to the Merchant, who then passes it on to the Acquirer. The Acquirer sends back a verification to the Merchant, who can then complete the transaction. From the *i*KP protocol perspective, the process of the Acquirer verifying the Customers credit with the Issuer and transfering the money is taken as a black box.

3.2 Security Requirements

Each of the parties involved has a number of potential security requirements for an electronic payment scheme.

- **Issuer/Acquirer**
  - Proof that the transaction was authorized by the Customer.
  - Proof that the transaction was authorized by the Merchant.
- **Merchant**
  - Proof that the transaction was authorized by the Acquirer.
  - Proof that the transaction was authorized by the Customer. This seemed like a slightly strange requirement since merchants are not likely to mind receiving unauthorized payments. On the other hand, it is very bad customer relations, and if the amount is large a customer is very likely to attempt to dispute the transaction.
- **Customer**
  - Unauthorized payment should be impossible.
  - Proof that the transaction was authorized by the Acquirer.
  - Proof that the Merchant is accredited with the Acquirer. This requirement is an attempt to give some evidence to the customer of the trustworthiness of a merchant.
  - Receipt from Merchant.
  - *Privacy and Anonymity* As was mentioned earlier, because iKP attempts to model credit card transactions, this is not as much a requirement as a desirable trait.

3.3 Protocol

The basic scenario (shown in Figure 2), is the same for each of the three iKP protocols.

Throughout the protocol discussion, the following terminology is used:

- $\mathcal{H}$: a strong collision resistant one-way hash function.

- E_i: encryption using the public key of party i.
- S_i: signing using the private key of party i.
- $Cert_i$ certification of the public key of party i.
- Offer: offer description, amount, currency, date, ID of merchant
- Order: order description, amount, currency, date, ID of merchant, delivery address
- Slip: amount, currency, date, ID of merchant, credit card number, expiration date, PIN, $\mathcal{H}$(Order).
- Auth: approved/rejected,$\mathcal{H}$(amount, currency, date, ID of merchant), $\mathcal{H}$(Order).

1KP

1KP is the most basic of the protocols. In 1KP, only the Acquirer (A) has a public key pair. The transactions in the protocol are as follows:

1. C $\longleftarrow$ M : Offer, $Cert_A$
2. C $\longrightarrow$ M : E_A(Slip), Order
3. Calculates $\mathcal{H}$(Order)

   M $\longrightarrow$ A: E_A(Slip), $\mathcal{H}$(Order)
4. Verifies steps, forwards data to payment system.

   M $\longleftarrow$ A: S_A(Auth, E_A(SLIP))
5. C $\longleftarrow$ M : S_A(Auth, E_A(SLIP))
6. C $\longleftarrow$ M : service, goods

There are a few interesting points to note about the protocol. First, since the Acquirer only sees a hash of the Order, the Acquirer does not see the offer description, providing for some privacy for the Customer. Additionally, both the Customer and Acquirer have no assurance of the identity of the Merchant in this scheme. Finally, the Customer is only identified by the correctness of the credit card number and the PIN.

It should be noted that 1KP has the advantage that it can be implemented fairly easily since only the Acquirer needs to have a public key.

2KP

2KP attempts to rectify the problem of assuring the identity of the Merchant. This is achieved by adding having the Merchant also have a public key pair. The modifications to the protocol are to have the Merchant send both the Customer and Acquirer a certificate, to have the Merchant sign messages 3, and to have the Merchant append the contents of message 3 to message 5. The entire protocol is now as follows:

1. C $\longleftarrow$ M : Offer, $Cert_A$, $Cert_M$
2. C $\longrightarrow$ M : E_A(Slip), Order
3. Calculates $\mathcal{H}$(Order)

   M $\longrightarrow$ A: $S_M(E_A(\text{Slip}), \mathcal{H}(\text{Order}))$, $Cert_M$
4. Verifies steps, forwards data to payment system.

   M $\longleftarrow$ A: $S_A(\text{Auth}, E_A(\text{SLIP}))$
5. C $\longleftarrow$ M : $S_M(E_A(\text{Slip}), \mathcal{H}(\text{Order}))$, $S_A(\text{Auth}, E_A(\text{SLIP}))$
6. C $\longleftarrow$ M : service, goods

It was noted in class that in the first message it would be preferable to have the Merchant sign the Offer. This step would add assurances to the Customer that the Offer is a valid one. It is also noted that instead of appending message 3 to message 5, the Merchant could digitally sign message 5, but that this would add an extra signature to the cost of the scheme.

3KP

In 3KP the Customer also has a public key pair. The protocol is modified to have the Customer send a Certificate to the Merchant (which is forwarded to the Acquirer), and to have the Customer sign message 2 (actually, message 2 is modified to contain the hash of the order instead of the order so that the Merchant can forward it). The entire protocol is now as follows:

1. C $\longleftarrow$ M : Offer, $Cert_A$, $Cert_M$
2. C $\longrightarrow$ M : $Cert_C$, $S_C(E_A(\text{Slip}), \mathcal{H}(\text{Order}))$
3. Calculates $\mathcal{H}(\text{Order})$

   M $\longrightarrow$ A: $S_M(S_C(E_A(\text{Slip}), \mathcal{H}(\text{Order})))$, $Cert_M$, $Cert_C$
4. Verifies steps, forwards data to payment system.

   M $\longleftarrow$ A: $S_A(\text{Auth}, E_A(\text{SLIP}))$
5. C $\longleftarrow$ M : $S_M(S_C(E_A(\text{Slip}), \mathcal{H}(\text{Order})))$, $S_A(\text{Auth}, E_A(\text{SLIP}))$
6. C $\longleftarrow$ M : service, goods

Note that in this scheme, every participant has a public key, so a full fledged certificate distribution must be implemented.

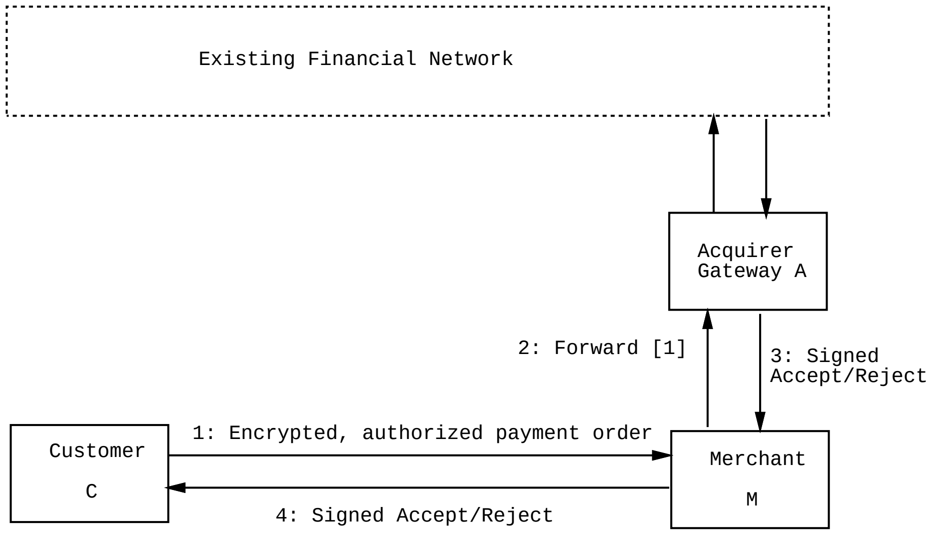


Figure 2: Scenario of iKP