Design, Implementation and Deployment of the iKP Secure Electronic Payment System

Mihir Bellare, Juan A. Garay et al.

" . . .At this day and age it is hardly necessary to justify , or stress the importance of electronic commerce… Indeed, the appeal of electronic commerce without electronic payment is limited. Moreover, *insecure* electronic payment methods are more likely to impede, than to promote, electronic commerce… "

Reviewer Qiang Dong

Outline

- Introduction
- Overview of e-commerce and the i-key protocol (iKP)
- Implementation of iKP
- Conclusion
- Questions

Introduction

- **Many secure electronic payment systems are being developed, including**
  - SEPP (Secure Electronic Payment Protocol) by IBM and Europay
  - iKP (I-Key-Protocol) by IBM later incorporated into SEPP
  - STT (Secure Transaction Technology) by Microsoft and Visa
  - SET (Secure Electronic Payment) by Visa/MasterCard is the current secure payment system standard
- **All e-payment systems depend on algorithms for encryption and authentication**
  - Most systems use RSA (Rivest-Shamir-Adleman)
  - Secret key, Public Key and Hash Function

Overview of iKP

- **What is iKP?**
  - A secure electronic payment protocol with i keys (i = 1, 2, 3)
  - Developed in 1995 at IBM Research Lab
  - It implements credit-card based transaction
  - iKP can be implemented by Hardware or Software
- **Why it is important?**
  - Security : Based on Public Key Cryptography
  - Simplicity : Based on existing financial network
  - Flexibility : Easy to extend to other account-based payment models
  - Efficiency : Lower the computational cost by using Hash function
  - SET still retain many of the iKP-esque features

Overview of E-Commerce

Payment Model

- **Parties in general credit-card payment system**
  - Buyer
  - Seller
  - Acquirer
  - Issuer
- **Parties in iKP**
  - Buyer
  - Seller
  - Acquirer

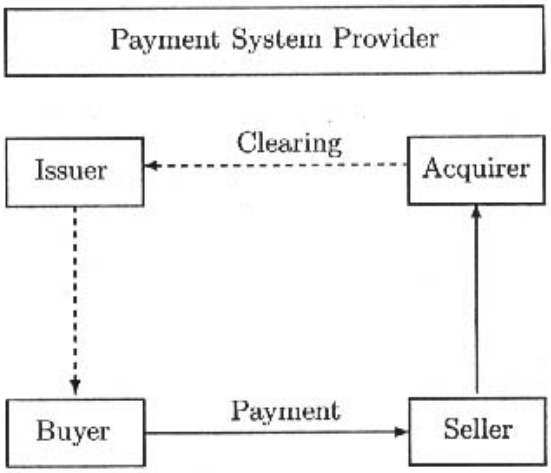

Fig. 1
GENERIC MODEL OF A PAYMENT SYSTEM

Overview of iKP Family

- 1KP
  - Acquirer possess a public key-pair. This only need a minimal PKI to provide certificates for a small number of acquirers (PKI only cover the Acquirer)
  - Buyers are authenticated on the basis of their credit-card numbers and optional secret PINs
  - 1KP doesn't offer non-repudiation for messages sent by buyers and Sellers. Why?

Overview of iKP Family

- 2KP
  - In addition to the Acquirer, the Seller holds public-key pair and certificates, thus achieving non-repudiation for massages originated by Sellers
  - By checking the certificate, Buyers know they are dealing with the *bona fide* Sellers
  - 2KP requires that PKI cover Acquirers and Sellers

Overview of iKP Family

- 3KP
  - Further more, Buyers hold public-key-pair and certificates, thus achieving non-repudiation for all parties involved in 3KP
  - Payment authenticated by combination of credit-card number, optional PIN and digital signature of Buyer
  - 3KP requires that PKI cover all the parties involved

Implementation Of iKP

Security Requirements

REQUIREMENTS/PROTOCOLS	1KP	2KP	3KP
Issuer/Acquirer			
A1. Proof of Transaction Authorization by Buyer	√	√	√√
A2. Proof of Transaction Authorization by Seller		√√	√√
Seller			
S1. Proof of Transaction Authorization by Acquirer	√√	√√	√√
S2. Proof of Transaction Authorization by Buyer			√√
Buyer			
B1. Unauthorized Payment is Impossible	√	√	√√
B2. Proof of Transaction Authorization by Acquirer	√√	√√	√√
B3. Certification and Authentication of Seller		√√	√√
B4. Receipt from Seller		√√	√√

Implementation Of iKP

It's Not Just a Paper Design!

- 1996: Spain Europay and IBM built a small scale system for trial, based on Zip-3KP.
- 1996: InterPay Nederland and Dutch banks offer e-commerce to 80 on-line merchants and 17000 users based on Zip-3KP.
- 1997: Japan EMP (Electronic Market Place) offers e-commerce to 5 on-line merchants and 2000 users.

Conclusion

- iKP makes an important step towards the current standard of secure payment system-SET. It had several operational prototypes which works well
- This paper is well written and not hard to understand. For a beginner in this field it is a good tutorial because of the simplicity and modularity of iKP

Questions

Why these protocols like iKP and SET were implemented by software, not hardware?

Thank You All