NetBill Security and Transaction Protocol
Cox Tygar and Sirbu

Shawn Butler

This paper describes and electronic commerce system that is designed to support low priced electronic transactions between merchants and buyers. NetBill attempts to ensure that: 1) the customer does not pay if he does not receive the merchandise, 2) the buyer can remain anonymous if desired, and 3) the merchant can verify the credentials of the buyer if necessary. The bulk of the paper describes a protocol used among the participants to achieve various types of transactions.

The NetBill system consists of three components: the buyer, the merchant, and NetBill server. The entities communicate using the NetBill protocols which can be divided into 3 phases: price request, goods delivery, and payment phases.

The price request phase is conducted between the buyer and the merchant. The customer can send the merchant a price request using a pseudonym if he wishes to remain anonymous. The buyer can also present any credentials to the merchant. At this time the buyer generates a Transaction ID (TID)that uniquely identifies this interchange. The merchant responds with a price quote and the TID. This phase can be repeated as many times as necessary. Neither party is obligated to purchase of sell any items.

In the goods delivery phase the buyer initiates the purchase of the goods by sending the TID to the merchant. The merchant responds by sending the encrypted goods and a checksum to the buyer. The merchant also includes a Electronic Payment Order ID (EPOID). The EPOID uniquely identifies the transaction to NetBill. The EPOID is globally unique to prevent replay attacks.

The buyer submits to the merchant an Electronic Payment Order as the first step in the Payment phase. The EPO is in two parts, encrypted and plain text. The plain text reflects some basic information about the transaction such as the customer's identity (or pseudonym), the price, merchant's identity, EPOID, and some cryptographic checksums of the Product Request Data and customer's account number. The encrypted portion of the EPO is all the information that NetBill needs to identify the buyer,the transaction, and the authorization from the buyer. The merchant endorses the EPO, adds the decryption key for the goods and forwards it to NetBill. Once NetBill verifies the information it sends a receipt to the merchant with the encryption key. The merchant then forwards the receipt on to the buyer. If the merchant doesn't forward the receipt the customer can ask NetBill directly for the receipt, thereby getting the key.

A notable feature of NetBill is that it attempts to use different forms of encryption at different points in the protocol. NetBill uses both DSA and RSA for performance reasons. Another notable feature of NetBill is that it is able to handle zero-priced good transactions. This enables customers to buy subscriptions or special priced merchant deals. NetBill supports Certified Deliveries using NetBill as an intermediary or certified deliveries without the NetBill Server. NetBill also supports verified and unverified delivery of goods.

Customer complaints can be easily handled under NetBill because the NetBill server can resolve most of the transactional disputes, such as whether the buyer paid and false charges. Other types of disputes must be handled through an arbitrator.