SET Cardholder Registration: The Secrecy Proofs

(Extended Abstract)

Lawrence C. Paulson

Computer Laboratory, Univ. of Cambridge, Cambridge, England
lcp@cl.cam.ac.uk

1 Introduction

Security protocols aim to protect the honest users of a network from the dishonest ones. Asymmetric (public key) cryptography is valuable, though it is normally used in conjunction with symmetric cryptography, where two users share a secret key, Asymmetric cryptography is typically used to securely exchange symmetric keys, which carry the bulk of the traffic. This mode of operation is faster than using expensive public-key encryption exclusively. It is also more secure, since the symmetric keys can be changed frequently. However, the protocol used to set up of this communication must be designed with care. For example, each message typically includes a nonce: a freshly-generated number that the other party must include in his response; the first party then knows that the response was not an old message replayed by an intruder. Many flaws have been discovered in security protocols [5].

Security protocol verification technologies have progressed in recent years. A variety of tools are available for analyzing protocols. Model checking is excellent for debugging a protocol, finding attacks in seconds [6,7]. Theorem proving is valuable too: it can analyze protocols in more detail and handles the protocols that are too big for model checking. Subgoals presented to the user suggest possible failure modes and give insights into how the protocol operates.

Past work on protocol verification has focused on protocols arising from the academic community. Only seldom have deployed protocols been investigated, such as Kerberos [3], SSL [8] and SSL’s successor, TLS [12]. Past work has largely focused on key exchange protocols. Such protocols allow two participants (invariably called Alice and Bob) to agree on a session key: a short-term symmetric key. In this paper, I would like to describe a project, joint with Bella, Massacci and Tramontano, to verify a very large commercial protocol: SET, or Secure Electronic Transactions [15].

2 The SET Protocol

People normally pay for goods purchased over the Internet using a credit card. They give their card number to the merchant, who claims the cost of the goods
against it. To prevent eavesdroppers from stealing the card number, the transaction is encrypted using the SSL protocol. This arrangement requires the customer and merchant to trust each other: an undesirable requirement even in face-to-face transactions, and across the Internet it admits unacceptable risks.

- The cardholder is protected from eavesdroppers but not from the merchant himself. Some merchants are dishonest: pornographers have charged more than the advertised price, expecting their customers to be too embarrassed to complain. Some merchants are incompetent: a million credit card numbers have recently been stolen from Internet sites whose managers had not applied patches (available free from Microsoft) to fix security holes [9].
- The merchant has no protection against dishonest customers who supply an invalid credit card number or who claim a refund from their bank without cause. Contrary to popular belief, it is not the cardholder but the merchant who has the most to lose from fraud. Legislation in most countries protects the consumer.

The SET protocol aims to reduce fraud by introducing a preliminary registration phase. Both cardholders and merchants must register with a certificate authority (CA) before they can engage in transactions. The cardholder thereby obtains electronic credentials to prove that he is trustworthy. The merchant similarly registers and obtains credentials. These credentials do not contain sensitive details such as credit card numbers. Later, when the customer wants to make purchases, he and the merchant exchange their credentials. If both parties are satisfied then they can proceed with the transaction. Credentials must be renewed every few years, and presumably are not issued to known fraudsters.

SET comprises 15 subprotocols, or transactions, in all. Some observers, noting its extreme complexity, predict that it will never be deployed. However, the recent large rise in credit card fraud [1] suggests that current arrangements are unsustainable. SET or a derivative protocol may well be deployed in the next several years. To a researcher, SET has a further attraction: it makes heavy use of primitives such as digital envelopes that protocol verifiers have not examined before now.

3 Cardholder Registration

As described above, each cardholder must register before he is allowed to make purchases. He proves his identity by supplying personal information previously shared with his issuing bank. He chooses a private key, which he will use later to sign orders for goods, and registers the corresponding public key, which merchants can use to verify his signature. In keeping with normal practice, SET requires each participant to have separate key pairs for signature and encryption.

Cardholder registration comprises six messages:

1. The cardholder contacts the CA to request registration.