Verifying the SET Registration Protocols

Giampaolo Bella
Computer Laboratory, University of Cambridge
15 JJ Thomson Avenue, Cambridge CB3 0FD (UK)
Email: giampaolo.bella@cl.cam.ac.uk
Dip. di Matematica e Informatica, Università di Catania
Viale A. Doria 6, I-95125 Catania (Italy)
Email: giamp@dmi.unict.it

Fabio Massacci (IEEE CS Member)
Dip. di Informatica e Telecomunicazioni, Università di Trento
via Sommarive 14, 38050 Povo (Trento) - Italy Email: massacci@ing.unitn.it

Lawrence C. Paulson
Computer Laboratory, University of Cambridge
15 JJ Thomson Avenue, Cambridge CB3 0FD (UK)
Email: lcp@cl.cam.ac.uk

***Abstract*—SET (Secure Electronic Transaction) is an immense e-commerce protocol designed to improve the security of credit card purchases.**

In this paper we focus on the initial bootstrapping phases of SET, whose objective is the registration of cardholders and merchants with a SET certificate authority. The aim of registration is twofold: getting the approval of the cardholder's or merchant's bank, and replacing traditional credit card numbers with electronic credentials that cardholders can present to the merchant, so that their privacy is protected.

These registration sub-protocols present a number of challenges to current formal verification methods. First, they do not assume that each agent knows the public keys of the other agents. Key distribution is one of the protocols' tasks. Second, SET uses complex encryption primitives (digital envelopes) which introduce dependency chains: the loss of one secret key can lead to potentially unlimited losses.

Building upon our previous work, we have been able to model and formally verify SET's registration with the inductive method in Isabelle/HOL. We have solved its challenges with very general techniques.

IEEE Keywords: Business communication, Communication system security, Computer network security, Protocols, Software verification and validation, Theorem proving

F. Massacci was supported by CNR and MURST grants. The work at Cambridge was funded by the EPSRC grant GR/R01156/R01 *Verifying Electronic Commerce Protocols*.

I. Introduction

Cryptographic protocols allow people to communicate securely across an open network, even in the presence of hostile or compromised agents. Such protocols are hard to design and numerous researchers have developed ways of finding errors automatically [10], [13] or proving protocols correct [6], [14]. (Many additional references could be given.) Here we report our verification of the registration protocols of SET, a giant protocol for electronic commerce, proposed by Visa and MasterCard as an industry standard [11].

The idea behind the registration protocols of SET is that only registered cardholders and merchants can engage in transactions. A registered cardholder has been cleared by a bank and has a digital certificate to prove it. Subsequently, he can show his certificates rather than his credit card number to an equally certified merchant. The merchant will rest assured that there is a credit card behind the private key signing a bill, and the cardholder will be sure that incompetent or dishonest merchants will not publish his credit card details on the internet.

At this level of abstraction, the registration pro-

tocols look trivial: they just distribute public key certificates. However, past experience shows that simplifying a protocol's encryption mechanisms can hide major errors [16]. SET presents two major challenges to formal methods:

1) it involves several levels of encryption, using many combinations of symmetric cryptography, asymmetric cryptography and hashing;
2) it does not assume that each agent has his own private key (so that the only problem is the distribution of the public keys), but allows cardholders and merchants to invent asymmetric keys at will.

The first challenge comes from SET's use of RSA *digital envelopes*. One part of a digital envelope is the main body of the message, encrypted using a fresh symmetric key. The other part contains that key and is encrypted with the recipient's public encryption key. The two parts may have some common data, possibly hashed, in order to confirm that they are tied together. This combination of symmetric and asymmetric encryption ought to be more efficient than using asymmetric crypto alone and more secure than using symmetric encryption alone. However, it makes a protocol much harder to analyze. For instance, assuming that long-term asymmetric keys are secure, as all verification techniques do, will not guarantee us that the data in a digital envelope is safe: the key may be lost.

Furthermore, digital envelopes can be used to send keys, which are used to package new envelopes, ad infinitum. A complicated case is in the last message exchange of cardholder registration, where a digital envelope conveys a symmetric key that the recipient uses to encrypt the reply. This creates dependency chains such that the loss of a secret key can lead to a cascade of losses. Nothing like this can be found in the customary benchmark for protocol verification methods, the Clark-Jacobs library [5]. Therefore, many protocol verification formalisms [8] assume that to prove secrecy it is enough to show that the long-term keys encrypting the short-term keys are safe. Past protocols were too simple to reveal this point.

The second challenging aspect of the SET protocols is the possibility for cardholders and merchants to invent public/private key pairs at will for their electronic credentials. The difference with session key and key agreement protocols is minimal: asymmetric keys join nonces and session keys among the objects that can be invented during a protocol run.

We do not make the usual assumption that each agent knows the other agents' public keys.

However, all current verification approaches functionally associate asymmetric and other long-term keys to agents. This modelling choice substantially eliminates asymmetric keys from the hard part of the modelling: namely reasoning about what an agent can encrypt and decrypt and the introduction of fresh values. Once asymmetric keys are fixed from the outset, and at most are unknown to the intruder, reasoning about asymmetric encryption is substantially reduced to an equality check between the agent holding the message and the agent associated to the key. In model checking, these modelling choices have further advantages: the introduction of fresh values can be limited to nonces and symmetric keys, thus cutting the explosion of the state space.

We have not only verified these protocols but found what appears to be a general method for treating such protocol mechanisms.

This paper presents an introduction to the SET registration protocols (§II). Next, the formal model of the registration protocols is presented (§III). The main secrecy proofs for cardholder registration and presented (§IV). A final section discusses related work and presents conclusions (§V).

II. The SET Registration Protocols

People normally pay for goods purchased over the Internet by giving the merchant their credit card details. To prevent eavesdroppers from stealing the card number, the message undergoes a session of the SSL protocol. This arrangement requires the cardholder and merchant to trust each other. That requirement is undesirable 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, some are incompetent at protecting sensitive information.
- The merchant has no protection against dishonest cardholders who supply an invalid credit card number or who claim a refund from their bank without cause. Contrary to popular belief, it is the merchant who has the most to lose from fraud. Legislation in most countries protects the cardholder.

As stated in the Introduction, SET aims to reduce fraud by introducing a preliminary registration process. 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. Later, when the cardholder wants to make purchases, he and the merchant exchange their credentials. If both parties are satisfied then they can proceed. SET includes separate subprotocols (called *transactions*) for cardholder and merchant registration.

When assessing the goals of this protocol it is important to note that SET is supposed to run within the web of trust of the current credit card infrastructure.

Customers do trust accredited VISA or MasterCard merchants when doing transactions in the physical worlds: when paying at the restaurant the customer just hands the credit card to the waiter and wait for him to return with a plausible looking receipt to sign. For what he knows, the mafia owned restaurant may be cloning his card. Yet, he is confident because outside the protocol there is a procedure to deal with fraudsters. The same is true for the merchant.

On the electronic world customers have no way to see the placard "VISA" on the restaurant window and merchants have no way to see the plastic card with the logo and the hologram on it.

The protocol only attempts to recreate this web of trust that gives confidence against misbehavior. In other words: in the Internet you can't see that the agent at the other side of a TCP/IP connection has a valid credit card and can't see the signature on the card. The SET protocol assures the merchant that the customer has a valid credit card with a corresponding signature. At the time of purchase, by looking at the credential and the signature on the transaction, the merchant can stay assured that he'll be paid. Dually, the customer is assured by SET that the merchant has signed the transaction.

Confidentiality of credit card data avoids potential problems due to penetration of merchant sites rather than willing misbehavior.

A. The Registration Phase

We focus first on *cardholder registration* (Figure 1), which is the more complicated of the two. The cardholder proves his identity by giving the CA 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. The cardholder receives a certificate, signed by the CA, that associates the public key to his identity. Notice that the protocol does not assume that the key submitted by the cardholder is unique, nor that is fresh. So, the usual assumption that the cardholder registers *his* key should be replaced by the more appropriate that the cardholder registers *some* key.

The protocol is complicated because it has many objectives. It must certify a signature key and associate it with the credit card number, while keeping the latter secret. In this way, the merchant can be assured that an order signed by a key certified by Visa's CA is matched by the corresponding credit card issued by Visa, even if he does not see the credit card number.

However, it has *not* the objective to provide authentication to the various parties as usually intended in the protocol verification literature (see Lowe [9] for some possible definitions). There is no problem here if the certification authority receives the same request more than once, or if there is a mismatch between the number of runs of the merchant and the certification authority, and so on. Such possibilities are foreseen in the specification which assumes that unreliable software or communication crashes may occur at any time. As long as an intruder has no way to trick a certification authority to associate a wrong key to a customer's credit card or to expose the credit card details the protocol has achieved its security goals.

Cardholder registration consists of six messages. We have abbreviated some of the SET terminology, for instance Chall_C has become NC1. Notice that SET requires each CA to have separate key pairs for signature and encryption.

a) Initiate Request: The cardholder sends his name to the CA, with a freshness challenge (NC1).

$$1.\ C \rightarrow \mathit{CA} : C, \mathrm{NC1}$$

b) Initiate Response: The CA responds to the challenge and returns its public key certificates, which are signed by the Root Certificate Authority. The cardholder needs the CA's public keys for the various SET protocols.

$$2.\ \mathit{CA} \rightarrow C : \mathsf{Sign}_{\mathit{CA}}(C, \mathrm{NC1}),\ \mathsf{Cert}_{\mathsf{RCA}}(\mathsf{pubEK}\,\mathit{CA}),\ \mathsf{Cert}_{\mathsf{RCA}}(\mathsf{pubSK}\,\mathit{CA})$$

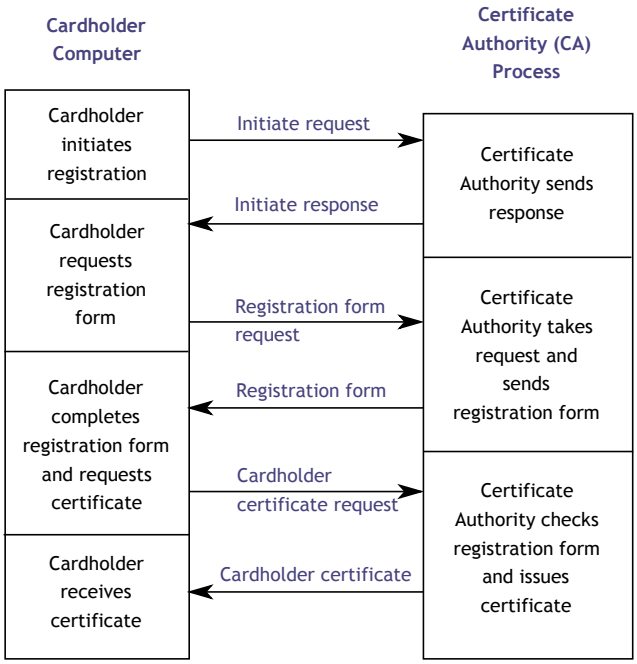

Fig. 1. Cardholder Registration

c) Registration Form Request: The cardholder requests a registration form. In this message, he submits his credit card number to the CA. SET calls this the **PAN**, for Principal Account Number. This message is our first example of a digital envelope: some data is encrypted using the key KC1, which is itself encrypted using the CA's public key.

$$3.\ C \rightarrow CA : \mathsf{Crypt}_{\mathrm{KC1}}(C,\ \mathrm{NC2},\ \mathsf{Hash}\,\mathrm{PAN}),\\ \mathsf{Crypt}_{\mathsf{pubEK}\,CA}(\mathrm{KC1}, \mathrm{PAN}, \mathsf{Hash}(C, \mathrm{NC2}))$$

d) Registration Form: The CA uses the credit card number to determine the cardholder's issuing bank and returns an appropriate registration form. SET does not specify the details of such forms, which we therefore omit from the formalization. The CA again sends its public key certificates.

$$4.\ CA \rightarrow C : \mathsf{Sign}_{CA}(C,\ \mathrm{NC2},\ \mathrm{NCA}),\\ \mathsf{Cert}_{\mathsf{RCA}}(\mathsf{pubEK}\,CA),\\ \mathsf{Cert}_{\mathsf{RCA}}(\mathsf{pubSK}\,CA)$$

e) Cardholder Certificate Request: The cardholder chooses an asymmetric signature key pair. He gives the CA the public key, $\mathsf{pubSK}\,C$, and the completed registration form. He also encloses CardSecret, a random number that must be kept secure permanently. This message is another digital envelope, using the key KC3. Another key, KC2, is sent to the CA to use for encrypting the response. The proliferation of keys complicates reasoning about this protocol.

$$5.\ C \rightarrow CA : \mathsf{Crypt}_{\mathrm{KC3}}(m,\ S),\\ \mathsf{Crypt}_{\mathsf{pubEK}\,CA}(\mathrm{KC3}, \mathrm{PAN}, \mathrm{CardSecret})$$
$$\text{where } m = C,\ \mathrm{NC3},\ \mathrm{KC2},\ \mathsf{pubSK}\,C$$
$$\text{and } S = \mathsf{Crypt}_{\mathsf{priSK}\,C}(\mathsf{Hash}(m, \mathrm{PAN}, \mathrm{CardSecret}))$$

f) Cardholder Certificate: The bank checks the various details and, if satisfied, authorises the CA to complete the registration. The CA signs a certificate that includes the cardholder's public signature key and the cryptographic hash of PANSecret: a secret number known to the cardholder. PANSecret is the exclusive-OR of the CardSecret (chosen by the cardholder) and NonceCCA (chosen by the CA). The cardholder will use the PANSecret to prove his identity when making purchases.

$$6.\ CA \rightarrow C : \mathsf{Crypt}_{\mathrm{KC2}}\\ (\mathsf{Sign}\,CA\,(C, \mathrm{NC3}, CA, \mathrm{NonceCCA}),\\ \mathsf{Cert}_{CA}(\mathsf{pubSK}\,C),\\ \mathsf{Cert}_{\mathsf{RCA}}(\mathsf{pubSK}\,CA)))$$

The *merchant registration* protocol (Figure 2) is simpler. No credit card number is involved. The CA determines the appropriate registration form merely on the basis of the merchant's name[1]. This eliminates one message exchange: there is no registration form request message. The merchant chooses two private keys, for signature and encryption, and registers the corresponding public keys (one at a time). The main goal of this protocol is to provide the merchant with certificates, signed by the CA, that associate the public keys to the merchant's identity. Here are the four messages in more detail.

g) Initiate Request: The merchant sends his name to the CA, with a freshness challenge (NM1).

$$1.\ M \rightarrow CA : M, \mathrm{NM1}$$

h) Registration Form: The CA determines the merchant's bank (known as the acquirer) and returns

[1]Observe that there are many more cardholders than merchants and that becoming an accredited merchant costs money and time, so that a name search is feasible. As for privacy, the name of a merchant and his accepted credit cards are public and indeed the more public the better for the merchant himself.

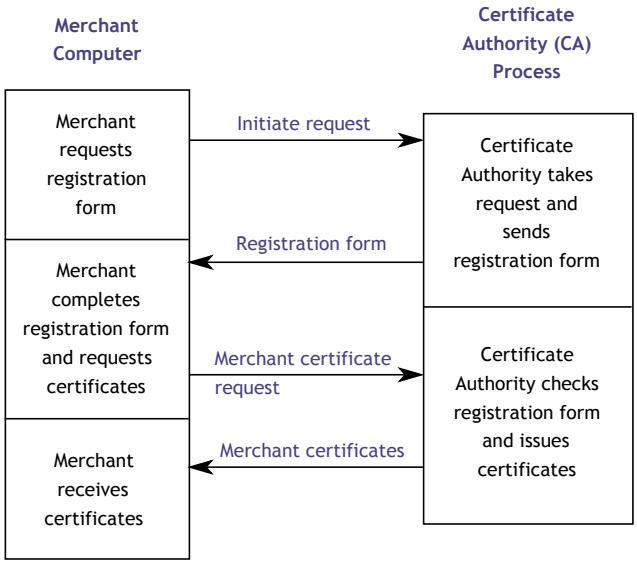

Fig. 2. Merchant Registration

an appropriate registration form, along with its public key certificates.

$$2.\ CA \to M : \mathsf{Sign}_{CA}(M,\ \mathrm{NM2},\ \mathrm{NCA}),\ \mathsf{Cert}_{\mathsf{RCA}}(\mathsf{pubEK}\ CA),\ \mathsf{Cert}_{\mathsf{RCA}}(\mathsf{pubSK}\ CA)$$

i) Merchant Certificate Request: The merchant chooses two asymmetric public/private key pairs, one for signature, the other for encryption. He submits the two public keys, $\mathsf{pubSK}\ M$ and $\mathsf{pubEK}\ M$, along with the completed registration form to the CA, who forwards it to the bank. This message is yet another digital envelope, using the session key KM1.

$$3.\ M \to CA : \mathsf{Crypt}_{\mathrm{KM1}}\ S,\ \ \mathsf{Crypt}_{\mathsf{pubEK}\ CA}\ \mathrm{KM1}$$

where $S =$

$$\mathsf{Sign}(\mathsf{priSK}\ M)(M, \mathrm{NM2}, \mathsf{pubSK}\ M, \mathsf{pubEK}\ M)$$

j) Merchant Certificates: The bank checks the various details and, if satisfied, authorises the CA to issue certificates. The CA signs two certificates, one including the merchant's public signature key and the merchant's identity, the other including the merchant's public encryption key and the merchant's identity. The CA wraps up the two certificates in a single message using no hashing, and sends it to the merchant. When the merchant receives the certificates, he is ready to sell goods over the Internet.

$$4.\ CA \to M : \mathsf{Crypt}_{\mathrm{KC2}}\ (\mathsf{Sign}\ CA(M, \mathrm{NM3}, CA, \mathrm{NonceCCA}),\ \mathsf{Cert}_{CA}(\mathsf{pubSK}\ M),\ \mathsf{Cert}_{\mathsf{RCA}}(\mathsf{pubSK}\ CA))$$

What is the point of verifying SET's registration protocols? The subsequent purchase protocols perform the actual E-commerce, and protocol verifiers often assume that participants already possess all needed credentials. However, the registration protocols are difficult, particularly when it comes to proving that cardholder registration actually keeps the PANSecret secret, an explicit goal of SET [11]. The digital envelopes introduce many keys and nonces, with non-trivial dependency chains.

III. Modelling the Registration Protocols

Our protocol models owe much to the work of Piero Tramontano, who devoted many hours to help us decipher and interpret 1000 pages of SET documentation [3]. Our aim was to capture the essential protocol mechanisms while omitting optional parts and needless complications.

We use the inductive method of protocol verification, which has been described elsewhere [14]. This operational semantics assumes a population of honest agents obeying the protocol and a dishonest agent (the Spy) who can steal messages intended for other agents, decrypt them using any keys at his disposal and send new messages as he pleases. Some of the honest agents are *compromised*: the Spy has full access to their secrets. A protocol is modelled by the set of all possible traces of events that it can generate. Events are of three forms:

- `Says A B X` means A sends message X to B.
- `Gets A X` means A receives message X.
- `Notes A X` means A stores X in his internal state.

There is no guarantee, in general, that a `Says A B X` event implies a `Gets B X` event because reception cannot be guaranteed over an insecure means like the network.

We have flattened SET's hierarchy of certificate authorities [11]. The Root Certificate Authority is responsible for certifying all other CAs. Our model includes compromised CAs, though we assume that

the root is uncompromised. The compromised CAs complicate the proofs — large numbers of session keys and other secrets fall into the hands of the Spy. But even if we assumed that all CAs were honest, a realistic model would have to include the possibility of secrets becoming compromised.

Here is a brief summary of the notation:

- `set_cr` is the set of traces allowed by cardholder registration;
- `set_mr` is the set of traces allowed by merchant registration;
- `used` gathers the set of items appearing in a trace, and serves to express freshness;
- `symkeys` is the set of symmetric keys;
- `Nonce`, `Pan`, `Key`, `Agent`, `Crypt` and `Hash` are obvious message constructors;
- $\{\!|X_1, \ldots, X_n|\!\}$ is an n-component message;
- `sign` is the message constructor for signatures, defined by
  `sign K X == {|X, Crypt K (Hash X)|},`
  where `K` is a private signing key.
- `certC` is the message constructor for a cardholder's public-key certificates, which includes his PAN `P` and the PanSecret `PS`. It is defined by
  ```
  signCert K X == {|X, Crypt K X|}
  certC P Ka PS T signK ==
    signCert signK
      {|Hash {|Nonce PS, Pan P|}, Key Ka, T|}
  ```
- `cert` is the message constructor for public-key certificates of CAs and merchants:
  ```
  cert A Ka T signK ==
    signCert signK {|Agent A, Key Ka, T|}
  ```

Since our earlier work on this protocol [3], we have streamlined the model. For example, the notion of crucial cryptographic keys has been eliminated, as we have found a simpler formalization of the many types of agents and their keys. Two public/private key pairs — one for signature, one for encryption — are functionally associated to each agent's name. For example, `priSK RCA` denotes the private signature key of the Root Certificate Authority. However, no agent knows anyone else's public keys at the beginning of a session but, rather, every agent uses public keys received inside certificates.

A. Cardholder Registration in Isabelle/HOL

A fragment of our inductive model for cardholder registration is shown in Figure 3. The figure omits the rules modelling the early messages of the protocol and the rules that are common to most protocols, such as the definition of the Spy's capabilities. It presents the full rules for messages 5 and 6, which are `SET_CR5` and `SET_CR6` respectively. Each rule details how to extend a given trace of the protocol (`#` is the list "cons" operator) and refers to a typical CA `CA i` and to a typical cardholder `C`, who is defined using the `Cardholder` constructor.

In rule `SET_CR5`, variable `evs5` refers to the current event trace. The preconditions of the rule require the cardholder to issue two fresh nonces `NC3` and `CardSecret`, and two fresh symmetric keys, `KC2` and `KC3`. Also, two events must have occurred in `evs5`: the `Says` event signifies that `C` sent an appropriate instance of message 3 to the CA; the `Gets` event signifies that `C` received the CA's reply, which carries a certificate signed by the Root Certificate Authority and establishing `EKi` to be the CA's public encryption key[2]. Another certificate states that `SKi` is the CA's public signature key.

Then, `C` encrypts using `EKi` a message containing his credit card number (`pan C`) and the key `KC3`, and encrypts using `KC3` a message containing the symmetric key `KC2` and the public signature key to be certified. The two encrypted messages constitute the digital envelope that `C` sends to the CA.

In rule `SET_CR6`, variable `evs6` refers to the current event trace. The rule may fire when the CA receives an instance of message 5, requesting a certificate for the key `cardSK`. The rule lets CA send protocol message 6, a digital envelope containing the desired certificate and encrypted by a symmetric key received from the cardholder. The certificate also contains the PANSecret, which is computed as the exclusive-OR of the `CardSecret` (sent by the cardholder) and `NonceCCA` (generated by the CA). While sending the message, the CA stores the key just certified in order to prevent its being certified more than once. The rule for message 6 checks that the key `cardSK` has not previously been registered by imposing the precondition

$$\texttt{Notes (CA i) (Key cardSK)} \notin \texttt{set evs6}$$

which elegantly replaces a less readable precondition we used initially [3].

Modelling `C`'s generation of fresh public/private key pairs is not difficult, as we have reported already [3]. It involves replacing `pubSK C` and `priSK C` with variables ranging over keys, and extending the pre-

[2]The flag `onlyEnc` in the certificate indicates that it refers to an encryption key, while `onlySig` indicates a signature key.

```
SET_CR5:
  "⟦evs5 ∈ set_cr;  C = Cardholder k;
    Nonce NC3 ∉ used evs5; Nonce CardSecret ∉ used evs5;
    NC3 ≠ CardSecret;
    Key KC2 ∉ used evs5; KC2 ∈ symKeys;
    Key KC3 ∉ symKeys; KC3 ∈ symKeys; KC2≠KC3;
    Gets C {|sign (invKey SKi) {|Agent C, Nonce NC2, Nonce NCA|},
             cert (CA i) EKi onlyEnc (priSK RCA),
             cert (CA i) SKi onlySig (priSK RCA)|}
        ∈ set evs5;
    Says C (CA i)
         {|Crypt KC1 {|Agent C, Nonce NC2, Hash (Pan (pan C))|},
          Crypt EKi {|Key KC1, Pan (pan C),
                      Hash {|Agent C, Nonce NC2|}|}|}
         ∈ set evs5⟧
⟹ Says C (CA i)
         {|Crypt KC3
          {|Agent C, Nonce NC3, Key KC2, Key (pubSK C),
           Crypt (priSK C)
             (Hash {|Agent C, Nonce NC3, Key KC2,
                     Key(pubSK C), Pan(pan C), Nonce CardSecret|})|},
          Crypt EKi {|Key KC3, Pan (pan C), Nonce CardSecret|}|}
    # evs5 ∈ set_cr"


SET_CR6:
  "⟦evs6 ∈ set_cr;
    Nonce NonceCCA ∉ used evs6;
    KC2 ∈ symKeys;  KC3 ∈ symKeys;  cardSK ∉ symKeys;
    Notes (CA i) (Key cardSK) ∉ set evs6;
    Gets (CA i) {|Crypt KC3 {|Agent C, Nonce NC3, Key KC2, Key cardSK,
                  Crypt (invKey cardSK)
                   (Hash{|Agent C, Nonce NC3, Key KC2,
                          Key cardSK, Pan(pan C), Nonce CardSecret|})|},
                  Crypt (pubEK (CA i)) {|Key KC3, Pan (pan C),
                                         Nonce CardSecret|}|}
      ∈ set evs6⟧
⟹ Says (CA i) C (Crypt KC2
                   {|sign (priSK (CA i))
                    {|Agent C,Nonce NC3,Agent(CA i), Nonce NonceCCA|},
                     certC (pan C) cardSK (XOR(CardSecret,NonceCCA))
                                   onlySig (priSK (CA i)),
                     cert (CA i) (pubSK(CA i)) onlySig (priSK RCA)|})
  # Notes (CA i) (Key cardSK)
  # evs6 ∈ set_cr"
```

Fig. 3. Modelling Cardholder Registration (fragment)

conditions of *SET_CR5* with the extra requirements that the newly introduced public keys are fresh and asymmetric.

B. Merchant Registration in Isabelle/HOL

The machinery developed above can be reused to model merchant registration. A typical merchant *M* is defined using the *Merchant* constructor. The inductive rules modelling the last two messages of the protocol appear in Figure 4.

Rule *SET_MR3* specifies that the merchant *M* generates a single session key *KM1* and asks for certification of both his public keys. This differs from the previous protocol, where cardholder generates two session keys and asks for certification of his signature key only. The rule may fire only if the merchant sent message 1 of the protocol, as stated by the *Says* event, and received message 2, as stated by the *Gets* event.

If the CA agrees to certify the merchant's keys,

```
SET_MR3:
  "⟦evs3 ∈ set_mr; M = Merchant k; Nonce NM2 ∉ used evs3;
    Key KM1 ∉ used evs3;  KM1 ∈ symKeys;
    Gets M {|sign (invKey SKi) {|Agent X, Nonce NM1, Nonce NCA|},
            cert (CA i) EKi onlyEnc (priSK RCA),
            cert (CA i) SKi onlySig (priSK RCA)|}
      ∈ set evs3;
    Says M (CA i) {|Agent M, Nonce NM1|} ∈ set evs3⟧
 ⟹ Says M (CA i)
         {|Crypt KM1 (sign (priSK M) {|Agent M, Nonce NM2,
                                       Key(pubSK M), Key(pubEK M)|}),
           Crypt EKi (Key KM1)|}
       # evs3 ∈ set_mr"


SET_MR4:
  "⟦evs4 ∈ set_mr; M = Merchant k;
    merSK ∉ symKeys;  merEK ∉ symKeys;
    Notes (CA i) (Key merSK) ∉ set evs4;
    Notes (CA i) (Key merEK) ∉ set evs4;
    Gets (CA i) {|Crypt KM1 (sign (invKey merSK)
                          {|Agent M, Nonce NM2, Key merSK, Key merEK|}),
                  Crypt (pubEK (CA i)) (Key KM1)|}
      ∈ set evs4⟧
⟹ Says (CA i) M {|sign (priSK (CA i))
                    {|Agent M, Nonce NM2, Agent (CA i)|},
                  cert   M   merSK  onlySig (priSK (CA i)),
                  cert   M   merEK  onlyEnc (priSK (CA i)),
                  cert (CA i) (pubSK (CA i)) onlySig (priSK RCA)|}
      # Notes (CA i) (Key merSK)
      # Notes (CA i) (Key merEK)
      # evs4 ∈ set_mr"
```

Fig. 4. Modelling Merchant Registration (fragment)

it must also record them, as stated by rule *SET_MR4*. The conclusion of the rule adds the three corresponding events to the current trace. The merchant's certificates have the same form as the CA's certificate — indeed, all of them are expressed using the same message constructor, *cert*. These certificates are sent in clear, since the message for issuing certificates "shall be signed but not encrypted if the [certificate recipient] is a Merchant or Payment Gateway" [12, p.191]. However, SET requires the last message of cardholder registration to be encrypted.

Merchant registration is simpler than cardholder registration. It involves fewer sensitive components. There is no equivalent of the PAN or of the PANSecret, and there are fewer digital envelopes.

IV. Secrecy Proofs for Cardholder Registration

For cardholder verification we proved 64 theorems in total; for merchant registration we proved 31. These include all the main goals for these protocols and all necessary lemmas. We have space to present only a small selection. We concentrate on the most difficult and interesting proofs concerning secrecy in cardholder registration. Here we have introduced the new methods to deal with digital envelopes.

A primary goal is that cardholder registration guarantees secrecy of the PANSecret. No message of the protocol sends this number, not even in encrypted form. Rather, both parties compute it as the exclusive-OR of other numbers. So, do those numbers remain secret? Since they are encrypted using symmetric keys, the proof requires a lemma that symmetric keys remain secret.

The first complication is that some symmetric keys do *not* remain secret, namely those involving a compromised CA. The second, major complication is that some symmetric keys are used to encrypt others: the loss of one key can compromise a second key, leading possibly to unlimited losses.

The problem of one secret depending on another

has occurred previously, with the Yahalom [15] and Kerberos [4] protocols. Both of these are comparatively simple: the dependency relation links only two items. Cardholder registration has many dependency relationships. It also has a dependency chain of length three: in the last message, a secret number is encrypted using a key (*KC2*) that was itself encrypted using another key (*KC3*).

To solve this problem, we have generalized the method described in earlier work to chains of any length. While the definitions become more complicated than before, they follow a uniform pattern. The idea is to define a relation, for a given trace, between pairs of secret items: (K, X) are related if the loss of the key K leads to the loss of the key or nonce X. Two new observations can be made about the dependency relation.

1) It should ignore messages sent by the Spy, since we can only hope to prove secrecy for honest participants. This greatly simplifies some proofs.
2) It must be transitive, since a dependency chain leading to a compromise could have any length. Past protocols were too simple to reveal this point.

Secrecy of session keys is proved as it was for Kerberos [4], by defining the relation *KeyCryptKey DK K evs* that takes two keys *DK* and *K*, and an event trace *evs*. It holds on a trace containing a message in which the first key encrypts the second key. As we shall see, reasoning about *KeyCryptKey* will allow us to prove that most symmetric keys remain secure.

From that result, one might think it would be easy to prove that nonces encrypted using those keys remain secret. However, secrecy proofs for nonces appear to require the same treatment as secrecy proofs for keys. We must define the dependency relation between keys and nonces. Then the proofs can be carried forward as it was for Yahalom [15], except that there are many key-nonce relationships rather than one.

A. Relations between secrets

The relation *KeyCryptKey DK K evs* is defined as a primitive recursive function in Figure 5. Rule *KeyCryptKey_Nil*, the base case of the recursion, states that the relation is false on an empty trace. Rule *KeyCryptKey_Cons* formalizes the recursive step. For the relation to hold on the extended trace *ev#evs* the relation must either hold on the original trace *evs*, or the new event *ev* must have a specific structure. It could be an instance of message 5 (shown above in §III) in which some principal who is not Spy uses *KC3* to encrypt *KC2*. Alternatively, *ev* could be any event in which someone encrypts *KC3* using a public key. In the latter case, *KeyCryptKey* holds of the corresponding private key, which can decrypt the message. In reading the definition, note that "$\vee$" denotes logical disjunction, while "|" is part of the "*case*" syntax.

Figure 6 defines the dependency relation for nonces. Here are some hints towards understanding this definition. The only important case involves *Says* events. The first disjunct refers to message 5, where key *KC3* encrypts nonce *NC3*; it also covers a similar encryption in message 3. The second and third disjuncts refer to message 6; they involve *KeyCryptKey* because that encryption uses a key received from outside. The fourth disjunct essentially says that we are not interested in asymmetric keys (they are never sent, so there is no risk of compromise).

B. Verification of Secrecy Properties

Now we outline the verification of cardholder registration. The handling of fresh public keys does not add technical difficulties thanks to Isabelle's level of automation. What we found difficult were the secrecy properties, and we concentrate on them here. We first sketch informally the key steps of our reasoning to give a feel of the proof effort. Three are the main lemmas:

- keys can be compromised only through the disclosure of other keys;
- keys sent by cardholders to uncompromised CAs are never disclosed;
- nonces cannot be compromised through the disclosure of keys;

Building on these lemmas, we are able to prove our key theorems:

- the CardSecret is secure if the cardholder sends the **certificate request** message to an uncompromised CA;
- the NonceCCA is secure if it is contained in a **cardholder certificate** received by the cardholder from an uncompromised CA;
- the PAN is secure unless the cardholder has sent a **certificate request** message to a compromised CA.

```
KeyCryptKey_Nil:
  "KeyCryptKey DK K [] = False"

KeyCryptKey_Cons:
  "KeyCryptKey DK K (ev # evs) =
   (KeyCryptKey DK K evs ∨
    (case ev of
       Says A B Z ⇒
         ((∃N X Y. A ≠ Spy ∧
                   DK ∈ symKeys ∧
                   Z = {|Crypt DK {|Agent A, Nonce N, Key K, X|}, Y|}) ∨
          (∃C. DK = priEK C))
     | Gets A' X ⇒ False
     | Notes A' X ⇒ False))"
```

Fig. 5. Relation between Keys in Cardholder Registration

```
KeyCryptNonce DK N (ev # evs) =
 (KeyCryptNonce DK N evs ∨
  (case ev of
    Says A B Z ⇒
     A ≠ Spy ∧
     ((∃X Y. Z = {|Crypt DK {|Agent A, Nonce N, X|}, Y|}) ∨
      (∃K i X Y.
        Z = Crypt K {|sign (priSK i) {|Agent B, Nonce N, X|}, Y|} ∧
        (DK=K ∨ KeyCryptKey DK K evs)) ∨
      (∃K i NC3 Y.
        Z = Crypt K
              {|sign(priSK i) {|Agent B, Nonce NC3, Agent(CA i), Nonce N|},
                Y|} ∧
        (DK=K ∨ KeyCryptKey DK K evs)) ∨
      (∃i. DK = priEK i))
  | Gets A' X ⇒ False
  | Notes A' X ⇒ False))
```

Fig. 6. Relation between Keys and Nonces in Cardholder Registration

Obviously, we have to trust the certificate authority. The CA's task is to certify that there is a correspondence between a certificate and a credit card number. To obtain this goal, the CA must be able to see the credit card number.

In the sequel, each theorem is stated first in English and then using Isabelle notation. Each has been mechanically verified with Isabelle/HOL, typically by some form of induction. Some of them are so-called regularity properties, which are easy to prove [14]. For example, one protocol goal is almost trivial: if a certificate bears the signature of an uncompromised CA, then it was sent by the CA.

To prove our main results we need a number of preliminary technical lemmas. For example, we never have `KeyCryptKey DK K evs` where `DK` is fresh (in the trace `evs`), since a fresh key cannot have been used to encrypt anything. Several other obvious properties of `KeyCryptKey` turn out to be needed in the proofs below.

We can then move on to the *session key compromise theorem*. It states that a key can be lost only by the keys related to it by `KeyCryptKey`. It is used in other proofs to reason about situations in which some session keys might be compromised.

Lemma 1—symKey_compromise: Except in trivial cases, no symmetric key can be compromised through the disclosure of other keys.

```
⟦evs ∈ set_cr; SK ∈ symKeys;
 ∀K∈KK. ¬ KeyCryptKey K SK evs⟧ ⟹
(Key SK ∈ analz(Key'KK ∪ knows Spy evs)) =
(SK∈KK ∨ Key SK ∈ analz(knows Spy evs))
```

We can interpret this theorem as asserting that `KeyCryptKey` expresses all circumstances in which a symmetric key can become compromised. The proof is a big, difficult induction consisting of 10 proof commands. The simplification step requires a specialized set of rewrite rules, including lemmas about

KeyCryptKey, and is relatively slow (14 seconds). The peculiar form of the lemma represents the generalization needed to make the induction succeed. Here are the preconditions in detail:

- *evs* ∈ *set_cr* simply means that *evs* is a trace of cardholder registration. All proofs about the protocol will include this assumption.
- *SK* ∈ *symKeys* means that *SK* is a symmetric key.
- ∀*K*∈*KK*. ¬*KeyCryptKey K SK evs* means that *KK* is a set of keys, none of which immediately compromises *SK* in the trace *evs*.

In the conclusion, the formula

```
Key SK ∈ analz (Key'KK ∪ knows Spy evs)
```

means that *SK* can be derived from *KK* together with the Spy's knowledge (which mainly consists of observable traffic). The right-hand side of the conclusion is

```
(SK∈KK ∨ Key SK ∈ analz (knows Spy evs))
```

which means that either *SK* is itself a member of the set *KK* or *SK* is already derivable from the Spy's knowledge alone.

We could simplify the right-hand side above, and many other formulas, by defining *KeyCryptKey* to be reflexive. The intuition is attractive, for then *KeyCryptKey* would hold when there was a chain of decryptions from one key to another, of length possibly zero. However, this change would strengthen the precondition of Lemma 1, making it harder to prove (when we need to use the induction hypothesis) and harder to apply.

Lemma 2—symKey_secrecy: Symmetric keys sent by cardholders to uncompromised CAs are never disclosed.

```
⟦CA i ∉ bad; K ∈ symKeys; evs ∈ set_cr;
 Says (Cardholder k) (CA i) X ∈ set evs;
 Key K ∈ parts {X}⟧
⟹ Key K ∉ analz (knows Spy evs)
```

This result follows from Lemma 1, but not trivially. It states a general law for any symmetric key (*K* above) that is part of (*K* ∈ *parts*{*X*}) any message *X* sent by the cardholder. Since the proof requires examination of all protocol steps, it involves another induction and the simplification again needs special rewrite rules concerning secrecy. It is not an explicit protocol goal — symmetric keys are just part of the underlying machinery — but it is obviously desirable.

Lemma 3—Nonce_compromise: No nonce can be compromised through the disclosure of keys except in trivial cases.

```
⟦evs ∈ set_cr;
 ∀K∈KK. ¬ KeyCryptNonce K N evs⟧ ⟹
(Nonce N ∈ analz (Key'KK ∪ knows Spy evs)) =
(Nonce N ∈ analz (knows Spy evs))
```

In both statement and proof, this result resembles Lemma 1. In particular, the precondition ∀*K*∈*KK*. ¬ *KeyCryptNonce K N evs* means that *KK* is a set of keys, none of which immediately compromises the nonce *N*. The conclusion is that the Spy could derive *N* with the help of the set *KK* only if he could have derived *N* without using that set. The situation is complicated by the many different nonces used in cardholder registration, only some of which are kept secret. So the proof is even longer than that of Lemma 1, despite its appealing to that lemma; it requires 14 proof steps and involves reasoning about both *KeyCryptKey* and *KeyCryptNonce*.

Theorem 1—CardSecret_secrecy: If a cardholder sends the **certificate request** message to an uncompromised CA, then the chosen CardSecret will remain secure.

```
⟦CA i ∉ bad;
 Says (Cardholder k) (CA i)
   {|X, Crypt EKi {|Key KC3, Pan p,
            Nonce CardSecret|}|} ∈ set evs;
 Gets A
   {|Z, cert (CA i) EKi onlyEnc (priSK RCA),
       cert (CA i) SKi onlySig (priSK RCA)|}
   ∈ set evs;
 KC3 ∈ symKeys;  evs ∈ set_cr⟧
⟹ Nonce CardSecret ∉ analz (knows Spy evs)
```

This is an important goal: SET purchases are safe only if CardSecret is uncompromised. The proof involves another complicated induction despite its use of Lemmas 1 and 3. In the preconditions, note that the cardholder builds the digital envelope using any symmetric key *KC3*; the public key, *EKi*, is bound to the CA through a certificate signed by *RCA*. The main body of the argument is an induction that additionally assumes *KC3* to be uncompromised; later, an appeal to Lemma 2 removes that assumption.

Theorem 2—NonceCCA_secrecy: If a cardholder sends the **certificate request** message to an uncompromised CA and receives in response the **cardholder certificate**, then the value of NonceCCA contained in the latter will remain secure.

```
⟦CA i ∉ bad;
 Gets (Cardholder k)
```

```
   (Crypt KC2
    {|sign(priSK(CA i))
      {|Agent C, Nonce N, Agent(CA i),
       Nonce NonceCCA|},
     X, Y|}) ∈ set evs;
 Says (Cardholder k) (CA i)
   {|Crypt KC3
      {|Agent C, Nonce NC3, Key KC2, X'|},
    Y'|} ∈ set evs;
 Gets A
   {|Z, cert(CA i) EKi onlyEnc (priSK RCA),
       cert(CA i) SKi onlySig (priSK RCA)|}
   ∈ symKeys;  evs ∈ set_cr⟧
⟹ Nonce NonceCCA ∉ analz(knows Spy evs)
```

This result is as important as Theorem 1, since both CardSecret and NonceCCA are ingredients of the all-important PANSecret. The proof resembles that of Theorem 1 but is a bit more complicated, since it refers to two protocol messages. Variables such as X and Y refer to irrelevant parts of messages.

This theorem is a guarantee to the cardholder: it is expressed in terms of events that the cardholder can verify. We have not proved the analogous guarantees for the CA. Although NonceCCA originates with the CA, its compromise would do the CA no harm.

Theorems 1 and 2 are as close as we can come to expressing the secrecy of the PANSecret, since our model does not let us reason about exclusive-OR. Our next goal is to prove secrecy of the PAN: the credit card number.

Lemma 4—analz_insert_pan: A PAN cannot be compromised through the disclosure of symmetric keys.

```
⟦evs ∈ set_cr;  K ∉ invKey‘pubEK‘range CA⟧
⟹
(Pan P ∈ analz(insert(Key K)(knows Spy evs)))
=
(Pan P ∈ analz(knows Spy evs))
```

This result resembles Lemma 3 but is much easier to prove because PANs are encrypted only with public keys. As the model does not allow public keys to be broken during a trace, no key dependency chains complicate the reasoning. In essence, the inductive argument examines all protocol messages to confirm that symmetric keys are never used to encrypt PANs.

The obscure premise `K ∉ invKey ‘ pubEK ‘ range CA` states that the key `K` is not the private encryption key of any CA. The lemma says that if the Spy can discover a PAN with the help of `K`, then he could have discovered the PAN without using `K`. To make the induction work, we had to prove a stronger statement (not shown); it generalizes the lemma above to replace `K` by a set of symmetric keys. The final guarantee about the PAN says that it remains secure unless it is sent to a compromised CA (for its private keys are known to the Spy).

Theorem 3—pan_confidentiality: If a PAN has been disclosed, then the cardholder has sent a **certificate request** message to a compromised CA.

```
⟦Pan (pan C) ∈ analz(knows Spy evs);
 C ≠ Spy; evs ∈ set_cr⟧ ⟹
∃i X K HN.
   Says C (CA i)
     {|X, Crypt (pubEK(CA i))
                {|Key K, Pan(pan C), HN|}|}
   ∈ set evs
∧ (CA i) ∈ bad
```

This result is proved by induction, using Lemma 4 and the usual rewriting rules for secrecy proofs.

Merchant registration is much easier to analyze than cardholder registration. The simpler form of the **certificate request** message eliminates the dependence between symmetric keys. The lack of the fields PAN, CardSecret and NonceCCA leaves us with little to prove secret.

V. Related Work and Conclusions

Of the many other efforts into protocol verification, the most relevant is TAPS by Ernie Cohen [6]. Given a protocol, Cohen's system automatically generates a *secrecy invariant*, which serves the same purpose as the relations `KeyCryptKey` and `KeyCryptNonce`. Potentially, TAPS could verify cardholder registration, though the protocol's size and complexity may present difficulties in the automatic generation of invariants.

As far as we are aware, no other group has attempted to verify the SET registration protocols directly out of the specifications. Recently, based on our previous formalization [3], Ernie Cohen has verified the card-holder registration with TAPS obtaining substantially the same results as ours. The same formalization has also been used in the course of the AVISS project [1] for verification with infinite state model checking. They could not verify the main secrecy and unicity goals (the AVISS systems are so far restricted to classical authentication properties), but an "attack" on authentication has been found: the nonces `NC3` and `NC2` do not provide injective agreement, and the CA may receive twice the same request for a certificate for the same key for the same

client. As we already noted here and in our previous work [3], agreement fails because it is optional to send back received nonces but this fact is immaterial, since it does not affect the goals of the protocol.

What can be concluded from our analysis of the SET registration protocol?

From the standpoint of protocol verification, the general treatment of secrecy proofs, as exemplified in `KeyCryptKey` and `KeyCryptNonce`, is a major outcome of our work. The definitions of these relations are complicated but conform to an obvious pattern that could be automated. Verifying the registration protocols was valuable preparation for our later verification of the purchase protocols [2].

The complicated RSA digital envelopes and signature conventions make proofs difficult and slow. Compared with other protocols that researchers have verified, SET's registration protocols use encryption heavily, resulting in gigantic terms or complex case splits. Sometimes Isabelle presents the user with subgoals spanning several pages of text. One should not attempt to prove such a monstrosity directly. One useful strategy is to look for terms that can be simplified and prove the corresponding rewrite rules. This may cut the monstrosity down to size.

Our model does not include the algebraic properties of exclusive-OR, such as $X \oplus Y \oplus X = Y$, and this prevents us from proving the security of the PANSecret. We assume that $X \oplus Y$ is secure if both X and Y are. Our treatment of the PANSecret amounts to assuming that it is computed as the hash of X and Y, which would certainly be an improvement over exclusive-OR. A bad CA can force the PANSecret to take on a chosen value N by setting NonceCCA to be CardSecret $\oplus$ N. The cardholder has no defence against this attack unless he knows the value of N.

From the standpoint of protocol security, one can conclude that the registration protocol has some constructions that make it a bit unwieldy and cumbersome, uses too many layers of encryption but that, all in all, it does what it claims to do in the specifications, given the assumptions about its environment (see again Section II).

It remains to be seen whether it does all that it should do. For instance, should the protocol also satisfy various forms of authentication and agreement? This is a tricky question because we eliminated fields that are immaterial to the main goals of the protocol but that may be essential for other security properties. For instance we have eliminated request-response identifiers which are recommended by Gong and Syverson [7] to make authentication protocols more robust and secure.

One may also argue that SET should also satisfy more advance properties such as non repudiation. For instance a cardholder should be able to prove to a third party that a misbehaving CA tampered with the PANSecret. However, the verification of these properties implies major changes in the specifications and in the assumptions about the environment, and is likely to result in dubious proofs of security or highly debatable attacks. The verification of additional properties must be based on a clearly defined and widely agreed model for e-commerce protocol goals revising the classical Dolev-Yao model for authentication protocol. We leave this open for future investigations.

Acknowledgments

We would like to thank P. Tramontano for helping us in the unwinding of the SET specifications. L. Compagna and Y. Chevalier for discussing their verification of the SET Registration within the AVISS project.

REFERENCES

[1] A. e. a. Armando. The aviss security protocol analysis tool. In *Proceedings of CAV-2002*, Lecture Notes in Comp. Sci. Springer-Verlag, 2002.

[2] G. Bella, F. Massacci, and L. C. Paulson. Verifying the SET purchase protocols. Technical Report 524, Computer Laboratory, University of Cambridge, Nov. 2001. To appear in *ACM Computer and Communication Security (CCS-2002*.

[3] G. Bella, F. Massacci, L. C. Paulson, and P. Tramontano. Formal verification of cardholder registration in SET. In F. Cuppens, Y. Deswarte, D. Gollman, and M. Waidner, editors, *Computer Security — ESORICS 2000*, LNCS 1895, pages 159–174. Springer, 2000.

[4] G. Bella and L. C. Paulson. Kerberos version IV: Inductive analysis of the secrecy goals. In J.-J. Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann, editors, *Computer Security — ESORICS 98*, LNCS 1485, pages 361–375. Springer, 1998.

[5] J. Clark and J. Jacob. A survey of authentication protocol literature: Version 1.0. Technical report, University of York, Department of Computer Science, November 1997. Available on the web at `http://www-users.cs.york.ac.uk/~jac/`. A complete specification of the Clark-Jacob library in CAPSL is available at `http://www.cs.sri.com/~millen/capsl/`.

[6] E. Cohen. TAPS: A first-order verifier for cryptographic protocols. In *Proc. of the 13th IEEE Comp. Sec. Found. Workshop*, pages 144–158. IEEE Comp. Society Press, 2000.

[7] L. Gong and P. Syverson. Fail-stop protocols: An approach to designing secure protocols. In *Proceedings of the 5th IFIP Working Conference on Dependable Computing for Critical Applications (DCCA-5)*, September 1995.

[8] J. Guttman. Security goals: Packet trajectories and strand spaces. In R. Focardi and F. Gorrieri, editors, *Foundations of Security Analysis and Design - Tutorial Lectures*, volume 2171 of *Lecture Notes in Comp. Sci.*, pages 197–261. Springer-Verlag, 2001.

[9] G. Lowe. A hierarchy of authentication specifications. In *Proc. of the 10th IEEE Comp. Sec. Found. Workshop*, pages 31–43. IEEE Comp. Society Press, 1997.

[10] G. Lowe. Casper: A compiler for the analysis of security protocols. *J. of Comp. Sec.*, 6(18-30):53–84, 1998.

[11] Mastercard & VISA. *SET Secure Electronic Transaction Specification: Business Description*, May 1997. Available electronically at `http://www.setco.org/set_specifications.html`.

[12] Mastercard & VISA. *SET Secure Electronic Transaction Specification: Programmer's Guide*, May 1997. Available electronically at `http://www.setco.org/set_specifications.html`.

[13] C. Meadows. Analysis of the Internet Key Exchange protocol using the NRL Protocol Analyzer. In *SSP-99*, pages 216–231. IEEE Comp. Society Press, 1999.

[14] L. C. Paulson. The inductive approach to verifying cryptographic protocols. *J. of Comp. Sec.*, 6:85–128, 1998.

[15] L. C. Paulson. Relations between secrets: Two formal analyses of the Yahalom protocol. *J. of Comp. Sec.*, 9(3):197–216, 2001.

[16] P. Ryan and S. Schneider. An attack on a recurive authentication protocol. a cautionary tale. *Inform. Processing Lett.*, 65(15):7–16, 1998.