Verifying Electronic Commerce Protocols

Lawrence C. Paulson

Computer Laboratory, University of Cambridge

1 Previous Research and Track Record

This proposal concerns protocol verification by formal proof. With EPSRC funding, Paulson has developed a new and highly successful approach to verifying security protocols: the *inductive method*. The protocols analyzed by this method include a standard Internet protocol (TLS, a descendant of SSL) [10] and one developed by a UK company, APM Ltd. [9]. APM's protocol was difficult to analyze using previous methods. The inductive analysis uncovered some flaws in it, suggesting a new and correct design. The present proposal is to apply the inductive method to e-commerce protocols, including SET (Secure Electronic Transactions). Outcomes will include a formalization of the protocol and a more general proof environment in which to analyze other protocols.

The work will be done within the Cambridge Automated Reasoning Group. Hardware verification was pioneered here by M. J. C. Gordon and his students. They introduced what have become standard techniques, such as the use of higher-order logic to model hardware and software systems. The group's work continues to attract worldwide attention. For example, John Harrison won the Distinguished Dissertation Award for his thesis on verification involving floating-point arithmetic; his subsequent recruitment by Intel is evidence that formal proof is relevant to industry.

The group has built two of the most important proof environments used today, namely HOL and Isabelle. Isabelle (developed by Paulson) is a generic theorem prover. It supports interactive proof in several formal systems, including first-order logic, higher-order logic and Zermelo-Frankel set theory. Derived logics can be supported as well as primitive formalisms. Researchers have used Isabelle to support complicated specification languages such as TLA and Z.

Several past projects at Cambridge involve Isabelle:

- *Combining HOL and Isabelle* (SERC ref. GR/H40570), 1992-95. This project applied Isabelle to HOL-style problems, the main application being proof support for Lamport's TLA (Temporal Logic of Actions).

- *Verifying ML Programs using Evaluation Logic* (SERC ref. GR/G53279), 1991–95. This project has clarified some of the subtle interactions that occur when references to a store interact with higher-order functions.

- *Authentication Logics: New Theory and Implementations* (EPSRC ref. GR/K77051), 1996-99. This project, concerned with proving the correctness of security protocols, led to the development of the inductive method. It also produced a detailed analysis of a digital cash protocol.

- *Mechanising Temporal Reasoning* (EPSRC ref. GR/K57381), 1995-99. This project investigated the verification of reactive systems using logics such as TLA and UNITY. An Isabelle proof environment for UNITY was developed and distributed.

- *Compositional Proofs of Concurrent Programs* (EPSRC ref. GR/M75440), 2000-03. This project, which has just started, continues *Mechanising Temporal Reasoning*. It concentrates on UNITY and the guarantees-calculus of Sanders and Chandy. A case study, a token allocation system, has been formalized.

The proposal is in the spirit of many previous projects at Cambridge. Hardware devices or software units are analyzed. New verification methodologies are developed and improved, with particular emphasis on automation. Success requires choosing a suitably abstract model, deriving tractable formal theories and building powerful tools.

The work will involve close collaboration with the Cambridge Security Group, which is a world-class source of expertise on security protocols. Additional expertise is available nearby from local firms such as Microsoft Research and SRI.

2 Description of Proposed Research

2 A. Background

Security protocols protect messages sent over a network from being read or altered by some enemy. Security protocols often use cryptography and are notoriously error-prone: a fault in the Needham-Schroeder public-key protocol (a trivial one by modern standards) lay undiscovered for over a decade.

Electronic commerce requires protocols of great complexity. To make a purchase over the Internet, the customer typically submits his credit card number to the merchant, protected by a protocol such as SSL. However, many potential customers are uneasy about revealing their credit card number over the Internet. The SET protocol [13, 14, 15] has been proposed by a consortium of credit card and software companies. SET aims to protect sensitive card-holder information, to ensure payment integrity and to authenticate merchants and card-holders.

The overall architecture of SET is based on a rooted hierarchy of *Certification Authorities* (CAs), whose task is to provide customers with digital certificates for signature and encryption. Customers must generate and safeguard their private keys. A normal run of the SET protocol consists of five phases. The first two phases — *Card-holder Registration* and *Merchant Registration* — are used by the protocol participants to register their keys and to get the appropriate certificates. The remaining three phases — *Purchase Request*, *Payment Authorization* and *Payment Capture* — constitute the electronic transaction itself. To accomplish these tasks SET uses numerous combinations of hashing, public key and symmetric key cryptography based on the PKCS#7 standards from RSA Laboratories [12].

SET has been deployed, for example, in Microsoft *Wallet*. Companies such as Hitachi, IBM and VeriSign are currently testing SET-based products.[1] Some security experts feel that, for various reasons, SET will never gain widespread acceptance. Whether it does or not, we can be certain that new e-commerce protocols will be developed. Unlike SSL, they will not require the customer to trust the merchant. These new protocols will probably share much of SET's architecture, as outlined in the previous paragraph.

Many researchers have looked at the problem of verifying e-commerce protocols, but much work remains to be done. Here are a few examples from the extensive literature. Brackin [5] analyzed two Cybercash protocols. His method 'addresses only parts of the protocol failure problem, but addresses these parts quickly and automatically.' Bolignano [4] described (in 1997) an approach combining the Coq tool with a translation of properties into finite automata; he claimed

[1] See `http://www.setco.org/interop_festival.html`, a SETCo Web page listing 33 new products that are undergoing testing.

to be working on SET, but no results have been published.[2] Kessler and Neumann [6] have designed a belief logic to analyse a single message of the payment phase of SET. These efforts are valuable, but in each case the formal model is very abstract, allowing obvious flaws to go undetected. The last two approaches rely on authentication logics, which have been known to deliver misleading results. Model-checking is a more reliable verification method; a recent example is the analysis by Shmatikov and Mitchell [16] of a contract signing protocol.

With previous EPSRC funding, the principal investigator has developed an inductive method for analyzing cryptographic protocols [9]. The method is built on simple foundations: an operational semantics of a system consisting of good agents, a bad agent, and trusted servers. It can easily be extended to model new hardware, such as smart cards. Properties are proved using Isabelle [8]. Although the proofs are not automatic, an expert user can analyze a protocol in days or weeks. Important protocols have been analyzed, such as Kerberos IV [3].

The objective of the proposed project is to conduct an inductive analysis of some e-commerce protocols, including SET. An inductive analysis of SSL (or rather of TLS as it is now called) has already been undertaken [10]. Preliminary experiments suggest that even SET can be analyzed, but it will be a much greater task. Some colleagues and I [2] have formalized the first phase of SET, namely Card-holder Registration, and proved a simple fact about it. Given enough time and resources, a more thorough analysis of SET should be possible.

2 B. Programme and Methodology

SET is complicated: its documentation [13, 14, 15] totals nearly 1000 pages. The project will identify and analyze those elements of SET that are of scientific interest. As usual with formal methods, we shall not be concerned with bit-level details, and whenever possible we shall regard cryptographic primitives as black boxes. By focussing on the top-level architecture, we expect our analysis to be relevant to other e-commerce protocols.

The programme of work will consist of proceeding through the five phases of SET, one after the other. In this first pass, in order to avoid getting bogged down, we shall prove only the more straightforward properties, while identifying deeper properties to be proved in a second pass. Straightforward properties include integrity of messages. Deeper properties include confidentiality and authenticity.

The analysis of SET will mainly be carried out by the research assistant, with the assistance of the principal investigator (Paulson). We expect to collaborate

[2] In an e-mail message, Jean Goubault-Larrecq said 'Unfortunately, the Groupements des Cartes Bancaires wanted to keep the resulting document (formalisation + proofs) confidential, so it is basically available to no one.'

with Dr. Fabio Massacci of the University of Siena, Italy. Dr. Massacci played a major role in the preliminary analysis of SET's Card-holder Registration phase.

A natural by-product of these proofs will be to extend the existing protocol verification environment with new theories and proof methods tailored to the cryptographic primitives used in SET. This extended environment will be valuable in its own right, and we shall apply it to other protocols.

While the SET analysis is under way, we shall look out for other e-commerce protocols to verify. New ones are regularly published in conferences such as *Security and Privacy* (Oakland) and *Financial Cryptography*, though only the most significant protocols can be verified in the time available. They are typically quite simple and could be analyzed by either the research assistant or the principal investigator. They may offer facilities not available in SET, such as micro-payments or non-repudiation.

Paulson will direct the project and will maintain and extend Isabelle. He will develop formal models of the protocols in conjunction with the research assistant.

Criteria for Success

1. to produce a simplified formal model of the SET protocol
2. to analyze this model formally, proving theorems and finding protocol flaws
3. to develop a proof environment for reasoning about e-commerce protocols in general

2 C. Relevance to Beneficiaries

Beneficiaries include the users of e-commerce protocols, the industries that develop and deploy such protocols, and academics undertaking research on such protocols.

A deeper understanding of SET will benefit everybody — e-businesses, their customers, and banks — with an interest in e-commerce. We have already found [2] many ambiguities in the SET specifications, and we can expect to find other flaws. Proving that parts of SET function correctly will be valuable to protocol designers. In the long term, protocol verification could reduce losses suffered by banks. It could improve customers' trust in on-line shopping, resulting in increased trade.

Among the academic beneficiaries will be researchers using other formal methods for protocol verification. For example, model-checking [7, 16] can find attacks against protocols automatically. Such researchers will not have to duplicate the task of understanding nearly 1000 pages of SET documentation; instead, they can translate our Isabelle theories into their chosen formalism.

The project work will inevitably include improvements to Isabelle, which benefits its users.

In short, the beneficiaries include

1. the users of e-commerce protocols
2. industries involved with e-commerce
3. researchers on formal methods for security

2 D. Dissemination and Exploitation

The work will consist of the SET analysis and a few smaller case studies. The resulting Isabelle theories and proof scripts will be distributed via the Internet. The models and findings will be described in journal and conference papers, and in lectures. New versions of Isabelle will be released periodically.

Paulson runs a course every couple of years, training researchers and industrialists in the use of Isabelle. He also supervises a steady stream of visitors, typically PhD students who stay for several months.

2 E. Justification of Resources

Staff

Paulson will work part-time directing the project. He proposes to employ one full-time research assistant who will carry out the major part of the workplan. Giampaolo Bella is available to fill this post. He would make an ideal appointment because of his extensive previous experience in protocol verification [1, 3] and, above all, his previous work on the SET protocol [2].

Travel and Subsistence

Conference attendance is essential to keep abreast of developments and to disseminate results. We are requesting funds to attend some of the main conferences. We may wish to attend relevant workshops at Schloß Dagstuhl and elsewhere. We are also requesting funds for visits to other institutions, as detailed on the application form.

Equipment

Isabelle is computationally demanding. We request a Linux-based workstation with 256MB of RAM. Tests have shown the 700MHz AMD Athlon processor to be an excellent Isabelle platform. Bella often works at home and while travelling,

so a good laptop (Toshiba Portege) is specified for his use. We also request a disc for storing large Isabelle images.

We include standard costs towards Laboratory computing infrastructure: filing systems, e-mail, etc., at £1750 per year. We request £440 consumables per year for toner cartridges, paper, backup tapes, workshop supplies, etc.

References

[1] Giampaolo Bella. Modelling security protocols based on smart cards. In Manuel Blum and C. H. Lee, editors, *Cryptographic Techniques and E-Commerce (CrypTEC'99)*, pages 139–146. City University of Hong Kong Press, 1999.

[2] Giampaolo Bella, Fabio Massacci, Lawrence C. Paulson, and Piero Tramontano. Formal verification of card-holder registration in SET. Technical Report 488, CUCL, 2000.

[3] Giampaolo Bella and Lawrence C. Paulson. Kerberos version IV: Inductive analysis of the secrecy goals. In Quisquater et al. [11], pages 361–375.

[4] Dominique Bolignano. Towards the formal verification of electronic commerce protocols. In *10th Computer Security Foundations Workshop*, pages 113–147. IEEE Computer Society Press, 1997.

[5] Stephen Brackin. Automatic formal analysis of two large commercial protocols. In Hilarie Orman and Catherine Meadows, editors, *Workshop on Design and Formal Verification of Security Protocols*. DIMACS, September 1997.

[6] Volker Kessler and Heike Neumann. A sound logic for analysing electronic commerce protocols. In Quisquater et al. [11], pages 345–360.

[7] Gavin Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using CSP and FDR. In T. Margaria and B. Steffen, editors, *Tools and Algorithms for the Construction and Analysis of Systems: second international workshop, TACAS '96*, LNCS 1055, pages 147–166. Springer, 1996.

[8] Lawrence C. Paulson. *Isabelle: A Generic Theorem Prover*. Springer, 1994. LNCS 828.

[9] Lawrence C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6:85–128, 1998.

[10] Lawrence C. Paulson. Inductive analysis of the Internet protocol TLS. *ACM Transactions on Information and System Security*, 2(3):332–351, August 1999.

[11] J.-J. Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann, editors. *Computer Security — ESORICS 98*, LNCS 1485. Springer, 1998.

[12] RSA Laboratories. *PKCS-7: Cryptographic Message Syntax Standard*, 1993. Available electronically at `http://www.rsasecurity.com/rsalabs/pkcs`.

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

[14] SETCo. *SET Secure Electronic Transaction Specification: Formal Protocol Definition*, May 1997. Available electronically at `http://www.setco.org/set_specifications.html`.

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

[16] Vitaly Shmatikov and John C. Mitchell. Analysis of a fair exchange protocol. In Nevin Heintze and Edmund Clarke, editors, *Formal Methods and Security Protocols*, 1999.

3 Diagrammatic project plan

The workplan allows two months for getting started. Then comes the first pass over the SET protocol. Two months are allowed for each of the five phases of SET. The second pass, in which deeper properties are proved, again allows two months per phase. Obviously, these are rough estimates: for instance, we have already made a start on the card-holder registration phase.

The remaining time is allotted to examining other e-commerce protocols. Isabelle development and maintenance continues throughout the 36 months.