Soundness Limits of Dolev-Yao Models

Michael Backes, Birgit Pfitzmann, Michael Waidner

Soundness Limits of Dolev-Yao Models

Michael Backes[1], Birgit Pfitzmann[2], and Michael Waidner[3]

[1] Saarland University, Saarbrücken, Germany, backes@cs.uni-sb.de
[2] IBM Research, Rueschlikon, Switzerland, bpf@zurich.ibm.com
[3] IBM Software Group, Somers, USA, wmi@us.ibm.com

Abstract. Automated tools such as model checkers and theorem provers for the analysis of security protocols typically abstract from cryptography by Dolev-Yao models, i.e., they replace real cryptographic operations by term algebras. The soundness of Dolev-Yao models with respect to real cryptographic security definitions has received significant attention in the last years. Until recently, all published results were positive, i.e., they show that various classes of Dolev-Yao models are indeed sound with respect to various soundness definitions.
Here we discuss impossibility results. In particular, we present such results for Dolev-Yao models with hash functions, and for the strong security notion of blackbox reactive simulatability (BRSIM)/UC. We show that the impossibility even holds if no secrecy (only collision resistance) is required of the Dolev-Yao model of the hash function, or if probabilistic hashing is used, or certain plausible protocol restrictions are made. We also survey related results for XOR. In addition, we start to make some impossibility results explicit that tacitly underly prior soundness results in the sense of motivating unusual choices in the Dolev-Yao models or the realizations. We also start to discuss which of the problems known for BRSIM/UC soundness extend to weaker soundness notions.

1 Dolev-Yao Models

Tools for proving security protocols typically abstract from cryptography by deterministic operations on abstract terms and simple cancellation rules. An example term is $\mathsf{E}_{pke_w}(\mathsf{hash}(\mathsf{sign}_{sks_u}(m, N_1), N_2))$, where m denotes a payload message and N_1, N_2 two nonces, i.e., representations of fresh random numbers. We wrote the keys as indices only for readability; formally they are normal operands in the term. A typical cancellation rule is $\mathsf{D}_{ske}(\mathsf{E}_{pke}(m)) = m$ for corresponding keys. The proof tools handle these terms symbolically, i.e., they never evaluate them to bitstrings. In other words, the tools perform abstract algebraic manipulations on trees consisting of operators and base messages, using only the cancellation rules, the message-construction rules of a particular protocol, and abstract models of networks and adversaries. Such abstractions, although different in details, are collectively called Dolev-Yao models after their first authors [15].

While Dolev-Yao models are no longer the only way of treating cryptography in automated tools, they are likely to remain important where they are applicable because of the strong simplification they offer to the tools, which enables the tools

to treat larger overall systems automatically than with more detailed models of cryptography.

2 Soundness Results

It is not obvious that a proof in a Dolev-Yao model implies security with respect to real cryptographic definitions. However, in the last years significant progress was made in showing that this is true in many cases. Early results considered passive attacks only [2, 1, 17]. The first result that allows active attacks [7] and thus the typical Dolev-Yao adversary model immediately used a very strong notion of soundness, blackbox reactive simulatability/UC [21, 22, 12]. This notion essentially means that a "real system", here the realization, can be plugged in for an "ideal system", here the Dolev-Yao model, safely in arbitrary environments. The result in [7] is also strong in allowing multiple cryptographic primitives. However, it makes some relatively unusual choices and one first-time addition in its Dolev-Yao model and needs additional type tagging and randomization in the realization. The result was extended to more cryptographic primitives in [8, 4] with increasing extensions to the Dolev-Yao models. General results on property preservation through the BRSIM notion imply certain other soundness notions for the same Dolev-Yao model and realization [21, 3], and additional specific soundness properties were proved in [6]. Stronger links to conventional Dolev-Yao-style type systems were provided in [19], and an integration into the Isabelle/HOL theorem prover in [23].

Later papers such as [20, 18, 13] define weaker soundness notions, such as integrity only or offline mappings between runs of the real and ideal systems, and/or allow less general protocol classes, e.g., only a specific class of key exchange protocols. For these cases, they can use simpler Dolev-Yao models and/or realizations than [7].

All the results about linking Dolev-Yao models and cryptography mentioned so far are essentially positive, i.e., soundness in some sense is shown. Furthermore, they concentrate on core cryptographic systems such as encryption and signatures; they do not contain hash or one-way functions, nor operations with algebraic properties such as XOR, although such operations exist in the Dolev-Yao models of many automated tools. Our work on impossibility was motivated by trying to add XOR and hashing to the BRSIM/UC soundness results, and being unsuccessful even if we were willing to make very significant changes or restrictions to the Dolev-Yao model, the protocol class using it, or the implementation.[4]

[4] We do obtain BRSIM/UC-style soundness, e.g., for hashing in the random oracle model and for XOR in the passive case. However, we do not find these positive results fully satisfying. Results that make similar strong restrictions while not even aiming at BRSIM/UC soundness were also obtained in [10, 16].

3 Impossibility Results

Given the state of the art of Dolev-Yao soundness results, it is interesting to consider impossibility results. For instance, one may ask the following questions:

- Is it really not possible to show soundness for hashes and XOR (and probably further related primitives) in the same strong BRSIM/UC sense as for encryption and signatures?
- In cases where positive results exist both for BRSIM/UC soundness and weaker soundness, with simpler systems in the latter case, is this an unavoidable tradeoff?
- Where positive results exist only for restricted protocol classes, or simpler results than in the general case, are all the restrictions really needed to achieve these results?

While we do not claim to have the final answer to all these questions, we can present a number of results.

3.1 Hashes

In particular, we present answers to the first question for hash functions. We first show that it is indeed impossible to realize the standard Dolev-Yao model of hashing with standard cryptographic hash functions in the sense of BRSIM/UC. However, we can go significantly further. In particular, we show impossibility even if we give up the secrecy of hashed messages in the Dolev-Yao model (leaving only collision resistance – this is a reasonable possibility in Dolev-Yao models). We also show impossibility if probabilistic hashing [11, 14] is used as the realization; this cryptographic primitive offers better secrecy than deterministic hashing and can sometimes be used instead of random oracles where deterministic hashing cannot. Moreover, we discuss that many plausible restrictions of the protocol classes do not help, although for some very strong restrictions we do achieve BRSIM/UC again.[5] (These results will be published as [9]; the report version does not yet contain the results on probabilistic hashing.)

3.2 XOR

We also give a survey on similar results for XOR from [5]. Furthermore, we give a short introduction into how one can set up impossibility proofs that hold across the multitude of significantly different rigorous definitions of Dolev-Yao models in the literature.

[5] This is also a little surprising as one of these restrictions allows standard ideal Dolev-Yao style secrecy and uses standard deterministic hash functions, i.e., the "canonical" setting. However, here only individual nonces (i.e., cryptographic objects with no other purpose, in contrast to payloads, keys, ciphertexts, etc.) can be hashed. Thus essentially only one-time signatures can be produced. Then even BRSIM/UC soundness for the Dolev-Yao model does not require secrecy of the individual bits of the real nonces.

3.3 Encryption and Authentication

Furthermore, for the first time we start surveying existing informal answers to the second and third question above and to make them more rigorous. Some issues concerned are the following: the leakage of the message length through encryptions, the need to make probabilistic encryption and signatures explicit in the Dolev-Yao model through a freshness construct on the respective term type, the need to additionally randomize certain realizations because of potential problems with adversary-chosen keys, and the possibility that symmetric authentications or ciphertexts are valid with respect to several adversary keys.

We also identify gaps where no such answers exist yet, and hope to stimulate discussions and future work on those.

Acknowledgments. We thank Martín Abadi, Véronique Cortier, Anupam Datta, Ante Derek, Cathy Meadows, John Mitchell, and Andre Scedrov for interesting discussions. This work is partially supported by the European Commission through the IST Programme under Contract IST-4-026764-NOE ReSIST.

References

1. M. Abadi and J. Jürjens. Formal eavesdropping and its computational interpretation. In *Proc. 4th TACS*, pages 82–94, 2001.
2. M. Abadi and P. Rogaway. Reconciling two views of cryptography: The computational soundness of formal encryption. In *Proc. 1st IFIP TCS*, volume 1872 of *LNCS*, pages 3–22. Springer, 2000.
3. M. Backes and B. Pfitzmann. Computational probabilistic non-interference. In *Proc. 7th European Symp. on Research in Computer Security (ESORICS)*, volume 2502 of *LNCS*, pages 1–23. Springer, 2002.
4. M. Backes and B. Pfitzmann. Symmetric encryption in a simulatable Dolev-Yao style cryptographic library. In *Proc. 17th IEEE CSFW*, pages 204–218, 2004.
5. M. Backes and B. Pfitzmann. Limits of the cryptographic realization of Dolev-Yao-style XOR. In *Proc. 10th ESORICS*, volume 3679 of *LNCS*, pages 178–196. Springer, 2005.
6. M. Backes and B. Pfitzmann. Relating symbolic and cryptographic secrecy. *IEEE Transactions on on Dependable and Secure Computing*, 2(2):109–123, 2005.
7. M. Backes, B. Pfitzmann, and M. Waidner. A composable cryptographic library with nested operations. In *Proc. 10th ACM CCS*, pages 220–230, 2003.
8. M. Backes, B. Pfitzmann, and M. Waidner. Symmetric authentication within a simulatable cryptographic library. In *Proc. 8th ESORICS*, volume 2808 of *LNCS*, pages 271–290. Springer, 2003.
9. M. Backes, B. Pfitzmann, and M. Waidner. Limits of the Reactive Simulatability/UC of Dolev-Yao models with hashes. In *Proc. 11th ESORICS*, LNCS. Springer, 2006. To appear. Preliminary version IACR Cryptology ePrint Archive 2006/068, http://eprint.iacr.org/.
10. M. Baudet, V. Cortier, and S. Kremer. Computationally sound implementations of equational theories against passive adversaries. In *Proc. 32nd Intern. Colloquium on Automata, Languages and Programming (ICALP)*, volume 3580 of *LNCS*, pages 652–663. Springer, 2005.

11. R. Canetti. Towards realizing random oracles: Hash functions that hide all partial information. In *Proc. CRYPTO 97*, pages 455–469. Springer, 1997.
12. R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proc. 42nd IEEE FOCS*, pages 136–145, 2001.
13. R. Canetti and J. Herzog. Universally composable symbolic analysis of mutual authentication and key exchange protocols. In *Proc. 3rd Theory of Cryptography Conf. (TCC)*, pages 380–403. Springer, 2006.
14. R. Canetti, D. Micciancio, and O. Reingold. Perfectly one-way probabilistic hash functions. In *Proc. 30th ACM STOC*, pages 131–140, 1998.
15. D. Dolev and A. C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.
16. F. D. Garcia and P. van Rossum. Sound computational interpretation of formal hashes. IACR Cryptology ePrint Archive 2006/014, Jan. 2006.
17. P. Laud. Semantics and program analysis of computationally secure information flow. In *Proc. 10th European Symp. on Programming (ESOP)*, pages 77–91, 2001.
18. P. Laud. Symmetric encryption in automatic analyses for confidentiality against active adversaries. In *Proc. 25th IEEE Symp. on Security & Privacy*, pages 71–85, 2004.
19. P. Laud. Secrecy types for a simulatable cryptographic library. In *Proc. 12th ACM CCS*, pages 26–35, 2005.
20. D. Micciancio and B. Warinschi. Soundness of formal encryption in the presence of active adversaries. In *Proc. 1st Theory of Cryptography Conf. (TCC)*, volume 2951 of *LNCS*, pages 133–151. Springer, 2004.
21. B. Pfitzmann and M. Waidner. Composition and integrity preservation of secure reactive systems. In *Proc. 7th ACM CCS*, pages 245–254, 2000.
22. B. Pfitzmann and M. Waidner. A model for asynchronous reactive systems and its application to secure message transmission. In *Proc. 22nd IEEE Symp. on Security & Privacy*, pages 184–200, 2001.
23. C. Sprenger, M. Backes, D. Basin, B. Pfitzmann, and M. Waidner. Cryptographically sound theorem proving. In *Proc. 19th IEEE CSFW*, 2006. To appear.