

JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Foreword

Jean Goubault-Larrecq
Guest Editor

Security is a very old concern, which until rather recently was mostly of interest in military or diplomatic circles, and therefore of rather limited interest to the public at large. The deployment of electronic commerce changed this drastically. This started notably with the advent of computerized communication in the 1970s, and with *smart cards* in the 1980s. Smart cards are really computers on a chip, and need to engage in securized dialogues with cash dispensers, payment terminals or other computer equipment. While this certainly made the concern for security more widespread, notably in the computer and telecommunications industry, it was certainly the hype around Internet and so-called e-commerce – electronic commerce over the World-Wide Web – of the late 1990s that made the notion of security, and in particular of cryptology and cryptographic protocols, a fundamental issue in computers and networks.

One fundamental concern in security is *secrecy*: how do you send a message to a remote friend in such a way that no spy can read it? This led to the art of *cryptography*. Soon other concerns came in, for example *authenticity*: how can your friend be sure that the message he got was indeed created by you, and not forged by a spy? Also, *integrity*: not only should the message originate from you, but it should not have been tampered with or otherwise modified. Also, *freshness*: the message should come from you, but it should also be recent, and not be a replay of some old message that you sent in ancient times.

Many *encryption* schemes have been devised over the years, from simple permutations of letters to modern algorithms like DES or RSA, or even based on number-theoretic or group-theoretic considerations. Cryptography also expanded its scope, and it was then recognized that not only strong encryption schemes, but also cryptographically secure pseudo-random generators, strong hash functions, and a few other constructs were needed. For a long time, it was believed that designing such strong encryption, random number generation or hashing schemes, was sufficient to ensure secure message exchanges.

Starting from the 1980s, researchers understood that even with perfect encryption schemes, message exchanges were still not necessarily secure. This led to the notion that *cryptographic protocols*, i.e., specified sequences of exchanges of messages, had to be verified and proved before they could be trusted. Although most attacks against cryptographic protocols are relatively trivial, it turned out to be rather difficult to find such attacks, or to be sure that there are none. A case in point is Needham and Schroeder's public-key protocol of 1978 [6], which was discovered flawed 17 years later only, by Gavin Lowe [3].

This issue is dedicated to models and methods for assessing computer security, with a strong emphasis on security of cryptographic protocols. Here is a brief synopsis of the papers in this issue.

Comon-Shmatikov. Hubert Comon and Vitaly Shmatikov survey formal models of cryptographic protocols, comparing the assumptions behind these models, and their respective scopes. These models are the ones that are in use today, and assume perfect cryptographic primitives. Some of them lend themselves to automation. In particular, Hubert Comon and Vitaly Shmatikov discuss decidability issues for cryptographic protocol verification in these settings.

Millen-Denker. One very successful family of models for cryptographic protocols is the so-called Dolev-Yao family of models. A number of automated tools exists that aim at verifying, or finding attacks on cryptographic protocols, based on such models. They include Cathy Meadows' NRL [5], Gavin Lowe and Bill Roscoe's CSP model checker FDR [4] applied to cryptographic protocols, or Jon Millen's CAPSL language, among others. CAPSL is a generic language for describing cryptographic protocols, designed to be interfaced with several verification tools. The architecture and goals of CAPSL are described in this issue by Jon Millen and Grit Denker. They proceed to describe a new extension of CAPSL, μ CAPSL, which provides a basis for describing broadcast protocols, such as Diffie-Hellman group authentication – an important topic, although rarely addressed until now.

Boreale-Gorla. Another model for cryptographic protocols stems from process algebra, starting with Martin Abadí and Andrew Gordon's spi-calculus. Principals and intruders are both modeled as processes. A number of classical tools for process analysis – bisimulation, reachability analysis – can be adapted to the cryptographic setting. However this is not trivial, and there are at least two ways that cryptographic properties can be specified and checked on processes. One way is to specify security properties as *indistinguishability*: e.g., a message is secret provided no intruder process can tell the difference between you working with the secret and you working with some other data. Another is *unreachability*: e.g., a message is secret provided you cannot reach a state where the Dolev-Yao intruder knows it. Michele Boreale and Daniele Gorla explore both points of view, and give the basic principles of an automatic cryptographic protocol checker called STA. Note that, surprisingly, the two viewpoints on security are in fact distinct and incomparable.

Pointcheval. David Pointcheval expounds the point of view of the cryptologist, for whom cryptographic primitives are only good up to some probabilistic extent, and assuming complexity-theoretic assumptions. This provides more detailed models than the ones described by Hubert Comon and Vitaly Shmatikov, but are less easily automated. Nonetheless these models provide finer information on the security of cryptographic primitives and protocols. David Pointcheval explains why not every notion of security is relevant here, and proposes a realistic notion of so-called *practical security* for cryptographic protocols.

Monniaux. A popular way of specifying and evaluating the security of cryptographic protocols, starting from a famous paper by Michael Burrows, Martin Abadí, and Roger Needham [1], was the family of cryptographic logics, including BAN and GNY [2]. These logics have been highly criticized since their inception. However, they formalize intuitive reasoning about beliefs of principals in cryptographic protocols. It is widely, but wrongly believed that there is no way we can decide whether a formula in these logics is valid or not. David Monniaux describes the principles behind these logics, and shows why most of these logics are actually decidable, by giving terminating decision algorithms.

Goré-Thê Nguyễn. Finally, Rajeev Prabhakar Goré and Phuong Thê Nguyễn address the problem of verifying security properties on smart cards. The emphasis here is not so much on security of *data*, in a fixed-code architecture, rather on security in the presence of *mobile code*. The authors survey methods for enforcing security of mobile code, which goes drastically further than plain cryptographic protocols. Then they give a proof-of-principle algorithm for proof search in the modal logic S4, which works on a smart card. This is a *tour de force*, considering how little memory smart card applications have at their disposal. The practical end goal is to enable smart card operating systems to check the conformance of downloaded applications to specific security policies expressed in modal logics in the style of BAN. This will be needed more and more in the future: not just data, but roaming programs must be checked for security.

The domain of computer security and cryptographic protocols is relatively large, and keeps growing. Furthermore, the computer industry is gradually integrating the notion of security in every aspect of computer-related activities. The papers in this issue provide a snapshot of the state of the art in the domain of methods for verifying cryptographic protocols as of 2002, and tries to be as comprehensive as possible. There is no doubt that the domain will flourish in the next years, providing exciting new perspectives.

Acknowledgments

Partially supported by the RNTL project EVA ("Explication et Vérification Automatique de protocoles cryptographiques"), the ACI jeunes chercheurs "Sécurité informatique, protocoles cryptographiques et détection d'intrusions", and the ACI Cryptologie "Psi-Robuste".

References

- [1] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication", *Proc. Roy. Soc.*, vol. 426(1871), pp. 233–271, 1989.
- [2] L. Gong, R. Needham, and R. Yahalom, "Reasoning about belief in cryptographic protocols", in *IEEE Symp. Res. Secur. Priv.*, 1990, pp. 234–248.
- [3] G. Lowe, "An attack on the Needham-Schroeder public-key protocol", *Inform. Proc. Lett.*, vol. 56, no. 3, pp. 131–133, 1995.
- [4] G. Lowe and B. Roscoe, "Using CSP to detect errors in the TMN protocol", *IEEE Trans. Softw. Eng.*, vol. 23, no. 10, pp. 659–669, 1997.

- [5] C. Meadows, "The NRL protocol analyzer: an overview", *J. Log. Program.*, vol. 26, no. 2, pp. 113–131, 1996.
- [6] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers", *Commun. ACM*, vol. 21, no. 12, pp. 993–999, 1978.



Jean Goubault-Larrecq was born in Rouen, France, in 1965. He studied at École Polytechnique, then at the Corps des Mines; he received his Ph.D. degree from École Polytechnique in 1993 and his habilitation in 1997. He worked at the research center of Bull S.A. for ten years, was an invited researcher at the University of

Karlsruhe in 1996, worked as a research engineer then project director at Dyade, a common technology transfer venture between Bull and INRIA, from 1996 to 2000. He is currently the full-time professor of computer science at the ENS Cachan, and head of the SECSI (SECu-rité des Systèmes d'Information) project at INRIA Futurs. His research domains include automated deduction, formal specification, models and methods for cryptographic protocols, intrusion detection, proof theory and modal logics, and algebraic topological methods in computer science.

e-mail: goubault@lsv.ens-cachan.fr

LSV/CNRS UMR 8643

and ENS Cachan ENS Cachan

61, avenue du président-Wilson

F-94235 Cachan Cedex

France