Formal Techniques for Information and Software Security: An Annotated Bibliography

Bart De Win *Bart Jacobs* *Wouter Joosen*
Gregory Neven *Frank Piessens*
Tine Verhanneman

Report CW 423, September 14, 2005

Katholieke Universiteit Leuven
Department of Computer Science
Celestijnenlaan 200A – B-3001 Heverlee (Belgium)

Formal Techniques for Information and Software Security: An Annotated Bibliography

Bart De Win *Bart Jacobs* *Wouter Joosen*
Gregory Neven *Frank Piessens*
Tine Verhanneman

Report CW 423, September 14, 2005

Department of Computer Science, K.U.Leuven

Abstract

This report is the result of an extensive literature survey performed by its authors. Our goal is to provide an overview of existing formal approaches to information and software security. A rough classification of the topics covered in the research literature and brief descriptions of these topics should help the reader find his or her way in the substantial body of research.

Keywords : software security, information security, formal methods.

1 Introduction

This document is the result of a literature survey done in the context of the SoBeNet project[1]. We survey solution techniques for information and software security, and focus specifically on formal, mathematical approaches because only techniques with such a formal foundation allow for provable claims about certain security aspects.

Any formal approach to security must be based on a formal description of the power of attackers. One must define precisely what an attacker is capable of in order to be able to prove that a system is secure (in some sense) against that attacker.

An important distinction is whether one considers attackers that manipulate "raw bits", i.e. attackers that have access to the physical representation of information, for instance because they control a communication line, or because they can steal a harddisk. We classify approaches that deal with such attackers under the heading *information security*, and treat them in section 2.

Under the heading *software security*, section 3 deals with the scenario where attackers interact with valuable resources through some software layer. In most works surveyed under that section, the formal model of the attacker is more implicit.

2 Information Security

Information security is achieved by means of *cryptography* [MvOV96]. Formal approaches to proving security properties of cryptographic primitives and protocols differ in their assumptions about the abilities of an attacker.

We distinguish between three important approaches. The most conservative approach is that of *information-theoretical security*, which avoids any assumptions that do not follow from the laws of Nature. This is of course a very strong notion of security, its main disadvantage being that only few schemes satisfy it, and many of those that do are completely impractical. The second approach we describe, *computational security*, builds on results in complexity theory and considers attackers to be probabilistic polynomial-time Turing machines. Security proofs under this approach rely on widely-believed but unproven assumptions such as the intractability of some mathematical problem, or on the existence of a very basic primitive such as one-way functions. The third approach, *formal security*, states assumptions about the abilities of attackers in some kind of formal system. A very promising feature of this approach is that it may allow for automated

[1]The SoBeNeT project is an IWT-SBO project on the development of secure application software. See http://sobenet.cs.kuleuven.ac.be/ for more information about the project.

generation and verification of security proofs; the flip side however is that it takes a very high (and arguably unrealistic) level of abstraction from basic cryptographic primitives such as encryption and signature schemes. Lastly, we will discuss some recent attempts to bridge the computational and formal approaches.

2.1 Information-Theoretical Security

Information-theoretical security is often referred to as *unconditional* security, which is a slightly misleading term as it seems to imply that it not based on any assumptions at all. This is not completely true, as it is hard to imagine cryptography in a world where for example true randomness doesn't exist, or where secrets cannot be kept hidden from an adversary [DM04]. Information-theoretical cryptography, however, does not impose bounds on the computational power of the adversary and does not rely on the unproven hardness of certain mathematical problems.

Shannon pioneered the field of information theory during the second world war, but his revolutionary results were only published afterwards [Sha48]. He was the first to understand how the amount of information (or *entropy*) contained in a message can be measured, and later applied it to cryptography [Sha49] by defining *perfect secrecy* of a cipher as the property that without the secret key, the ciphertext contains no information about the original plaintext at all.

Shamir's secret sharing scheme [Sha79] is one of the few practical information-theoretically secure cryptographic primitives.

More practical schemes are obtained by adding extra assumptions that seem to be true in the physical world that surrounds us, e.g. the availability of noisy channels [Wyn75, CK78, Mau93], limitations on the adversary's memory[Mau92, CM97], or Heisenberg's uncertainty principle in quantum mechanics [Wie83, BBB$^+$92]. An overview of information-theoretical cryptography was written by Maurer [Mau99]. An overview of cryptography based on noisy channels is due to Wolf [Wol99].

Overall, information-theoretical cryptography provides the strongest security guarantees, but most schemes are so impractical that they can only be used in extremely high-security environments.

2.2 Computational Security

Computational security makes assumptions about the computational power of attackers, and about the computational hardness of certain mathematical problems, often called *primitives*. A typical example is the problem of factoring large numbers.

The early eighties saw the introduction of the approach of *provable security* [BM82, Yao82, GM84], sometimes more appropriately called *reduc-*

tionist security, which was further brought to practice during the nineties [Bel98]. The idea of provable security is to provide, along with a scheme, a mathematical proof showing that any attack on the scheme can be transformed into an attack on an underlying primitive or mathematical problem, thereby directly tying the security of the scheme to the security of its building blocks.

Obviously, such security proofs are relative to their assumptions: if building quantum computers becomes feasible, the assumption that factoring large numbers is hard ceases to be realistic. Moreover, any security proof needs to make assumptions about the information that an attacker can gather, and does not provide any guarantees against adversaries that break these assumptions. Good examples of such attacks are timing [Koc96] and power analysis [KJJ99] attacks, where the adversary extracts additional information by carefully measuring the time or energy required to perform cryptographic operations.

2.2.1 Security Notions

Before anything useful can be said about the security of a scheme, it must be made perfectly clear what is understood under its security. This is captured by the *security notion* associated to the primitive, which is usually described in terms of a game or experiment. The adversary, modelled as a probabilistic algorithm, is given certain inputs and has access to certain oracles, and is challenged to create an output that is considered "offending" to the scheme.

Deciding on a suitable security notion that is strong enough to be meaningful for practical purposes, yet weak enough to be achievable by real-world schemes, is an important and time-consuming task that should not be underestimated. Security notions may take a long time to crystallize, and in fact it is not uncommon for multiple notions to exist (and have good reason for their existence) in parallel. Public-key encryption for example has an extended history of suggested adversarial goals and attack models, ranging from indistinguishability of ciphertexts under chosen-plaintext attack [GM84], non-adaptive chosen-ciphertext attack [NY90] and adaptive chosen-ciphertext attack; over non-malleability of ciphertexts [DDN91] under the same sorts of attack [DDN91, DDN95, DDN00]; to the very high-level concept of plaintext awareness [BR98]. After the publication of relations among these notions [BDPR98], the community seemed to settle with indistinguishability under adaptive chosen-ciphertext attack as the "holy grail" for public-key encryption, although Canetti et al. [CKN03] recently suggested to slightly loosen the definition again.

2.2.2 Theoretical Results

The goal of this research track is to find minimal assumptions (or separation results) for existence of cryptographic primitives. Common assumptions are existence of (trapdoor) one-way functions and permutations. E.g., it is known that if one-way functions exist, then so do families of pseudo-random functions [GGM86], pseudo-random permutations [LR88] (and hence block ciphers), signature schemes [Rom90], pseudo-random generators [HILL99] and commitment schemes [Nao91, HILL99].

2.2.3 Idealizations for Practical Schemes

THE RANDOM ORACLE MODEL. Motivated by the lack of provably secure constructions that were efficient enough to replace heuristic schemes in use around the mid-nineties, Bellare and Rogaway [BR93] suggested the *random oracle model* as a compromise between theory and practice, sacrificing a piece of provable security to buy efficiency. They used this paradigm to prove the security of their OAEP (Optimal Asymmetric Encryption Padding) [BR98, Sho02] and PSS (Probabilistic Signature Scheme) schemes [BR96]. These are just as efficient as the heuristic schemes in use at the time, and gradually made their way into industrial standards such as PKCS#1 and IEEE P1363. The random oracle model has since been used in numerous security proofs throughout the literature.

The idea of the random oracle model is to prove security in an imaginary model where all algorithms, including the adversary, have access to an oracle that implements a random function, meaning that images are independently and uniformly distributed over the domain of the function. When implemented in practice, the random oracle is replaced with a "good" cryptographic hash function. The hash functions are hoped to sufficiently mimic the unpredictable behavior of a random oracle to preserve security in the real world.

A lot of controversy exists about the true value of security proofs in the random oracle model, and indeed, they should be treated with care. Assuming hash functions to behave like random oracles is not just a strong assumption, it is plainly false: obviously, no efficiently computable function can ever be assumed to be unpredictable. Moreover, critiques have been found separating the random oracle model from the standard model. Canetti, Goldreich and Halevi [CGH98] designed (contrived) encryption and signature schemes that are secure in the random oracle model, but that are insecure when the random oracle is instantiated with *any* function ensemble. Later, Nielsen [Nie02] showed that the problem of non-interactive non-committing encryption has no solution in the standard model, while it has a simple solution in the random oracle model. Goldwasser and Tauman [GK03] demonstrated the existence of a (contrived) identification scheme

for which the Fiat-Shamir transform produces an insecure signature scheme when the random oracle is instantiated with *any* function ensemble. The Fiat-Shamir transform [FS86] converts a class of identification schemes into signature schemes and was proven to be security-preserving in the random oracle model [PS00, AABN02]. Recently, a random oracle-using solution for the quite natural problem of cca-preserving asymmetric encryption was found to be uninstantiable [BBP04]. While the proposed scheme is quite natural, it has to be instantiated with a contrived symmetric encryption scheme to come to a contradiction.

The generic group model The generic group model [Nec94, Sho97] idealizes the group structure of an algebraic group: the adversary only has access to random encodings for group elements and has oracle access to the group operation, so it cannot use tricks particular to one type of groups. Discrete logs, CDH and DDH are provably exponentially hard in these groups, active security of Schnorr identification scheme can be proven in this model. Other schemes proven in this model include [SJ00, Bro02], but separation results similar to those of random oracle model exist [Den02].

The ideal cipher model replaces a block cipher by a family of truly random and independent permutations [BR02]. It is even richer (i.e. less realistic) than the random oracle model. Schemes proven secure in this model include Schnorr identification [BR02] and password-based authenticated key exchange [BPR00].

2.2.4 Universal Composability

Universal Composability is a model proposed by Canetti [Can01] where security remains guaranteed even when it is composed with an arbitrary set of protocols, and when an unbounded number of protocol instances are executed concurrently in an adversarially controlled manner. Traditionally, cryptographic primitives are seen as stand-alone problems. The UC framework also inspects the security of a single, stand-alone execution of the protocol, but the framework guarantees preservation of security when the protocol is run in complex settings where a protocol instance may be run concurrently with many other protocol instances, on potentially related inputs and in an adversarially controlled way.

Universally composable protocols exist for a number of protocol problems, including message authentication [BCK98, Can01], key exchange [CK01] and digital signatures [BH03].

2.3 Formal Security

In this approach, certain abstract assumptions are made about existing cryptographic primitives, and under these assumptions protocols based on these

primitives are shown to be secure. The most widely used set of assumptions was first articulated by Dolev and Yao [DY83], and is known as the Dolev-Yao model.

The idea of formalizing these assumptions in some kind of formal system was pioneered by Burrows, Abadi and Needham [BAN89]. Their BAN-logic is a belief logic that formalizes what participants can believe at each stage of a protocol execution. It spawned a very succesful research track, where many variants of their logic were proposed [GNY90, AT91, vO93, SvO96], and these logics were successful in finding flaws in real protocols. However, the abstractions made in the formalization are sometimes irrealistic, and some practical protocols that are provably secure in such logics were later found to be insecure [Low96, Pau98].

Next to belief logics, process calculi [Hoa85, Sch97] were used as a formalism for proving properties of protocol under Dolev-Yoa-like assumptions. The succesful SPI calculus [AG97, AG99] is an extension of the π-calculus with operations for cryptographic primitives. Security is defined through equivalence of two protocol specifications from viewpoint of adversary.

A good overview of the field of formal protocol security is given by Paul Syverson [SC01].

2.4 Bridging the Computational and Formal Approaches

Abadi and Rogaway [AR00, AJ01, AR02] pioneered the idea of relating the computational and formal approaches. They provided a computational justification for a formal treatment of symmetric-key encryption, by relating formal *equivalence* to computational *indistinguishability*. While Abadi and Rogaway only considered the security of encryption against passive adversaries, the idea of relating computational and formal approaches has attracted much attention, and very recent results also deal with active adversaries and other security primitives [MW04, BPW03, BPW04].

3 Software Security

Software security is about making sure that a given software layer that manages certain valuable resources appropriately implements a specified security policy.

So very broadly speaking, software security is about correctness, about conformance of an implementation to a specification (where the specification is the security policy). Hence, any technology to improve software quality from that point of view is also security relevant. This includes general-purpose specification and verification techniques, as well as programming language technologies to ensure *safety* of a language. In this survey however, we restrict our attention to formal approaches that specifically focus on security.

We distinguish three such concerns in the following sections. Under the heading *access control*, we survey formal approaches to regulate access to valuable resources in multi-user systems. *Information flow* is about controlling the flow of information in a computer system. Finally, the section on *code access security* surveys techniques that limit the amount of damage that partially trusted pieces of code can cause. Obviously, there are strong connections between these three topics.

3.1 Access Control

Access Control is one of the oldest security concerns, and has been studied intensively since the early seventies. Most approaches start from Lampson's seminal access control model ([Lam74]). In this model, the software layer has notions of *objects* encapsulating resources, and *subjects* trying to access these resources. A *reference monitor* guards the access to objects, according to the current protection state represented by an access control matrix.

Key research questions that have been addressed include:

1. What are suitable policy models to formulate the exact policy that the reference monitor should enforce? Famous models include the Discretionary Access Control Model [oD83], the Mandatory Access Control Model [BL73, BL75], Role Based Access Control Models [SCFY96, FSG+01] and a variety of specific purpose systems [Bib77, CW87, BN89] or general purpose policy languages [JSS97]. Driving forces for this research line include expressivity of the model, suitability for modeling real-world policies, and manageability and composability of policies.

2. What kind of meta-questions can we answer for various models of the system? In order to answer the key question "Is the system secure?", one should model subjects and objects formally at a suitable level of abstraction. Such a model is called a *protection system*, and an interesting line of research has investigated a number of models, including the well-known Harrison-Ruzzo-Ullman model [HRU76], the Take-Grant model [BS79, JLS76, Bis84, Sny81], the Schematic Protection Model [San88, AS90], and the Typed Access Matrix model [San92]. These models provide insights in the algorithmic decidability of security.

Very good textbooks and surveys on the research on access control exist. The book by Matt Bishop [Bis03] and the surveys by Samarati et al. [dVPS03, SdV01] are good starting points.

3.2 Information Flow

Because of the large influence of the military on computer security research in the seventies, information flow policies have received a great amount of attention. The basic model was articulated by Denning [Den76]. Goguen and Meseguer [GM82] extended the idea to concurrent systems through the notion of *non-interference*. The Bell-LaPadula access control model [BL73] is a policy model for access control that attempts to capture information flow security. But information flow security can also be enforced by static verification of the programs that manipulate the information. The first formulation of this idea is again due to Denning [DD77], and recently there has been a whole new line of research that addresses information flow security by using static typing [HVY00, SV98, HR98, Mye99, MS01]. A good survey of this research track is given by Sabelfeld and Myers [SM03].

3.3 Code Access Security

As component-based development gained in popularity, the security issues of mixing more and less trusted components in a single application have attracted more and more attention. The issues of potentially malicious code sharing an address space with trusted code were first studied in the context of extensible operating systems under the name of Software Fault Isolation [WLAG93]. With the advent of Java and applets, mechanisms for sandboxing less trusted components became an important research track [WBDF97]. Java's mechanism of stack-inspection based sandboxing has received extensive attention [WF98, FG02, ES00, BN04]. Stack inspection has been studied formally [FG02], alternative mechanisms have been proposed [AF03], as well as type systems to ensure the absence of security exceptions [SS00, PSS01, PSS03].

The idea of Proof-Carrying Code [NL96, Nec97, App01] also originated in the field of extensible operating systems, and the idea of code (components) carrying their own formal security guarantees in checkable form has been studied intensively. Certifying compilation [Koz98, SMH01] compiles a safe high-level language to assembly code and the corresponding proof that the code satisfies the high-level safety properties.

The increasing importance of application-level security policies triggered interest in studying the formal properties of existing enforcement mechanisms [Sch00]. Various enforcement mechanisms [ES00, LBW04] have been studied, including the limits of what such mechanisms can enforce [HMS03].

4 Conclusion

Information and software security have been studied mainly in isolation. However, in distributed systems the interplay between cryptographic mech-

anism and software security mechanisms is crucial. While some seminal papers [ABLP93] have recognized this for a long time, and while state-of-the-art operating systems and middleware succesfully integrate information security and software security mechanisms, this has not yet been sufficiently addressed at the application level. Dealing with distribution and security at the level of, for instance, the programming language is an interesting and challenging research topic for the coming years.

References

[AABN02] Michel Abdalla, Jee Hea An, Mihir Bellare, and Chanathip Namprempre. From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In L. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 418–433. Springer-Verlag, April 2002.

[ABLP93] Martín Abadi, Michael Burrows, Butler Lampson, and Gordon Plotkin. A calculus for access control in distributed systems. *ACM Transactions on Programming Languages and Systems*, 15(4):706–734, September 1993.

[AF03] Martín Abadi and Cédric Fournet. Access control based on execution history. In *NDSS*, 2003.

[AG97] Martín Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: The spi calculus. In *Proceedings of the 4th Conference on Computer and Communications Security*, pages 36–47. ACM Press, 1997.

[AG99] Martín Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: The spi calculus. *Information and Computation*, 148(1):1–70, 1999. A preliminary version of this paper appeared as [AG97].

[AJ01] Martín Abadi and Jan Jürjens. Formal eavesdropping and its computational interpretation. In N. Kobayashi and B.C. Pierce, editors, *Theoretical Aspects of Computer Software (4th International Symposium, TACS '01)*, volume 2215 of *Lecture Notes in Computer Science*, pages 82–94. Springer-Verlag, 2001.

[App01] Andrew W. Appel. Foundational proof-carrying code. In *Proceedings of the 16th Annual IEEE Symposium on Logic in Computer Science*, page 247. IEEE Computer Society, 2001.

[AR00] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (The computational soundness of formal encryption). In J. van Leeuwen, O. Watanabe, M. Hagiya, P. D. Mosses, and T. Ito, editors, *Theoretical Computer Science, Exploring New Frontiers of Theoretical Informatics, International Conference IFIP TCS 2000*, volume 1872 of *Lecture Notes in Computer Science*, pages 3–22. Springer-Verlag, 2000.

[AR02] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (The computational soundness of formal encryption). *Journal of Cryptology*, 15(2):103–127, 2002.

[AS90] P. E. Ammann and R. S. Sandhu. Extending the creation operation in the schematic protection model. In *Sixth Annual Computer Security Applications Conference*, pages 340–348, 1990.

[AT91] Martín Abadi and Mark R. Tuttle. A semantics for a logic of authentication (extended abstract). In *10th ACM Symposium on Principles of Distributed Computing*, pages 201–216. ACM, 1991.

[BAN89] Michael Burrows, Martín Abadi, and Roger M. Needham. A logic of authentication. *Proceedings of the Royal Society of London, Series A*, 426:233–271, 1989. A preliminary version appeared as Research Report 39, Digital Systems Research Center, February 1989.

[BBB+92] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John A. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, 1992.

[BBP04] Mihir Bellare, Alexandra Boldyreva, and Adriana Palacio. An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 171–188. Springer-Verlag, 2004.

[BCK98] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols (extended abstract). In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 419–428. ACM Press, 1998.

[BDPR98] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In H. Krawczyk, editor, *Advances in Cryptology*

– *CRYPTO 1998*, volume 1462 of *Lecture Notes in Computer Science*, pages 26–45. Springer-Verlag, 1998.

[Bel98] Mihir Bellare. Practice-oriented provable security. In Eiji Okamoto, George I. Davida, and Masahiro Mambo, editors, *Proceedings of First International Workshop on Information Security (ISW 97)*, volume 1396 of *Lecture Notes in Computer Science*, pages 221–231. Springer-Verlag, 1998.

[BH03] Michael Backes and Dennis Hofheinz. How to break and repair a universally composable signature functionality. Cryptology ePrint Archive, Report 2003/240, 2003. `http://eprint.iacr.org/`.

[Bib77] K. J. Biba. Integrity considerations for security computer systems. Technical Report MTR-3153, MITRE Corp., Bedford, MA, 1977.

[Bis84] J. Biskup. Some variants of the take-grant protection model. *Information Processing Letters*, 19(3):151–156, 1984.

[Bis03] Matt Bishop. *Computer Security, Art and Science*. Addison Wesley, 2003.

[BL73] D. Bell and L. LaPadula. Secure computer systems, vol. I: Mathematical foundations and vol. II : A mathematical model. Technical Report MTR-2547, MITRE Corp., Bedford, MA, 1973.

[BL75] D. Bell and L. LaPadula. Secure computer system unified exposition and multics interpretation. Technical Report MTR-2997, MITRE Corp., Bedford, MA, July 1975.

[BM82] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo random bits. In IEEE, editor, *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, pages 112–117. IEEE Computer Society Press, 1982.

[BN89] David F. C. Brewer and Michael J. Nash. The chinese wall security policy. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 206–214. IEEE Computer Society Press, May 1989.

[BN04] Anindya Banerjee and David A. Naumann. Stack-based access control and secure information flow. *Journal of Functional Programming*, 2004. To appear.

[BPR00] Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 139–155. Springer-Verlag, 2000.

[BPW03] Michael Backes, Birgit Pfitzmann, and Michael Waidner. A composable cryptographic library with nested operations. In V. Atluri and T. Jaeger, editors, *Proceedings of the 10th Conference on Computer and Communications Security*, pages 220–230. ACM Press, 2003.

[BPW04] Michael Backes, Birgit Pfitzmann, and Michael Waidner. A general composition theorem for secure reactive systems. In M. Naor, editor, *First Theory of Cryptography Conference, TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 336–354. Springer-Verlag, 2004.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In ACM, editor, *Proceedings of the 1st Conference on Computer and Communications Security*, pages 62–73. ACM Press, November 1993.

[BR96] Mihir Bellare and Phillip Rogaway. The exact security of digital signatures - How to sign with RSA and Rabin. In U. Maurer, editor, *Advances in Cryptology – EUROCRYPT 1996*, volume 1070 of *Lecture Notes in Computer Science*, pages 399–416. Springer-Verlag, 1996.

[BR98] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In A. De Santis, editor, *Advances in Cryptology – EUROCRYPT 1994*, volume 950 of *Lecture Notes in Computer Science*, pages 92–111. Springer-Verlag, 1998.

[BR02] John Black and Phillip Rogaway. Ciphers with arbitrary finite domains. In B. Preneel, editor, *Topics in Cryptology – CT-RSA 2002*, volume 2271 of *Lecture Notes in Computer Science*, pages 114–130. Springer-Verlag, 2002.

[Bro02] Daniel R. L. Brown. Generic groups, collision resistance, and ecdsa. Cryptology ePrint Archive, Report 2002/026, 2002. `http://eprint.iacr.org/`.

[BS79] Matt Bishop and Lawrence Snyder. The transfer of information and authority in a protection system. In *Proceedings of the seventh ACM symposium on Operating systems principles*, pages 45–54. ACM Press, 1979.

[Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science*, pages 136–145. IEEE Computer Society Press, 2001.

[CGH98] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle model, revisited. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 209–218. ACM Press, 1998.

[CK78] Imre Csiszár and János Körner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24:339–348, 1978.

[CK01] Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In B. Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 453–474. Springer-Verlag, 2001.

[CKN03] Ran Canetti, Hugo Krawczyk, and Jesper Buus Nielsen. Relaxing chosen-ciphertext security. In D. Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 565–582. Springer-Verlag, 2003.

[CM97] Christian Cachin and Ueli M. Maurer. Unconditional security against memory-bounded adversaries. In B. Kaliski Jr., editor, *Advances in Cryptology – CRYPTO 1997*, volume 1294 of *Lecture Notes in Computer Science*, pages 292–306. Springer-Verlag, 1997.

[CW87] D. D. Clark and D. R. Wilson. A comparison of commercial and military computer security policies. In *Proceedings of the Symposium on Security and Privacy 1987*, pages 184–193. IEEE Press, 1987.

[DD77] Dorothy E. Denning and Peter J. Denning. Certification of programs for secure information flow. *Commun. ACM*, 20(7):504–513, 1977.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pages 542–552. ACM Press, 1991.

[DDN95] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. Technical Report CS95-27, Weizmann Institute of Science, 1995.

[DDN00] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. *SIAM Journal on Computing*, 30(2):391–437, 2000.

[Den76] Dorothy E. Denning. A lattice model of secure information flow. *Commun. ACM*, 19(5):236–243, 1976.

[Den02] Alexander W. Dent. Adapting the weaknesses of the random oracle model to the generic group model. In Y. Zheng, editor, *Advances in Cryptology – ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 100–109. Springer-Verlag, 2002.

[DM04] Stefan Dziembowski and Ueli M. Maurer. Optimal randomizer efficiency in the bounded-storage model. *Journal of Cryptology*, 17(1):5–26, 2004.

[dVPS03] Sabrina De Capitani di Vimercati, Stefano Paraboschi, and Pierangela Samarati. Access control: principles and solutions. *Softw. Pract. Exper.*, 33(5):397–421, 2003.

[DY83] Danny Dolev and Andrew C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[ES00] Ulfar Erlingsson and Fred B. Schneider. IRM enforcement of Java stack inspection. In *Proceedings of the 2000 IEEE Symposium on Security and Privacy (S&P 2000)*, pages 246–255. IEEE Computer Society, 2000.

[FG02] Cédric Fournet and Andrew D. Gordon. Stack inspection: theory and variants. In *Proceedings of the 29th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 307–318. ACM Press, 2002.

[FS86] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. Odlyzko, editor, *Advances in Cryptology – CRYPTO 1986*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer-Verlag, August 1986.

[FSG+01] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. Proposed NIST standard for role-based access control. *ACM Trans. Inf. Syst. Secur.*, 4(3):224–274, 2001.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, October 1986.

[GK03] Shafi Goldwasser and Yael Tauman Kalai. On the (in)security of the Fiat-Shamir paradigm. In *Proceedings of the 44th Annual Symposium on Foundations of Computer Science*, pages 102–113. IEEE Computer Society Press, 2003.

[GM82] J. A. Goguen and J. Meseguer. Security policies and security models. In IEEE Computer Society Press, editor, *Proceedings of the 1982 IEEE Symposium on Security and Privacy*, pages 11–20, 1982.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, April 1984.

[GNY90] Li Gong, Roger M. Needham, and Raphael Yahalom. Reasoning about belief in cryptographic protocols. In *Proceedings of the 1990 IEEE Symposium on Security and Privacy*, pages 234–248. IEEE Computer Society Press, 1990.

[HILL99] Johan Hastad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[HMS03] K. Hamlen, G. Morrisett, and F. Schneider. Computability classes for enforcement mechanisms, 2003.

[Hoa85] Charles A. R. Hoare. *Communicating Sequential Processes*. Prentice-Hall, 1985.

[HR98] Nevin Heintze and Jon G. Riecke. The SLam calculus: programming with secrecy and integrity. In ACM, editor, *Conference record of POPL '98: the 25th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, San Diego, California, 19–21 January 1998*, pages 365–377, New York, NY, USA, 1998. ACM Press.

[HRU76] Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman. Protection in operating systems. *Commun. ACM*, 19(8):461–471, 1976.

[HVY00] Kohei Honda, Vasco Thudichum Vasconcelos, and Nobuko Yoshida. Secure information flow as typed process behaviour. In *Proceedings of the 9th European Symposium on Programming Languages and Systems*, pages 180–199. Springer-Verlag, 2000.

[JLS76] A. K. Jones, R. J. Lipton, and L. Snyder. A linear algorithm for deciding security. In *17th Annual Symposium on Foundations of Computer Science*, pages 33–41. IEEE, 1976.

[JSS97] Sushil Jajodia, Pierangela Samarati, and V. S. Subrahmanian. A logical language for expressing authorizations. In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, page 31. IEEE Computer Society, 1997.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In M. Wiener, editor, *Advances in Cryptology – CRYPTO 1999*, Lecture Notes in Computer Science, pages 388–397. Springer-Verlag, 1999.

[Koc96] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz, editor, *Advances in Cryptology – CRYPTO 1996*, Lecture Notes in Computer Science, pages 104–113. Springer-Verlag, 1996.

[Koz98] D. Kozen. Efficient code certification. Technical Report TR98-1661, Computer Science Department, Cornell University, 1998.

[Lam74] B. W. Lampson. Protection. *Operating Systems Review*, 8(1):18–24, January 1974.

[LBW04] Jay Ligatti, Lujo Bauer, and David Walker. Edit automata: Enforcement mechanisms for run-time security policies. *International Journal of Information Security*, 2004. To appear.

[Low96] Gavin Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In Tiziana Margaria and Bernhard Steffen, editors, *Tools and Algorithms for Construction and Analysis of Systems, Second International Workshop, TACAS '96*, volume 1055 of *Lecture Notes in Computer Science*, pages 147–166. Springer-Verlag, 1996.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2):373–386, 1988.

[Mau92] Ueli M. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992.

[Mau93] Ueli M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[Mau99] Ueli M. Maurer. Information-theoretic cryptography. In M. Wiener, editor, *Advances in Cryptology – CRYPTO 1999*, volume 1666 of *Lecture Notes in Computer Science*, pages 47–64. Springer-Verlag, 1999.

[MS01] Heiko Mantel and Andrei Sabelfeld. A Generic Approach to the Security of Multi-threaded Programs. In *Proceedings of the 14th IEEE Computer Security Foundations Workshop*, pages 126–142, Cape Breton, Nova Scotia, Canada, June 11–13 2001. IEEE Computer Society.

[MvOV96] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[MW04] Daniele Micciancio and Bogdan Warinschi. Soundness of formal encryption in the presence of active adversaries. In M. Naor, editor, *First Theory of Cryptography Conference, TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 133–151. Springer-Verlag, 2004.

[Mye99] Andrew C. Myers. JFlow: Practical mostly-static information flow control. In *Symposium on Principles of Programming Languages*, pages 228–241, 1999.

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4(2):151–158, 1991.

[Nec94] V.I. Nechaev. Complexity of a determinate algorithm for the discrete logarithm. *Mathematical Notes*, 55(2):165–172, 1994.

[Nec97] George C. Necula. Proof-carrying code. In *Proceedings of the 24th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 106–119. ACM Press, 1997.

[Nie02] Jesper Buus Nielsen. Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case. In M. Yung, editor, *Advances in Cryptology – CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 111–126. Springer-Verlag, 2002.

[NL96] George C. Necula and Peter Lee. Safe kernel extensions without run-time checking. *SIGOPS Oper. Syst. Rev.*, 30(SI):229–243, 1996.

[NY90] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen-ciphertext attacks. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*. ACM Press, 1990.

[oD83] Department of Defense. *Trusted Computer System Evaluation Criteria (Orange Book)*. Department of Defense, 1983.

[Pau98] Lawrence C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6(1–2):85–128, 1998.

[PS00] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000.

[PSS01] François Pottier, Christian Skalka, and Scott F. Smith. A systematic approach to static access control. In *Proceedings of the 10th European Symposium on Programming Languages and Systems*, pages 30–45. Springer-Verlag, 2001.

[PSS03] François Pottier, Christian Skalka, and Scott Smith. A systematic approach to static access control. *ACM Transactions on Programming Languages and Systems*, November 2003. To appear.

[Rom90] John Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, pages 387–394. ACM Press, 1990.

[San88] Ravinderpal Singh Sandhu. The schematic protection model: its definition and analysis for acyclic attenuating schemes. *J. ACM*, 35(2):404–432, 1988.

[San92] R. S. Sandhu. The typed access matrix model. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 122–136, 1992.

[SC01] Paul F. Syverson and Iliano Cervesato. The logic of authentication protocols. In *FOSAD '00: Revised versions of lectures given during the IFIP WG 1.7 International School on Foundations of Security Analysis and Design on Foundations of Security Analysis and Design*, pages 63–136, London, UK, 2001. Springer-Verlag.

[SCFY96] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. Role-based access control models. *IEEE Computer*, 29(2):38–47, 1996.

[Sch97] Steve Schneider. Verifying authentication protocols with CSP. In *10th Computer Security Foundations Workshop (CSFW '97)*, pages 3–17. IEEE Computer Society, 1997.

[Sch00] Fred B. Schneider. Enforceable security policies. *ACM Trans. Inf. Syst. Secur.*, 3(1):30–50, 2000.

[SdV01] Pierangela Samarati and Sabrina De Capitani di Vimercati. Access control: Policies, models, and mechanisms. In *FOSAD '00: Revised versions of lectures given during the IFIP WG 1.7 International School on Foundations of Security Analysis and Design on Foundations of Security Analysis and Design*, pages 137–196, London, UK, 2001. Springer-Verlag.

[Sha48] Claude E. Shannon. A mathematical theory of communication. *Bell Systems Technical Journal*, 27:379–423 and 623–656, 1948.

[Sha49] Claude E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28:656–715, 1949.

[Sha79] Adi Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11):612–613, 1979.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In W. Fumy, editor, *Advances in Cryptology – EUROCRYPT 1997*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer-Verlag, 1997.

[Sho02] Victor Shoup. OAEP reconsidered. *Journal of Cryptology*, 15(4):223–249, 2002.

[SJ00] Claus-Peter Schnorr and Markus Jakobsson. Security of signed ElGamal encryption. In T. Okamoto, editor, *Advances in Cryptology – ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 73–89. Springer-Verlag, 2000.

[SM03] A. Sabelfeld and A. Myers. Language-based information-flow security. *IEEE Journal on Selected Areas in Communications*, 21, 2003.

[SMH01] Fred B. Schneider, J. Gregory Morrisett, and Robert Harper. A language-based approach to security. In *Informatics - 10 Years Back. 10 Years Ahead.*, pages 86–101, London, UK, 2001. Springer-Verlag.

[Sny81] L. Snyder. Theft and conspiracy in the take-grant model. *Journal of Computer and Systems Sciences*, 23(3):333–347, December 1981.

[SS00] Christian Skalka and Scott Smith. Static enforcement of security with types. *ACM SIGPLAN Notices*, 35(9):34–45, 2000.

[SV98] Geoffrey Smith and Dennis Volpano. Secure information flow in a multi-threaded imperative language. In *Proceedings of the 25th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 355–364. ACM Press, 1998.

[SvO96] Paul F. Syverson and Paul C. van Oorschot. A unified cryptographic protocol logic. NRL Publication 5540-227, Naval Research Lab, 1996.

[vO93] Paul C. van Oorschot. Extending cryptographic logics of belief to key agreement protocols. In *Proceedings of the 1st Conference on Computer and Communications Security*, pages 232–243. ACM Press, 1993.

[WBDF97] Dan S. Wallach, Dirk Balfanz, Drew Dean, and Edward W. Felten. Extensible security architectures for Java. In *16th Symposium on Operating Systems Principles*, pages 116–128, 1997.

[WF98] Dan S. Wallach and Edward W. Felten. Understanding Java stack inspection. In *Proceedings of the 1998 IEEE Symposium on Security and Privacy*, pages 52–63. IEEE Computer Society, 1998.

[Wie83] Stephen Wiesner. Conjugate coding. *Sigact News*, 15(1):78–88, 1983. Original manuscript written ca. 1970.

[WLAG93] Robert Wahbe, Steven Lucco, Thomas E. Anderson, and Susan L. Graham. Efficient software-based fault isolation. In *Proceedings of the fourteenth ACM symposium on Operating systems principles*, pages 203–216. ACM Press, 1993.

[Wol99] Stefan Wolf. Unconditional security in cryptography. In Ivan Damgård, editor, *Lectures on Data Security, Modern Cryptology in Theory and Practice, Summer School, Aarhus, Denmark, July 1998*, volume 1561 of *Lecture Notes in Computer Science*, pages 217–250. Springer-Verlag, 1999.

[Wyn75] Aaron D. Wyner. The wire-tap channel. *Bell Systems Technical Journal*, 54(8):1355–1387, 1975.

[Yao82] Andrew C. Yao. Theory and applications of trapdoor functions (extended abstract). In IEEE, editor, *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, pages 80–91. IEEE Computer Society Press, 1982.