SECURITY ANALYSIS OF NETWORK PROTOCOLS

[1]Kamlesh, [2] Puneet Rani

[1,2]Computer Science & Engineering Department, M.D.U, (India)

ABSTRACT

This paper presents the study of network protocol in respect of security . . In this paper a study of various papers and articles is done, and in this paper we explain two central problems associated with the design and security analysis of network protocols that use cryptographic primitives. The main goal is to develop methods for proving properties of complex protocols by combining independent proofs of their parts

Keywords: Introduction, Derivative, Problem, PCL, PCL Logic

I. INTRODUCTION

Protocols that enable secure communication over an untrusted network constitute an important part of the current computing infrastructure. Common examples of such protocols are SSL [53], TLS [44], Kerberos [10], and the IPSec [37] and IEEE 802.11i [1] protocol suites. SSL and TLS are used by internet browsers and web servers to allow secure transactions in applications like online banking. The IPSec protocol suite provides confidentiality and integrity at the IP layer and is widely used to secure corporate VPNs. IEEE 802.11i provides data protection and integrity in wireless local area networks, while Kerberos is used for network authentication.

The design and security analysis of such network protocols presents a difficult problem. In several instances, serious security vulnerabilities were uncovered in protocols many years after they were first published or deployed [105, 59, 1, 16, , 68]. While some of these attacks rely on subtle properties of cryptographic primitives, a large fraction can be traced to intricacies in designing protocols that are robust in a concurrent execution setting. To further elaborate this point, let us consider the concrete example of the SSL protocol.

In SSL, a client typically sets up a key with a web server.

II. PROBLEMS

There are two problems associated with security analysis of network protocolsThe first problem pertains to the secure composition of protocols, where the goal is to develop methods for proving properties of complex protocols by combining independent proofs of their parts. In order to address this problem, we have developed a framework consisting of two formal systems: Protocol Derivation System (PDS) and Protocol Composition Logic (PCL). PDS supports syntactic derivations of complex protocols, starting from basic components, and combining or extending them using a sequence of composition, refinement, and transformation operations. PCL is a Floyd-Hoare style logic that supports axiomatic proofs of protocol properties. The eventual goal is to develop proof methods for PCL for every derivation operation in PDS, thereby enabling the parallel development of protocols and their security proofs.

The second problem pertains to the computational soundness of symbolic protocol analysis.

At a high-level, this means that a logical method for protocol analysis should have an associated soundness theorem, which guarantees that a completely symbolic analysis or proof has an interpretation in the standard complexity-theoretic model of modern cryptography. Our approach to this problem involves defining

complexity-theoretic semantics and proving a soundness theorem for a variant of PCL which we call Computational PCL. While the basic form of the logic remains unchanged, there are certain important differences involving the interpretation of implication in terms of conditional probability and the semantics of the predicates used to capture secrecy properties

III DERIVATIVE SYSTEM OF PROTOCOL

There are many researches can be done for the analysis of security of network protocols .Many researchers recognize that the common authentic and key exchange protocols are built by using standard concept.Thecommon building blocks include Diffie-Hellman key exchange to avoid replay, certificates from an accepted authority to validate public keys, and encrypted or signed messages that can only be created or read by identifiable parties. An informal practice of presenting protocols incrementally, starting from simple components and extending them by features and functions, is used in [44], with efforts to formalize the practice appearing in [23]. Our framework for deriving security protocols consists of a set of basic building blocks called components and a set of operations for constructing new protocols from old ones. These operations may be divided into three different types: composition, refinement and transformation. A component is a basic protocol step or steps, used as a building block for larger protocols. Diffie-Hellman key exchange and challenge-response are examples of basic components. A composition operation combines two protocols. Parallel composition and sequential composition are two examples of composition operations. A refinement operation acts on message components of a single protocol. For example replacing plaintext by an encrypted one is a refinement. A refinement does not change the number of messages or the basic structure of a protocol. A transformation operates on a single protocol, and may modify several steps of a protocol by moving data from one message to another, combining steps, or inserting one or more additional steps. For example, moving data from one protocol message to an earlier message (between the same parties) is a transformation .

IV. PROTOCOL COMPOSITION LOGIC

Protocol Composition Logic (PCL) is a logic for proving security properties of network protocols. A preliminary version of PCL was presented in [49, 50]. In subsequent work [35,36, 39, 37, 60], we have significantly extended the logic and developed new proof methods. Currently, we are able to prove authentication and secrecy properties of common security protocols by derivations of twenty to sixty lines of proof. The reason for this succinctness is that the proof rules of the logic state general properties of protocol traces that can be reused for many different protocols. The logic is different from previous “belief” logics like BAN [24] and from explicit reasoning about protocol participants and the intruder as in Paulson’s Inductive Method [10]. In a sense, the goal of this work was to retain the readability and ease of use of BAN logic while providing the same degree of assurance in the security of protocols as Paulson’s Inductive Method. The logic is designed around a process calculus with actions for each protocol step. Protocol actions are annotated with assertions in a manner resembling dynamic logic for sequential imperative programs. The semantics of our logic is based on sets of traces of protocol executions, following the standard symbolic model of protocol execution and attack. Security proofs involve local reasoning about properties guaranteed by individual actions and global reasoning about actions of honest principals who faithfully follow the protocol. One central idea is that assertions associated with an action will hold in any protocol execution that contains this action.

V. PCL PROOF SYSTEM

we present a method for reasoning about compound protocols from their parts. In general terms, we address two basic problems in compositional security. The first may be called additive combination – we wish to combine protocol components in a way that accumulates security properties. For example, we may wish to combine a basic key exchange protocol with an authentication mechanism to produce a protocol for authenticated key exchange. The second basic problem is ensuring nondestructive combination. If two mechanisms are combined, each serving a separate purpose, then it is important to be sure that neither one degrades the security properties of the other. For example, if we add an alternative mode of operation to a protocol, then some party may initiate a session in one mode and simultaneously respond to another session in another mode, using the same public key or long-term key in both. Unless the modes are designed not to interfere, there may be an attack on the multi-mode protocol that would not arise if only one mode were possible.

VI. CONCLUSION

we have presented several results in the area of security analysis of network protocols. Our main contribution is PCL—a logic for proving security propertiesof network protocols. Security proofs in PCL are relatively short and intuitive and scale to protocols of practical interest. Two central results for this logic are a composition theorem and a computational soundness theorem. The composition theorem allows proofs of complex protocols to be built up from proofs of their constituent sub-protocols. It is formulated and proved by adapting ideas from the assume-guarantee paradigm for reasoning about distributed systems. The computational soundness theorem guarantees that, for a class of security properties and protocols, axiomatic proofs in a fragment of PCL carry the same meaning as hand-proofs done by cryptographers

VII. ACKNOWLEDGMENT

I show my thanks to all the departments' personals and sponsors who give us an opportunity to present and express my paper on this level .

REFERENCES

[1] IEEE P802.11i/D10.0. Medium Access Control (MAC) security enhancements, amendment 6 to IEEE Standard for local and metropolitan area networks part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications., April 2004.

[2] IEEE P802.16e/D10.0. IEEE Standard for local and metropolitan area networks. Part 16: Air interface for fixed and mobile broadband wireless access systems. Amendment for physical and medium access control layers for combined fixed and mobile operation in licensed bands., August 2005.

[3] M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In 28th ACM Symposium on Principles of Programming Languages, pages 104–115,\ 2001.

[4] M. Abadi and A. Gordon. A calculus for cryptographic protocols: the spi calculus. Information and Computation, 148(1):1–70, 1999. Expanded version available as SRC Research Report 149 (January 1998).

[5] M. Abadi and A. D. Gordon. A bisimulation method for cryptographic protocol. In Proc. ESOP 98, Lecture notes in Computer Science. Springer, 1998.

[6] M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: the spi calculus. Information and Computation, 143:1–70, 1999. Expanded version available as SRC Research Report 149 (January 1998). 120

[7] M. Abadi and P. Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). Journal of Cryptology, 15(2):103–127, 2002.

[8] W. Aiello, S.M. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A.D. Keromytis, and O. Reingold. Just fast keying (JFK), 2002. Internet draft.

[9] J. Alves-Foss and T. Soule. A weakest precondition calculus for analysis of cryptographic protocols. In DIMACS Workshop on Design and Formal Verification of Crypto Protocols, 1997.

[10] M. Backes, A. Datta, A. Derek, J. C. Mitchell, and M. Turuani. Compositional analysis of contract-signing protocols. In Proceedings of 18th IEEE Computer Security Foundations Workshop, pages 94–110. IEEE, 2005.

[11] M. Backes, A. Datta, A. Derek, J. C. Mitchell, and M. Turuani. Compositional analysis of contract signing protocols. In Proceedings of 18th IEEE Computer Security Foundations Workshop. IEEE, 2005. to appear.

[12] M. Backes, B. Pfitzmann, and M. Waidner. Reactively secure signature schemes. In Proceedings of 6th Information Security Conference, volume 2851 of Lecture Notes in Computer Science, pages 84–95. Springer, 2003.

[13] M. Backes, B. Pfitzmann, and M.Waidner. A universally composable cryptographic library. Cryptology ePrint Archive, Report 2003/015, 2003.

[14] M. Backes, B. Pfitzmann, and M. Waidner. A general composition theorem for secure reactive systems. In Proceedings of 1st Theory of Cryptography Conference, volume 2951 of Lecture Notes in Computer Science. Springer, 2004.

[15] M. Barr and C. Wells. Category Theory for Computing Science. Prentice Hall, New York, 1999. Third Edition.

[16] M. Baugher, B. Weis, T. Hardjono, and H. Harney. The Group Domain of Interpretation, 2003. RFC 3547.

[17] S. Bellantoni. Predicative Recursion and Computational Complexity. PhD thesis, University of Toronto, 1992.

[18] M. Bellare, A. Boldyreva, and S. Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In Advances in Cryptology – EUROCRYPT 2000, Proceedings, pages 259–274, 2000.

[19] M. Bellare, R. Canetti, and H. Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols. In Proceedings of 30th Annual Symposium on the Theory of Computing. ACM, 1998.

[20] M. Bellare and P. Rogaway. Entity authentication and key distribution. In Advances in Cryprtology - Crypto ’93 Proceedings. Springer-Verlag, 1994.

[21] M. Bellare and P. Rogaway. Entity authentication and key distribution. In Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO ’93), pages 232–249. Springer-Verlag, 1994.

[22] G. Berry and G. Boudol. The chemical abstract machine. Theoretical Computer Science, 96:217–248, 1992.

[23] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, and M. Yung. Systematic design of a family of attack resistant authentication protocols. IEEE Journal n Selected Areas in Communications, 1(5), June 1993.

[24] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. ACM Transactions on Computer Systems, 8(1):18–36, 1990.

[25] L. Buttyan, S. Staamann, and U.Wilhelm. A simple logic for authentication protocol design. In Proceedings of 11th IEEE Computer Security Foundations Workshop, pages 153–162. IEEE, 1999.

[26] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In Proc. 42nd IEEE Symp. on the Foundations of Computer Science. IEEE, 2001. Full version available at http://eprint.iacr.org/2000/067/.

[27] R. Canetti and M. Fischlin. Universally composable commitments. In Proc. CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 19–40, Santa Barbara, California, 2001. Springer.

[28] R. Canetti and H. Krawczyk. Universally composable notions of key exchange and secure channels. In Advances in Cryptology—EUROCRYPT 2002, volume 2332 of Lecture Notes in Computer Science, pages 337–351. Springer, 2002.

[29] R. Canetti, E. Kushilevitz, and Y. Lindell. On the limitations of universally composable two-party computation without set-up assumptions. In Advances in Cryptology—EUROCRYPT 2003, volume 2656 of Lecture Notes in Computer Science, pages 68–86. Springer, 2003.

[30] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai. Universally composable twoparty and multi-party secure computation. In Proc. ACM Symp. on the Theory of Computing, pages 494–503, 2002.

[31] R. Canetti, C. Meadows, and P. Syverson. Environmental requirements for authentication protocols. In Proceedings of Software Security - Theories and Systems, Mext- NSF-JSPS International Symposium, ISSS, LNCS 2609, pages 339–355. Springer- Verlag, 2003.

[32] J. A. Clark and J. L. Jacob. Searching for a solution: Engineering tradeoffs and the evolution of provably secure protocols. In Proceedings IEEE Symposium on Research in Security and Privacy, pages 82–95. IEEE, 2000.

[33] V. Cortier and B. Warinschi. Computationally sound, automated proofs for security protocols. In Proceedings of 14th European Symposium on Programming (ESOP'05), Lecture Notes in Computer Science. Springer-Verlag, 2005.

[34] I. Damgard and J. B. Nielsen. Universally composable efficient multiparty computation from threshold homomorphic encryption. In Proc. CRYPTO 2003, volume 2729 of Lecture Notes in Computer Science, pages 247–264, Santa Barbara, California, 2003. Springer.

[35] A. Datta, A. Derek, J. C. Mitchell, and D. Pavlovic. A derivation system for security protocols and its logical formalization. In Proceedings of 16th IEEE Computer Security Foundations Workshop, pages 109–125. IEEE, 2003.

[36] A. Datta, A. Derek, J. C. Mitchell, and D. Pavlovic. Secure protocol composition (Extended abstract). In Proceedings of ACM Workshop on Formal Methods in Security Engineering, pages 11–23, 2003.

[37] A. Datta, A. Derek, J. C. Mitchell, and D. Pavlovic. Abstraction and refinement in protocol derivation. In Proceedings of 17th IEEE Computer Security Foundations Workshop, pages 30–45. IEEE, 2004.

[38] A. Datta, A. Derek, J. C. Mitchell, and D. Pavlovic. A derivation system and compositional logic for security protocols. Journal of Computer Security, 2004. to appear.

[39] A. Datta, A. Derek, J. C. Mitchell, and D. Pavlovic. Secure protocol composition. In Proceedings of 19th Annual Conference on Mathematical Foundations of Programming Semantics, volume 83 of Electronic Notes in Theoretical Computer Science, 2004.

[40] A. Datta, A. Derek, J. C. Mitchell, A. Ramanathan, and A. Scedrov. The impossibility of realizable ideal functionality. Cryptology ePrint Archive, Report 2005/211, 2005.

[41] A. Datta, A. Derek, J. C. Mitchell, and B. Warinschi. Key exchange protocols: Security definition, proof method and applications, 2005. In preparation.

[42] A. Datta, R. K¨usters, J.C. Mitchell, and A. Ramanathan. On the Relationships Between Notions of Simulation-Based Security. In J. Kilian, editor, Proceedings of the 2nd Theory of Cryptography Conference (TCC 2005), volume 3378 of Lecture Notes in Computer Science, pages 476–494. Springer-Verlag, 2005.

[43] A. Datta, J. C. Mitchell, and D. Pavlovic. Derivation of the JFK protocol. Technical Report KES.U.02.03, Kestrel Institute, 2002.

[44] T. Dierks and C. Allen. The Tls Protocol Version 1.0, 1999. RFC 2246.