zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Biondi, Fabrizio; **Legay, Axel**; **Malacaria, Pasquale**; **Wąsowski, Andrzej**
Quantifying information leakage of randomized protocols. (English) Zbl 1328.68142
Theor. Comput. Sci. 597, 62-87 (2015).

Summary: The quantification of information leakage provides a quantitative evaluation of the security of a system. We propose the usage of Markovian processes to model deterministic and probabilistic systems. By using a methodology generalizing the lattice of information approach we model refined attackers capable to observe the internal behavior of the system, and quantify the information leakage of such systems. We also use our method to obtain an algorithm for the computation of channel capacity from our Markovian models. Finally, we show how to use the method to analyze timed and non-timed attacks on the Onion Routing protocol.

MSC:

68Q87 Probability in computer science (algorithm analysis, random structures, phase transitions, etc.)
68M12 Network protocols
68Q60 Specification and verification (program logics, model checking, etc.)
94A60 Cryptography

Cited in **1** Document

Keywords:

model checking; quantitative information flow; information leakage; Markov chain; Markov decision process; channel capacity; probabilistic system

Full Text: DOI

References:

[1] Malacaria, P., Algebraic foundations for information theoretical, probabilistic and guessability measures of information flow, (2011), CoRR

[2] Clark, D.; Hunt, S.; Malacaria, P., A static analysis for quantifying information flow in a simple imperative language, J. Comput. Secur., 15, 321-371, (2007)

[3] Heusser, J.; Malacaria, P., Quantifying information leaks in software, (Gates, C.; Franz, M.; McDermott, J. P., ACSAC, (2010), ACM), 261-269

[4] Chatzikokolakis, K.; Palamidessi, C.; Panangaden, P., Anonymity protocols as noisy channels, Inform. Comput., 206, 378-401, (2008) · Zbl 1147.68394

[5] Chen, H.; Malacaria, P., Quantifying maximal loss of anonymity in protocols, (Li, W.; Susilo, W.; Tupakula, U. K.; Safavi-Naini, R.; Varadharajan, V., ASIACCS, (2009), ACM), 206-217

[6] B. Köpf, G. Smith, Vulnerability bounds and leakage resilience of blinded cryptography under timing attacks, in: [40], pp. 44-56.

[7] Köpf, B.; Basin, D. A., An information-theoretic model for adaptive side-channel attacks, (Ning, P.; di Vimercati, S. D.C.; Syverson, P. F., ACM Conference on Computer and Communications Security, (2007), ACM), 286-296

[8] Millen, J. K., Covert channel capacity, (IEEE Symposium on Security and Privacy, (1987)), 60-66

[9] Goldschlag, D. M.; Reed, M. G.; Syverson, P. F., Onion routing, Commun. ACM, 42, 39-41, (1999)

[10] Murdoch, S. J.; Danezis, G., Low-cost traffic analysis of tor, (Proceedings of the 2005 IEEE Symposium on Security and Privacy, SP '05, (2005), IEEE Computer Society Washington, DC, USA), 183-195

[11] Abbott, T. G.; Lai, K. J.; Lieberman, M. R.; Price, E. C., Browser-based attacks on tor, (Borisov, N.; Golle, P., Privacy Enhancing Technologies, Lecture Notes in Computer Science, vol. 4776, (2007), Springer), 184-199

[12] Applebaum, D., Probability and information: an integrated approach, (2008), Cambridge University Press New York, NY, USA · Zbl 1154.60001

[13] Cover, T. M.; Thomas, J. A., Elements of information theory, (2006), Wiley · Zbl 1140.94001

[14] Shannon, C. E., A mathematical theory of communication, Bell Syst. Tech. J., 27, 379-423, (1948) · Zbl 1154.94303

[15] Biondi, F.; Legay, A.; Nielsen, B. F.; Wasowski, A., Maximizing entropy over Markov processes, (Dediu, A. H.; Martín-Vide, C.; Truthe, B., LATA, Lecture Notes in Computer Science, vol. 7810, (2013), Springer), 128-140 · Zbl 1377.68127

© 2021 FIZ Karlsruhe GmbH

[16] Biondi, F.; Legay, A.; Nielsen, B. F.; Wasowski, A., Maximizing entropy over Markov processes, J. Log. Algebr. Methods Program., 83, 384-399, (2014) · Zbl 1371.68175

[17] Smith, G., Quantifying information flow using MIN-entropy, (QEST, (2011), IEEE Computer Society), 159-167

[18] Smith, G., On the foundations of quantitative information flow, (de Alfaro, L., FOSSACS, Lecture Notes in Computer Science, vol. 5504, (2009), Springer), 288-302 · Zbl 1234.68101

[19] Backes, M.; Köpf, B.; Rybalchenko, A., Automatic discovery and quantification of information leaks, (IEEE Symposium on Security and Privacy, (2009), IEEE Computer Society), 141-153

[20] Alvim, M. S.; Chatzikokolakis, K.; Palamidessi, C.; Smith, G., Measuring information leakage using generalized gain functions, (Chong, S., CSF, (2012), IEEE), 265-279

[21] Boreale, M.; Pampaloni, F., Quantitative information flow under generic leakage functions and adaptive adversaries, (Ábrahám, E.; Palamidessi, C., FORTE, Lecture Notes in Computer Science, vol. 8461, (2014), Springer), 166-181

[22] Landauer, J.; Redmond, T., A lattice of information, (CSFW, (1993)), 65-70

[23] H. Yasuoka, T. Terauchi, Quantitative information flow - verification hardness and possibilities, in: [40], pp. 15-27. · Zbl 1359.68201

[24] Winskel, G., The formal semantics of programming languages - an introduction, Foundation of Computing Series, (1993), MIT Press · Zbl 0919.68082

[25] Malacaria, P., Risk assessment of security threats for looping constructs, J. Comput. Secur., 18, 191-228, (2010)

[26] McIver, A.; Meinicke, L.; Morgan, C., Compositional closure for Bayes risk in probabilistic noninterference, (Abramsky, S.; Gavoille, C.; Kirchner, C.; Meyer auf der Heide, F.; Spirakis, P. G., ICALP (2), Lecture Notes in Computer Science, vol. 6199, (2010), Springer), 223-235 · Zbl 1288.68024

[27] McIver, A.; Morgan, C.; Smith, G.; Espinoza, B.; Meinicke, L., Abstract channels and their robust information-leakage ordering, (Abadi, M.; Kremer, S., POST, Lecture Notes in Computer Science, vol. 8414, (2014), Springer), 83-102

[28] Nakamura, Y., Entropy and semivaluations on semilattices, Kodai Math. Semin. Rep., 22, 443-468, (1970) · Zbl 0222.06004

[29] Biondi, F.; Legay, A.; Malacaria, P.; Wasowski, A., Quantifying information leakage of randomized protocols, (Giacobazzi, R.; Berdine, J.; Mastroeni, I., Verification, Model Checking, and Abstract Interpretation, 14th International Conference. Proceedings, VMCAI, 2013, Rome, Italy, January 20-22, Lecture Notes in Computer Science, vol. 7737, (2013), Springer), 68-87 · Zbl 1329.68188

[30] Chen, T.; Han, T., On the complexity of computing maximum entropy for Markovian models, (Raman, V.; Suresh, S. P., 34th International Conference on Foundation of Software Technology and Theoretical Computer Science, FSTTCS 2014, December 15-17, 2014, New Delhi, India, LIPIcs, vol. 29, (2014), Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik), 571-583 · Zbl 1360.68501

[31] McIver, A.; Meinicke, L.; Morgan, C., Hidden-Markov program algebra with iteration, Math. Structures Comput. Sci., 25, 320-360, (2015) · Zbl 1362.68052

[32] Volpano, D. M.; Irvine, C. E.; Smith, G., A sound type system for secure flow analysis, J. Comput. Secur., 4, 167-188, (1996)

[33] O'Neill, K. R.; Clarkson, M. R.; Chong, S., Information-flow security for interactive programs, (CSFW, (2006), IEEE Computer Society), 190-201

[34] Alvim, M. S.; Andrés, M. E.; Palamidessi, C., Quantitative information flow in interactive systems, J. Comput. Secur., 20, 3-50, (2012)

[35] Malacaria, P.; Chen, H., Lagrange multipliers and maximum information leakage in different observational models, (Erlingsson, Úlfar; Pistoia, M., PLAS, (2008), ACM), 135-146

[36] Chen, H.; Malacaria, P., The optimum leakage principle for analyzing multi-threaded programs, (Kurosawa, K., ICITS, Lecture Notes in Computer Science, vol. 5973, (2009), Springer), 177-193 · Zbl 1286.68311

[37] Chothia, T.; Guha, A., A statistical test for information leaks using continuous mutual information, (CSF, (2011), IEEE Computer Society), 177-190

[38] Köpf, B.; Mauborgne, L.; Ochoa, M., Automatic quantification of cache side-channels, (Madhusudan, P.; Seshia, S. A., CAV, Lecture Notes in Computer Science, vol. 7358, (2012), Springer), 564-580

[39] Preda, M. D.; Giacobazzi, R., Semantics-based code obfuscation by abstract interpretation, J. Comput. Secur., 17, 855-908, (2009)

[40] (Proceedings of the 23rd IEEE Computer Security Foundations Symposium, CSF 2010, July 17-19, 2010, Edinburgh, United Kingdom, (2010), IEEE Computer Society)

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.

© 2021 FIZ Karlsruhe GmbH