Vorlesung Rechnersicherheit
Literaturliste

Prof. Dr.-Ing. Volker Roth

Sommersemester 2017

Literatur

[1] Robert Morris and Ken Thompson. Password security: A case history. *Commun. ACM*, 22(11):594–597, November 1979.

[2] Joseph Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *Proc. IEEE Symposium on Security and Privacy*, 2012.

[3] Geoffrey Sampson and William A. Gale. Good-turing frequency estimation without tears. *Journal of Quantitative Linguistics*, 2(3):217–237, 1995.

[4] Matt Weir, Sudhir Aggarwal, Breno de Medeiros, and Bill Glodek. Password cracking using probabilistic context-free grammars. In *Proc. IEEE Symposium on Security and Privacy*, pages 391–405, 2009.

[5] J. Ma, W. Yang, M. Luo, and N. Li. A study of probabilistic password models. In *Proc. IEEE Symposium on Security and Privacy*, 2014.

[6] Philippe Oechslin. Making a faster cryptanalytic time-memory trade-off. In *Proc. CRYPTO*, volume 2729 of *LNCS*, pages 617–630. Springer, 2003.

[7] Arvind Narayanan and Vitaly Shmatikov. Fast dictionary attacks on passwords using time-space tradeoff. In *Proc. CCS*, pages 364–372, 2005.

[8] Ari Juels and Ronald L. Rivest. Honeywords: Making password-cracking detectable. In *Proc. CCS*, pages 145–160, 2013.

[9] Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart. Cracking-resistant password vaults using natural language encoders. In *Proc. IEEE Symposium on Security and Privacy*, 2015.

[10] Benjamin Güldenring, Volker Roth, and Lars Ries. Knock Yourself Out: Secure authentication with short re-usable passwords. In *Proc. Network and Distributed System Security Symposium*. The Internet Society, 2015.

[11] Morrie Gasser. *Building a Secure Computer System*. Van Nostrand Reinhold, 1988.

[12] Dorothy Elizabeth Robling Denning. *Cryptography and Data Security*. Addison-Wesley, 1982.

[13] Lawrence Snyder. On the synthesis and analysis of protection systems. *SIGOPS Oper. Syst. Rev.*, 11(5):141–150, November 1977.

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

[15] Yossef Oren, Vasileios P. Kemerlis, Simha Sethumadhavan, and Angelos D. Keromytis. The spy in the sandbox: Practical cache attacks in JavaScript and their implications. In *Proc. Conference on Computer and Communications Security*, CCS, pages 1406–1418. ACM, 2015.

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

[17] J. S. Fenton. Memoryless subsystems. *Comput. J.*, 17(2):143–147, 1974.

Optionale Literatur

[18] Joseph Bonneau and Sören Preibusch. The password thicket: technical and market failures in human authentication on the web. In *Proc. WEIS*, 2010.

[19] R. Veras, C. Collins, and J. Thorpe. On the semantic patterns of passwords and their security impact. In *Proc. NDSS*. Internet Society, 2014.

[20] Markus Dürmuth, Fabian Angelstorf, Claude Castelluccia, Daniele Perito, and Abdelberi Chaabane. OMEN: faster password guessing using an ordered markov enumerator. In *International Symposium on Engineering Secure Software and Systems (ESSoS)*, volume 8978 of *LNCS*. Springer, 2015.

[21] Martin M. Hellman. A cryptoanalytic time-memory trade off. *IEEE Transactions on Information Theory*, 26:401–406, 1980.

[22] Ari Juels and Thomas Ristenpart. Honey encryption: Security beyond the brute-force bound. In *Proc. EUROCRYPT*, volume 8441 of *LNCS*, pages 293–310. Springer Berlin Heidelberg, 2014.

[23] Hristo Bojinov, Elie Bursztein, Xavier Boyen, and Dan Boneh. Kamouflage: Loss-resistant password management. In *Proc. ESORICS*, pages 286–302, 2010.

[24] Stuart Schechter, A. J. Bernheim Brush, and Serge Egelman. It's no secret. measuring the security and reliability of authentication via "secret" questions. In *Proc. IEEE Symposium on Security and Privacy*, pages 375–390, 2009.

[25] Ajay Chander, Drew Dean, and John C. Mitchell. A state-transition model of trust management and access control. In *Proc. IEEE Computer Security Foundations Workshop*, pages 27–43. IEEE Computer Science Press, June 2001.

[26] Eran Tromer, Dag Arne Osvik, and Adi Shamir. Efficient cache attacks on AES, and countermeasures. *J. Cryptol.*, 23(2):37–71, January 2010.

[27] Dennis Volpano, Cynthia Irvine, and Geoffrey Smith. A sound type system for secure flow analysis. *J. Comput. Secur.*, 4(2-3):167–187, January 1996.