**参考文献**

[1] 第41次《中国互联网络发展状况统计报告》发布[J]. 中国广播, 2018(3).

[2] 俞佳宝, 胡爱群, 朱长明, 等. 无线通信设备的射频指纹提取与识别方法[J]. 密码学报, 2016(05):433-446.

[3] 袁红林. 基于射频指纹的无线网络物理层认证关键技术研究[D]. 东南大学, 2011.

[4] Chaabouni R. Break WEP Faster with Statistical Analysis[J]. Epfl, 2006.

[5] Mavridis I P, Androulakis A I E, Halkias A B, et al. Real-Life Paradigms of Wireless Network Security Attacks: Panhellenic Conference on Informatics, 2011[C].

[6] Ross A, Jain A. Information fusion in biometrics[J]. Pattern Recognition Letters, 2003,24(13):2115-2125.

[7] Tuyls P, Goseling J. Capacity and Examples of Template-Protecting Biometric Authentication Systems[M]. Springer Berlin Heidelberg, 2004.

[8] Talbot K I, Duley P R, Hyatt M H. Specific emitter identification and verification[J]. Technology Review, 2003.

[9] Riezenman M J. Cellular security: better, but foes still lurk[J]. Spectrum IEEE, 2000,37(6):39-42.

[10] Langley L E. Specific emitter identification (SEI) and classical parameter fusion technology: Wescon/'93. Conference Record, 2002[C].

[11] Guo F, Chiueh T. Sequence Number-Based MAC Address Spoof Detection[J]. Lecture Notes in Computer Science, 2005,3858:309-329.

[12] 顾杨. 基于无线设备特征指纹的无线钓鱼接入点检测技术研究[D]. 南京邮电大学, 2014.

[13] Desmond L C C, Yuan C C, Tan C P, et al. Identifying unique devices through wireless fingerprinting: ACM Conference on Wireless Network Security, WISEC 2008, Alexandria, Va, Usa, March 31 - April, 2008[C].

[14] Pang J, Greenstein B, Gummadi R, et al. 802.11 user fingerprinting: Annual ACM international conference on Mobile computing and networking, Montreal(CA), 2007[C].

[15] Sieka B. Active fingerprinting of 802.11 devices by timing analysis: Ccnc 2006. 2006 IEEE Consumer Communications and NETWORKING Conference, 2006[C].

[16] Gao K, Corbett C, Beyah R. A passive approach to wireless device fingerprinting: Ieee/ifip International Conference on Dependable Systems and Networks, 2010[C].

[17] Lyon G. Nmap: a free network mapping and security scanning tool[EB/OL]. [11-5]. https://nmap.org/.

[18] Yarochkin F, Kydyraliev M, Arkin O. Xprobe project[EB/OL]. http://ofirarkin.wordpress.com/xprobe/.

[19] Eckersley P. How Unique Is Your Web Browser? Privacy Enhancing Technologies, International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings, 2010[C].

1. Yen T F, Xie Y, Yu F, et al. Host Fingerprinting and Tracking on the Web:Privacy and Security Implications[J]. 2012, 11(1):111 - 124.
2. Mowery K, Bogenreif D, Yilek S, et al. Fingerprinting Information in JavaScript Implementations[C]// Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on. IEEE, 2011:9-12.
3. Acar G, Juarez M, Nikiforakis N, et al. FPDetective:dusting the web for fingerprinters[C]// ACM Sigsac Conference on Computer & Communications Security. ACM, 2013:1129-1140.
4. Łukasz Olejnik, Castelluccia C, Janc A. Why Johnny Can't Browse in Peace: On the Uniqueness of Web Browsing History Patterns[J]. Hot Topics in Privacy Enhancing Technologies, 2012, 69(1-2):63-74.
5. Bratus S, Cornelius C, Kotz D, et al. Active behavioral fingerprinting of wireless devices[C]// ACM Conference on Wireless Network Security. ACM, 2008:56-61.
6. Radhakrishnan S V, Uluagac A S, Beyah R. GTID: A Technique for Physical Device and Device Type Fingerprinting[J]. IEEE Transactions on Dependable & Secure Computing, 2015, 12(5):519-532.
7. Khlifi H, Gregoire J C. Estimation and removal of clock skew from delay measures[C]// IEEE International Conference on Local Computer Networks. IEEE, 2004:144-151.
8. Kohno T, Broido A, Claffy K C. Remote Physical Device Fingerprinting[C]// Security and Privacy, 2005 IEEE Symposium on. IEEE, 2005:211-225.
9. Cristea M, Groza B. Fingerprinting Smartphones Remotely via ICMP Timestamps[J]. IEEE Communications Letters, 2013, 17(6):1081-1083.
10. Langley L E. Specific emitter identification (SEI) and classical parameter fusion technology[C]// Wescon/'93. Conference Record. IEEE, 2002:377-381.
11. Lanze F, Panchenko A, Braatz B, et al. Clock skew based remote device fingerprinting demystified[C]// Global Communications Conference. IEEE, 2012:813-819.
12. Neumann C, Heen O, Onno S. An Empirical Study of Passive 802.11 Device Fingerprinting[J]. 2014:593-602.
13. Franklin J, Mccoy D, Tabriz P, et al. Passive data link layer 802.11 wireless device driver fingerprinting[C]// Conference on Usenix Security Symposium. USENIX Association, 2006:167--178.
14. Gerdes R M, Daniels T, Mina M, et al. Device Identification via Analog Signal Fingerprinting: A Matched Filter Approach.[C]// 144 Proceedings of the Network and Distributed System Security Symposium. 2004:78.
15. Brik V, Banerjee S, Gruteser M, et al. Wireless device identification with radiometric signatures[C]// ACM International Conference on Mobile Computing and NETWORKING. ACM, 2008:116-127.
16. Nguyen N T, Zheng G, Han Z, et al. Device fingerprinting to enhance wireless security using nonparametric Bayesian method[C]// INFOCOM, 2011 Proceedings IEEE. IEEE, 2011:1404-1412.
17. Li Z, Xu W, Miller R, et al. Securing wireless systems via lower layer enforcements[C]// ACM Workshop on Wireless Security. ACM, 2006:33-42.
18. Shi Y, Jensen M A. Improved Radiometric Identification of Wireless Devices Using MIMO Transmission[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(4):1346-1354.
19. Das A, Borisov N, Caesar M. Do You Hear What I Hear?: Fingerprinting Smart Devices Through Embedded Acoustic Components[C]// ACM Sigsac Conference on Computer and Communications Security. ACM, 2014:441-452.
20. Dey S, Roy N, Xu W, et al. AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable[M]. 2014.
21. Breiman L I, Friedman J H, Olshen R A, et al. Classification and Regression Trees (CART)[J]. Encyclopedia of Ecology, 1984, 40(3):582-588.
22. Breiman L. Random Forests[J]. Machine Learning, 2001, 45(1):5-32.
23. Cortes C, Vapnik V. Support-vector networks[J]. Machine Learning, 1995, 20(3):273-297.
24. Hsu C W. A practical guide to support vector classification[J]. 2003, 67(5).
25. 周志华. 《机器学习》[J]. 中国民商, 2016(3).
26. Kohavi R. A study of cross-validation and bootstrap for accuracy estimation and model selection[C]// International Joint Conference on Artificial Intelligence. Morgan Kaufmann Publishers Inc. 1995:1137-1143.