References

[1] N. Eagle, “txteagle: Mobile crowdsourcing,” in *International Conference on Internationalization, Design and Global Development*. Springer, 2009, pp. 447–456.

[2] A. Vasilateanu, I. C. Radu, and A. Buga, “Environment crowd-sensing for asthma management,” in *2015 E-Health and Bioengineering Conference (EHB)*. IEEE, 2015, pp. 1–4.

[3] A. Sîrbu, M. Becker, S. Caminiti, B. De Baets, B. Elen, L. Francis, P. Gravino, A. Hotho, S. Ingarra, V. Loreto *et al.*, “Participatory patterns in an international air quality monitoring initiative,” *PLOS one*, vol. 10, no. 8, p. e0136763, 2015.

[4] Z. Xu, H. Zhang, V. Sugumaran, K.-K. R. Choo, L. Mei, and Y. Zhu, “Participatory sensing-based semantic and spatial analysis of urban emergency events using mobile social media,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, pp. 1–9, 2016.

[5] S. Konomi, K. Wakasa, M. Ito, and K. Sezaki, “User participatory sensing for disaster detection and mitigation in urban environments,” in *International Conference on Distributed, Ambient, and Pervasive Interactions*. Springer, 2016, pp. 459–469.

[6] Z. Liu, S. Jiang, P. Zhou, and M. Li, “A participatory urban traffic monitoring system: The power of bus riders,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2851–2864, 2017.

[7] P. Zhou, Z. Chen, and M. Li, “Smart traffic monitoring with participatory sensing,” in *Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems*, 2013, pp. 1–2.

[8] J. R. Douceur, “The sybil attack,” in *International workshop on peer-to-peer systems*. Springer, 2002, pp. 251–260.

[9] J. Borsub and P. Papadimitratos, “Hardened registration process for participatory sensing,” in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2018, pp. 281–282.

[10] B. Barrett, “An artist used 99 phones to fake a google maps traffic jam,” https://www.wired.com/story/99-phones-fake-google-maps-traffic-jam/, Feb. 2020.

[11] R. K. Ganti, F. Ye, and H. Lei, “Mobile crowdsensing: current state and future challenges,” *IEEE communications Magazine*, vol. 49, no. 11, pp. 32–39, 2011.

[12] I. F. Akyildiz and M. C. Vuran, *Wireless sensor networks*. John Wiley & Sons, 2010, vol. 4.

[13] D. Christin, “Privacy in mobile participatory sensing: Current trends and future challenges,” *Journal of Systems and Software*, vol. 116, pp. 57–68, 2016.

[14] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick, “A survey on privacy in mobile participatory sensing applications,” *Journal of systems and software*, vol. 84, no. 11, pp. 1928–1946, 2011.

[15] D. Christin, C. Büchner, and N. Leibecke, “What’s the value of your privacy? exploring factors that influence privacy-sensitive contributions to participatory sensing applications,” in *38th Annual IEEE Conference on Local Computer Networks-Workshops*. IEEE, 2013, pp. 918–923.

[16] CBSNEWs, “Did the internet kill privacy? facebook photos lead to a teacher losing her job; what expectations of privacy exist in the digital era?” http://www.cbsnews.com, 2011.

[17] CBCNEWs, “Depressed woman loses benefits over facebook photos,” ://www.cbc.ca.

[18] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, “SPPEAR: security & privacy-preserving architecture for participatory-sensing applications,” in *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*, 2014, pp. 39–50.

[19] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, “Shield: A data verification framework for participatory sensing systems,” in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2015, pp. 1–12.

[20] T. Giannetsos, S. Gisdakis, and P. Papadimitratos, “Trustworthy People-Centric Sensing: Privacy, Security and User Incentives Road-Map,” in *IEEE IFIP Mediterranean Ad Hoc Networking Workshop (IEEE IFIP MedHocNet)*, Piran, Slovenia, June 2014. doi: 10.1109/MedHocNet.2014.6849103 pp. 39–46.

[21] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, “Security, privacy, and incentive provision for mobile crowd sensing systems,” *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 839–853, 2016.

[22] M. Khodaei, H. Jin, and P. Papadimitratos, “SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,” *IEEE Transactions on Intelligent Transportation Systems (IEEE TITS)*, vol. 19, no. 5, pp. 1430–1444, May 2018. doi: 10.1109/TITS.2017.2722688

[23] M. Khodaei, H. Noroozi, and P. Papadimitratos, “Scaling Pseudonymous Authentication for Large Mobile Systems,” in *Proceedings of the 12th ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*, Miami, FL, USA, May 2019. doi: 10.1145/3317549.3323410. ISBN 978-1-4503-6726-4 pp. 174–185.

[24] M. Khodaei and P. Papadimitratos, “The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,” *IEEE Vehicular Technology Magazine (IEEE VT-Mag)*, vol. 10, no. 4, pp. 63–69, December 2015. doi: 10.1109/MVT.2015.2479367

[25] S. Gisdakis, M. LaganÃ, T. Giannetsos, and P. Papadimitratos, “SEROSA: Service Oriented Security Architecture for Vehicular Communications,” in *IEEE Vehicular Networking Conference (IEEE VNC)*, Boston, MA, USA, December 2013. doi: 10.1109/VNC.2013.6737597. ISSN 2157-9857 pp. 111–118.

[26] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, “Secure Vehicular Communication Systems: Design and Architecture,” *IEEE*

Communications Magazine, vol. 46, no. 11, pp. 100–109, November 2008. doi: 10.1109/MCOM.2008.4689252

[27] M. Khodaei and P. Papadimitratos, "Scalable & Resilient Vehicle-Centric Certificate Revocation List Distribution in Vehicular Communication Systems," *IEEE Transactions on Mobile Computing (IEEE TMC)*, vol. 20, no. 7, pp. 2473–2489, July 2021. doi: https://doi.org/10.1109/TMC.2020.2981887

[28] M. Khodaei and P. Papadimitratos, "Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs," in *11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*, Stockholm, Sweden, June 2018. doi: 10.1145/3212480.3212481. ISBN 9781450357319 pp. 172–183.

[29] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate Revocation List Distribution in Vehicular Communication Systems," in *ACM MobiCom Workshop on Vehicular Ad Hoc Networks (ACM VANET)*, San Francisco, CA, USA, September 2008, pp. 86–87.

[30] S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos, "Secure and Privacy-Preserving Smartphone-Based Traffic Information Systems," *IEEE Transactions on Intelligent Transportation Systems (IEEE ITS)*, vol. 16, no. 3, pp. 1428–1438, 2015. doi: 10.1109/TITS.2014.2369574

[31] M. Khodaei and P. Papadimitratos, "Cooperative Location Privacy in Vehicular Networks: Why Simple Mix-zones are not Enough," *IEEE Internet Of Things (IoT) Journal*, vol. 8, no. 10, pp. 7985–8004, May 2021. doi: https://doi.org/10.1109/JIOT.2020.3043640

[32] H. Zhang, D. She, and Z. Qian, "Android root and its providers: A double-edged sword," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 1093–1104.

[33] L. Webinar, "Api hooking," https://www.cynet.com/attack-techniques-hands-on/api-hooking/, Nov. 2020.

[34] L. Nguyen-Vu, N.-T. Chau, S. Kang, and S. Jung, "Android rooting: An arms race between evasion and detection," *Security and Communication Networks*, vol. 2017, 2017.

[35] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: A near-optimal social network defense against sybil attacks," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, 2008, pp. 3–17.

[36] A. Dua, N. Bulusu, W.-C. Feng, and W. Hu, "Towards trustworthy participatory sensing," in *Proceedings of the Usenix Workshop on Hot Topics in Security*, vol. 6, 2009.

[37] K. Mekliche and S. Moussaoui, "L-p2dsa: Location-based privacy-preserving detection of sybil attacks," in *2013 11th International Symposium on Programming and Systems (ISPS)*. IEEE, 2013, pp. 187–192.

[38] K. Rabieh, M. M. Mahmoud, T. N. Guo, and M. Younis, "Cross-layer scheme for detecting large-scale colluding sybil attack in vanets," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 7298–7303.

[39] A. Festag, P. Papadimitratos, and T. Tielert, "Design and Performance of Secure Geocast for Vehicular Communication," *IEEE Transactions on Vehicular Technology (IEEE TVT)*, vol. 59, no. 5, pp. 2456–2471, June 2010. doi: 10.1109/TVT.2010.2045014

[40] M. Poturalski, P. Papadimitratos, and J. P. Hubaux, "Formal Analysis of Secure Neighbor Discovery in Wireless Networks," *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, vol. 10, no. 6, pp. 355–367, November 2013. doi: 10.1109/TDSC.2013.17

[41] M. Fiore, C. E. Casetti, C. F. Chiasserini, and P. Papadimitratos, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing (IEEE TMC)*, vol. 12, no. 2, pp. 289–303, February 2013. doi: 10.1109/TMC.2011.258

[42] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Čapkun, and J.-P. Hubaux, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 132–139, February 2008. doi: 10.1109/MCOM.2008.4473095

[43] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, 2006, pp. 267–278.

[44] G. Wang, B. Wang, T. Wang, A. Nika, H. Zheng, and B. Y. Zhao, “Ghost riders: Sybil attacks on crowdsourced mobile mapping services,” *IEEE/ACM transactions on networking*, vol. 26, no. 3, pp. 1123–1136, 2018.

[45] N. Verchok and A. Orailoğlu, “Hunting sybils in participatory mobile consensus-based networks,” in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 2020, pp. 732–743.

[46] C. Gomez, J. Oller, and J. Paradells, “Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology,” *Sensors*, vol. 12, no. 9, pp. 11 734–11 753, 2012.

[47] M. Woolley, “Bluetooth core specification v5.1,” https://www.bluetooth.com/wp-content/uploads/2019/03/Bluetooth_5-FINAL.pdf/, Jan. 2019.

[48] A. A. Morgan, G. S. B. Humaid, and A. I. Moustafa, “Using bluetooth low energy for positioning systems within overcrowded environments: A real in-field evaluation,” *Computers & Electrical Engineering*, vol. 93, p. 107314, 2021.

[49] M. Demirbas and Y. Song, “An rssi-based scheme for sybil attack detection in wireless sensor networks,” in *2006 International symposium on a world of wireless, mobile and multimedia networks (WoWMoM’06)*. ieee, 2006, pp. 5–pp.

[50] Darvin, “Detecting magisk hide,” https://darvincitech.wordpress.com/2019/11/04/detecting-magisk-hide/, Apr. 2019.

[51] A. Developer, “Shrink, obfuscate, and optimize your app,” https://developer.android.com/studio/build/shrink-code, Feb. 2020.

[52] GuardSqure, “What is mobile application shielding,” https://www.guardsquare.com/mobile-application-shielding, Feb. 2020.

For DIVA

```
{
"Author1": {
        "Last name": "Li",
        "First name": "Ronghua",
        "Local User Id": "u100001",
        "E-mail": "ronghua@kth.se",
        "ORCiD": "0000-0002-00001-1234",
        "organisation": {"L1": "School of Electrical Engineering and Computer Science ",
                    }
       },
"Degree": {"Educational program": "Master’s Programme, Communication Systems, 120 credits"},
"Title": {
        "Main title": "Advanced Hardened Registration Process for Mobile Crowd Sensing",
        "Language": "eng" },
"Alternative title": {
        "Main title": "Avancerad Härdad registreringsprocess för Mobile Crowd Sensing",
        "Language": "swe"
},
"Supervisor1": {
            "Last name": "Eryonucu",
            "First name": "Cihan",
            "Local User Id": "u100003",
            "E-mail": "eryonucu@kth.se",
            "organisation": {"L1": "School of Electrical Engineering and Computer Science ",
                        "L2": "Computer Science" }
          },
"Examiner1": {
            "Last name": "Papadimitratos",
            "First name": "Panos",
            "Local User Id": "xxxxxxxxx",
            "E-mail": "papadigm@kth.se",
            "organisation": {"L1": "School of Electrical Engineering and Computer Science ",
                        "L2": "Computer Science" }
          },
"Other information": {
"Year": "2022", "Number of pages": "??,??"}
}
```