even when the operating system of the drone has been compromised. Liu *et al.* [20] investigate the problem of ensuring a drone has not strayed into no-fly zones. To do this, they leverage the TrustZone to keep a tamper-proof log of the drone's GPS locations, which then provide an alibi to a third-party auditor that the drone was in compliance. However, they do not consider the problem of ensuring that the drone respects a host's privacy policies when it is within permitted airspace.

ROS Security. There has been a modest amount of research into identifying the key security vulnerabilities of ROS, and proposals by which these can be overcome [9]. McClean *et al.* [21] analyzed ROS and identified a number of vulnerabilities such as plain text communication between nodes, unprotected TCP ports, unencrypted data storage and a lack of an authentication mechanism for nodes.

Some of the key security vulnerabilities within ROS are inherent in the publish-subscribe paradigm that it employs. Publishers are unable to control the consumption of their data, and subscribers are unable to verify the integrity of received messages. Rodriguez *et al.* [26] have proposed to use message level encryption between nodes and find that it is a feasible solution even for low-power robots. Prior work has also proposed integration of the ROSC++ package with TLS to provide end-to-end encrypted communication channels [9]. Dieber *et al.* [10] develop an authentication mechanism that allows publishers and subscribers verify each others' identities and establish the integrity of messages exchanged between them. These and similar enhancements are under consideration as part of the Secure ROS [32, 33] framework, which is under active development.

5 SUMMARY

Drones are now widely available and are soon proposed for use in commercial settings. These drones will pose a massive threat to security and privacy unless active steps are taken now to develop suitable policy regulations and enforcement technologies. This paper takes a step in that direction by proposing the notion of restricted spaces for drones and demonstrating an IFC-based mechanism to enforce privacy policies on drones.

Acknowledgments. We thank the reviewers for their comments and Silvia Santini for shepherding the paper. This work was supported in part by a Ramanujan Fellowship from the Government of India and by the Robert Bosch Centre for Cyber-Physical Systems.

REFERENCES

[1] FlytOS: Operating system for drones. https://flytbase.com/flytos/.
[2] MAVROS – MAVLink extendable communication node for ROS with proxy for ground control station. http://wiki.ros.org/mavros.
[3] 112th Congress. FAA Modernization and Reform Act of 2012, February 2012. https://www.congress.gov/112/plaws/publ95/PLAW-112publ95.pdf.
[4] ARM. Security technology building a secure system using TrustZone technology (white paper). *ARM Limited*, 2009.
[5] A. Azab, P. Ning, J. Shah, Q. Chen, R. Bhutkar, G. Ganesh, J. Ma, and W. Shen. Hypervision across worlds: Real-time kernel protection from the ARM TrustZone secure world. In *ACM Conference on Computer and Communications Security*, 2014.
[6] F. Brasser, D. Kim, C. Liebchen, V. Ganapathy, L. Iftode, and A-R. Sadeghi. Regulating ARM TrustZone devices in restricted spaces. In *ACM International Conference on Mobile Systems, Applications, and Services*, 2016.
[7] A. Cavoukian. *Privacy and drones: Unmanned aerial vehicles.* Information and Privacy Commissioner of Ontario, Canada Ontario, 2012.
[8] Civil Aviations Authority (CAA). CAP 722, Unmanned Aircraft System Operations in UK Airspace - Guidance, March 2015. https://publicapps.caa.co.uk/docs/33/CAP%20722%20Sixth%20Edition%20March%202015.pdf.
[9] B. Dieber, B. Breiling, S. Taurer, S. Kacianka, S. Rass, and P. Schartner. Security for the Robot Operating System. *Robotics and Autonomous Systems*, 98, 2017.
[10] B. Dieber, S. Kacianka, S. Rass, and P. Schartner. Application-level security for ROS-based applications. In *2016 IEEE International Conference on Intelligent Robots and Systems*, 2016.
[11] Directorate General of Civil Aviation. Requirements for Operation of Civil Remotely Piloted Aircraft System (RPAs), August 2018. http://dgca.nic.in/cars/D3X-X1.pdf.
[12] W. Enck, P. Gilbert, B-C. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. Sheth. Taintdroid: An information-flow tracking system for Realtime privacy monitoring on smartphones. In *ACM/USENIX Symposium on Operating System Design and Implementation*, 2010.
[13] Federal Aviation Administration (FAA). Small Unmanned Aircraft Systems (sUAS), June 2016. https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_107-2.pdf.
[14] K. Hartmann and C. Steup. The vulnerability of UAVs to cyber attacks-an approach to the risk assessment. In *IEEE International Conference on Cyber Conflict*, 2013.
[15] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *IEEE Conference on Technology for Homeland Security*, 2012.
[16] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys. Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, 31(4), 2014.
[17] C. Koettl and B. Marcolini. A closer look at the drone attack on Maduro in Venezuela, August 2018. https://www.nytimes.com/2018/08/10/world/americas/venezuela-video-analysis.html.
[18] M. Krohn, A. Yip, M. Brosdky, N. Cliffer, F. Kaashoek, E. Kohler, and R. Morris. Information flow control for standard os abstractions. In *ACM Symposium on Operating Systems Principles*, 2007.
[19] R. Liu and M. Srivastava. PROTC: Protecting drone's peripherals through ARM TrustZone. In *3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*, 2017.
[20] T. Liu, A. Hojjati, A. Bates, and K. Nahrstedt. Alidrone: Enabling trustworthy proof-of-alibi for commercial drone compliance. In *IEEE International Conference on Distributed Computing Systems*, 2018.
[21] J. McClean, C. Stull, C. Farrar, and D. Mascareñas. A Preliminary Cyber-Physical Security Assessment of the Robot Operating System (ROS). In *Unmanned Systems Technology XV*, volume 8741, 2013.
[22] A. Nadkarni, B. Andow, W. Enck, and S. Jha. Practical DIFC enforcement on Android. In *USENIX Security Symposium*, 2017.
[23] J-S. Pleban, R. Band, and R. Creutzburg. Hacking and securing the AR. Drone 2.0 quadcopter: investigations for improving the security of a toy. In *Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2014*, volume 9030, 2014.
[24] M. Quigley, K. Conley, B. Gerkey, J. Faust, T. Foote, J. Leibs, R. Wheeler, and A. Y. Ng. ROS: An open-source Robot Operating System. In *ICRA workshop on open source software*, 2009.
[25] Transparency Market Research. Robot Operating System Market - Snaphshot, 2018. https://www.transparencymarketresearch.com/robot-operating-system-market.html.
[26] F. J. Rodríguez-Lera, V. Matellán-Olivera, J. Balsa-Comerón, Á-M. Guerrero-Higueras, and C. Fernández-Llamas. Message Encryption in Robot Operating System: Collateral Effects of Hardening Mobile Robots. *Frontiers in ICT*, 5, 2018.
[27] R. Sailer, X. Zhang, T. Jaeger, and L. van Doorn. Design and implementation of a TCG-based integrity measurement architecture. In *USENIX Security Symposium*, 2004.
[28] S-H. Seo, J. Won, E. Bertino, Y. Kang, and D. Choi. A security framework for a drone delivery service. In *2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*, 2016.
[29] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler. Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In *Radionavigation Laboratory Conference Proceedings*, 2012.
[30] E. Vattapparamban, İ. Güvenç, A. İ Yurekli, K. Akkaya, and S. Uluağaç. Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In *2016 International Wireless Communications and Mobile computing Conference*, 2016.
[31] W. Wang, Y. Sun, H. Li, and Z. Han. Cross-layer attack and defense in cognitive radio networks. In *IEEE Global Communications Conference*, 2010.
[32] R. White, G. Caiazza, H. Christensen, and A. Cortesi. Using and developing secure ROS1 systems. In *Robot Operating System*, 2019.
[33] R. White, D. Christensen, I. Henrik, and D. Quigley. SROS: Securing ROS over the Wire, in the Graph, and through the Kernel. *arXiv preprint arXiv:1611.07060*, 2016.
[34] A. Young. Passenger jet carrying 240 people nearly hits a drone at 15,000ft, 2018. https://www.dailymail.co.uk/news/article-6172229/Passenger-jet-carrying-240-people-nearly-hits-drone-15-000ft.html.