a nie na domyślnych portach z określonych adresów IP, logowanie roota przez SSH powinno zostać wyłączone, powinno zostać wymuszone używanie silnych haseł uwierzytelniania na poziomie użytkownika, a także zapewnione szyfrowanie przechowywanych danych. Ponadto należy stosować metody starannej ochrony i wymiany kluczy kryptograficznych oraz utrzymania certyfikatów, obowiązkowych podpisów cyfrowych i poziomów dostępu, umożliwiających ich bezpieczne przechowywanie [37].

PODSUMOWANIE I PRZYSZŁE PERSPEKTYWY

Pomimo że ogólna poprawa cyberbezpieczeństwa robota nie jest prostym zadaniem, to ważne jest uwzględnienie od samego początku takich zaleceń jak: bezpieczne cykle życia oprogramowania, szyfrowanie komunikacji robota, aktualizowanie oprogramowania, udzielanie dostępu tylko autoryzowanym użytkownikom, dostarczanie metod przywracania robota do bezpiecznego stanu fabrycznego, wdrażanie najlepszych praktyk w zakresie bezpieczeństwa cybernetycznego, edukowanie osób zajmujących się rozwojem robotów i kadry kierowniczej w zakresie cyberbezpieczeństwa, zapewnianie użytkownikom możliwości wyrażania opinii na temat potencjalnych luk w zabezpieczeniach oraz promowanie audytów bezpieczeństwa przed fazą produkcji. W tym celu niezbędne jest egzekwowanie wczesnych i zapobiegawczych zasad bezpiecznego projektowania dla aplikacji robotów.

Celem tego rozdziału była identyfikacja potencjalnych zagrożeń dla bezpieczeństwa i prywatności w powszechnie stosowanym ROS, podnosząc w ten sposób świadomość na temat cyberbezpieczeństwa robotów i potrzebę dopracowania branżowych zasad bezpieczeństwa, tak aby uniknąć konsekwentnego wprowadzenia niepewnych robotów na rynek.

Oprócz dogłębnej analizy literatury dotyczącej bezpieczeństwa danych w robotyce ujawniono kilka błędów bezpieczeństwa w powszechnie przyjętym rozwiązaniu ROS oraz przedstawiono analizę propozycji mających na celu zabezpieczenie aplikacji robotów bazujących na ROS. Podano również ogólne zalecenia i środki bezpieczeństwa na różnych poziomach do kierowania wdrażaniem i rozlokowaniem systemów bazujących na jednym lub wielu robotach. W przyszłości planowane jest opracowanie komercyjnie użytecznego systemu opartego na ROS dla wielu robotów, który byłby przeznaczony do monitorowania infrastruktury obejmującej kluczowe środki bezpieczeństwa cybernetycznego i prywatności, w ramach trwającego projektu R&D STOP.

PODZIĘKOWANIA

Prace te były wspierane przez projekt badawczy **S**eguranças robó**T**icos co**OP**erativos (STOP) (ref. CENTRO-01-0247-FEDER-017562), współfinansowany przez „Agência Nacional de Inovação” w ramach programu Portugal2020.

Autorzy dziękują Bernhardowi Dieberowi z Joanneum Research, Institute for Robotics and Mechatronics, za dostarczenie kodu źródłowego *secure-ros-transport* oraz Ruffin White z University of California w San Diego za pomoc w zainstalowaniu *SROS*.

LITERATURA

1. E. Garcia, M. A. Jimenez, P. G. Santos, M. Armada, “The Evolution of Robotics Research”. *IEEE Robotics & Automation Magazine*, 14 (1), pp. 90–103, March 2007.

2. S. Morante, J. G. Victores, C. Balaguer, “Cryptobotics: Why Robots Need Cyber Safety”. *Frontiers in Robotics and AI*, 2 (23), pp. 1–4, September 2015.
3. T. Denning, C. Matuszek, K. Koscher, J. R. Smith, T. Kohno, “A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons”. In *11th International Conference on Ubiquitous Computing (UbiComp 2009)*, Orlando, Florida, USA, September 30–October 3, 2009.
4. N. Nevejans, “European Civil Law Rules in Robotics”. Study requested by the European Parliament’s Committee on Legal Affairs, *Policy Department C: Citizens’ Rights and Constitutional Affairs*, pp. 1–34, October 2016.
5. D. Portugal, M. S. Couceiro, R. P. Rocha, “Applying Bayesian Learning to Multi-Robot Patrol”. In *Proceedings of the 2013 International Symposium on Safety, Security and Rescue Robotics (SSRR 2013)*, Linköping, Sweden, October 21–26, 2013.
6. M. Quigley, B. Gerkey, K. Conley, J. Faust, T. Foote, J. Leibs, E. Berger, R. Wheeler, A. Ng, “ROS: An Open-Source Robot Operating System. In *Proceedings of the IEEE International Conference on Robotics and Automation (ICRA 2009), Workshop On Open Source Software*, Kobe, Japan, May 12–17, 2009.
7. C. Cerrudo, L. Apa, “Hacking Robots Before Skynet”. In *Cybersecurity Insight*, IOActive Report, Seattle, Washington, USA, 2017. https://media.scmagazine.com/documents/287/hacking-robots-before- skynet_71714.pdf
8. I. Asimov, *I, Robot*. Gnome Press, December 1950. https://en.wikipedia.org/wiki/I,_Robot
9. M. Finnicum, S. T. King, “Building Secure Robot Applications”. In *Proc. of the USENIX Workshop on Hot Topics in Security, 20th USENIX Security Symposium*, San Francisco, CA, USA, August 2011.
10. W. Adi, “Mechatronic Security and Robot Authentication”. In *IEEE Symposium on Bioinspired Learning and Intelligent Systems for Security (BLISS)*, Edinburgh, Scotland, pp. 77–82, August 20–21, 2009.
11. G. S. Lee, B. Thuraisingham, “Cyberphysical Systems Security Applied to Telesurgical Robotics”. *Computer Standards & Interfaces*, 34, pp. 225–229, 2012.
12. S. Yong, D. Lindskog, R. Ruhl, P. Zavarsky, “Risk Mitigation Strategies for Mobile Wi-Fi Robot Toys from Online Pedophiles”. In *Proc. of IEEE 3rd Int. Conf. on Privacy, Security, Risk and Trust and IEEE 3rd Int. Conf. on Social Computing*, Boston, MA, USA, October 2011.
13. A. Caiti, V. Calabrò, G. Dini, A. Lo Duca, A. Munafò, “Secure Cooperation of Autonomous Mobile Sensors Using an Underwater Acoustic Network”. *Sensors*, 12, pp. 1967–1989, 2012.
14. F. Higgins, A. Tomlinson, K. M. Martin, “Survey on Security Challenges for Swarm Robotics”. In *Proc. of the 5th International Conf. on Autonomic and Autonomous Systems*, Valencia, Spain, April 2009.
15. N. P. Hoand, D. Pishva, “A TOR-Based Anonymous Communication Approach to Secure Smart Home Appliances”. *ICACT Transactions on Advanced Communications Technology (TACT)*, 3 (5), pp. 517–525, September 2014.
16. T. Bonaci, J. Herron, T. Yusuf, J. Yan, T. Kohno, H. J. Chizeck, “To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robotics”, *arXiv: 1504:04339*, pp. 1–11, April 2015.
17. J. S. Pleban, R. Band, R. Creutzburg, “Hacking and Securing the AR. Drone 2.0 Quadcopter—Investigations for Improving the Security of a Toy”. In *Proc. of IS&T/SPIE Electronic Imaging*. The International Society for Optical Engineering, San Francisco, California, January 2014.
18. B. Friedman, “Value-Sensitive Design”. *Interactions*, 3(6), pp. 16–23, ACM, 1996.
19. J. Machado Santos, D. Portugal, R. P. Rocha, “An Evaluation of 2D SLAM Techniques Available in Robot Operating System”. In *Proc. of the 2013 International Symposium on Safety, Security and Rescue Robotics (SSRR 2013)*, Linköpping, Sweden, October 21–26, 2013.
20. R. Rusu, S. Cousins, “3D is Here: Point Cloud Library (PCL)”. In *Proceeding of the IEEE International Conference on Robotics and Automation (ICRA 2011)*, Shanghai, China, May 2011.
21. J. R. McClean, C. Stull, C. Farrar, D. Mascareñas, “A Preliminary Cyber-Physical Security Assessment of the Robot Operating System (ROS)”. In *Proc. of SPIE Defense, Security, and Sensing. The International Society for Optical Engineering*, Baltimore, Maryland, Vol 8741, May 2013.

22. V. Hax, N. Filho, S. Botelho, O. Mendizabal, "ROS as Middleware to Internet of Things". *Journal of Applied Computing Research*, 2(2), pp. 91–97, July–December 2012.
23. T. Schneider, "Distributed Networks Using ROS—Cross-Network Middleware Communication using IPv6". *Diploma Thesis*, Department of Electrical Engineering and Information Technology, Technical University of Munich, Munich, Germany, October 2012.
24. A. Tiderko, F. Hoeller, T. Röling, "The ROS Multimaster Extension for Simplified Deployment of Multi-Robot Systems". *Robot Operating System (ROS), The Complete Reference (Volume 1), Studies in Computational Intelligence*, 625, pp. 629–650, Sprinter 2016.
25. R. Dóczi, F. Kis, B. Sütő, V. Póser, G. Kronreif, E. Jósvai, M. Kozlovszky, "Increasing ROS 1. x Communication Security for Medical Surgery Robot". *In Proc. of the 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC 2016)*, pp. 4444–4449, Budapest, Hungary, October 2016.
26. G. Caiazza, "Security Enhancements of Robot Operating System". *Master Thesis*, Department of Environmental Sciences, Informatics and Statistics, Universitá Ca'Foscari Venezia, Venezia, Italy, 2016.
27. J. Huang, C. Erdogan, Y. Zhang, B. Moore, Q. Luo, A. Sundaresan, G. Rosu, "ROSRV: Runtime Verification for Robots". In *Runtime Verification (RV 2014)*. chapter Notes in Computer Science, vol 8734. Springer. https://link.springer.com/chapter/10.1007/978-3-319-11164-3_20
28. R. White, H. I. Christensen, M. Quigley, "SROS: Securing ROS Over the Wire, in the Graph, and through the Kernel". In *Humanoids Workshop: Towards Humanoid Robots OS (HUMANOIDS 2016)*, Cancun, Mexico, November 15, 2016.
29. F. Lera, J. Balsa, F. Casado, C. Fernández, F. Rico, V. Matellán, "Cybersecurity in Autonomous Systems: Evaluating the Performance of Hardening ROS". In *Proc. of the 17th Workshop of Physical Agents (WAF 2016)*, Malaga, Spain, June 16–17, 2016.
30. M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, L. E. Bassham, E. Roback, J. F. Dray Jr. "Advanced Encryption Standard (AES)". *Federal Inf. Process. Stds. (NIST FIPS)*, pp. 1–51, Report 197, November 2001.
31. A. Sundaresan, L. Gerard, M. Kim, "Secure ROS 0.9.2 documentation". Available at: https://sri-csl.github.io/secure˙ros. July 2017.
32. B. Dieber, S. Kacianka, S. Rass, P. Schartner, "Application-Level Security for ROS-Based Applications". *In Proc. of the 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2016)*, Daejeon, South Korea, October 9–14, 2016.
33. B. Breiling, B. Dieber, P. Schartner, "Secure Communication for the Robot Operating System". *In Proc. of the 2017 IEEE International Systems Conference (SysCon 2017)*, Montreal, QC, Canada, April 24–27, 2017.
34. B. Dieber, B. Breiling, S. Taurer, S. Kacianka, S. Rass, P. Schartner, "Security for the Robot Operating System". *Robotics and Autonomous Systems*, 98, pp. 192–203, Elsevier, the Netherlands, December 2017.
35. C. Crick, G. Jay, S. Osentosiki, B. Pitzer, O. C. Jenkins, "Rosbridge: ROS for Non-ROS Users". In *Proc. of the 15th International Symposium on Robotics Research (ISRR)*, Flagstaff, AZ, USA, August 28– September 1, 2011.
36. R. Toris, C. Shue, S. Chernova, "Message Authentication Codes for Secure Remote Non-Native Client Connections to ROS Enabled Robots". In *Proc. of the 2014 IEEE International Conference on Technologies for Practical Robot Applications (TePRA)*, Woburn, MA, USA, April 14–15, 2014.
37. D. Portugal, S. Pereira, M. S. Couceiro, "The Role of Security in Human-Robot Shared Environments: *A Case Study in ROS-based Surveillance Robots*". In *Proc. of the 26th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN 2017)*, Lisbon, Portugal, August 28– September 1, 2017.