R

Robots

Marie-Helen Maras

Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords

Robots · Critical infrastructure · Privacy · Security

Definition

Robots are machines with computer software that are designed to automatically perform a variety of noncomplex and/or complex tasks.

Introduction

Robots are machines with computer software that are designed to automatically perform a variety of noncomplex and/or complex tasks. Some robots look like machines (e.g., SoftBank Robotics' Pepper and Knightscope's Rosie), while others are anthropomorphic (e.g., Hanson Robotics' Sophia) (Fouraker 2018; Son 2018). Robots are deployed in public and private sectors around the world to cut costs associated with human labor and to enhance the efficiency of operations. Robots are

predominately built to enable their real-time and remote access for efficiency purposes. The real-time and remote access of robots adversely impacts the security of these objects and the privacy of data aggregated, analyzed, and shared by these objects.

Robots in Critical Infrastructure Sectors

Robots have been deployed in many critical infrastructure sectors for a variety of reasons. In the commercial sector, robots are used in certain sub-sectors, such as retail and lodging. For example, robots have been used in the hospitality industry (e.g., hotels). Japan is famous for its hotels with robots, which not only check-in guests, clean rooms, store luggage, and bring luggage and other items to guests' rooms, but are also located within the guests' rooms to provide them with services (Choi et al. 2020; Malaea 2019). During the 2020 coronavirus pandemic, robots were used in Japan to greet coronavirus patients placed within hotels (Reuters 2020). Some US hotels also use robots to deliver items to guests' rooms, among other activities (Martin 2016). In addition, robots have been used in the: healthcare sector to conduct remote robotic assisted surgeries; manufacturing of goods, such as cars and digital technology; financial sector for customer service (e.g., Pepper has been deployed in HSBC banks branches); transportation sector, particularly the airports to provide travelers with flight and airport

information and to clean airports; and defense sector, where robots deliver goods and services, and even medical care in battlefields (Son 2018; Fouraker 2018; Babe 2017; Holmes 2020; D'Monte 2015; Creswell et al. 2018; Beiser 2018; Sykes 2018).

Moreover, robots are used for security and emergency management purposes. For instance, Talon and PackBot robots are used in border security to investigate tunnels found at the US border, which are used to illegally smuggle drugs, weapons, and people into the country (McNeill and Machi 2009). These robots conduct reconnaissance and can relay information about what they find back to the agency that is using them. Furthermore, robots are used in natural and human-made disaster response because they can traverse hazardous terrains and provide relief and/or monitor locations where it is unsafe for humans to be (e.g., locations with extreme radiation levels that would cause harm to human beings).

Security Concerns

Many robots were not built with cybersecurity and/or security in mind. Because of this, robots are susceptible to cybersecurity threats because they can be remotely accessed for maintenance and operation. A case in point are the vulnerabilities identified in the in-room robots of Japan's HIS Group hotel chain. Specifically, the vulnerabilities enabled remote access to the in-room robots and enabled perpetrators to control the camera and microphone in order to see and listen to the guests in the rooms (Parrish 2017). Robots interact with their immediate environments and collect and process contextual information to operate within these environments. These operations result in the vast collection, processing, and ultimately sharing of contextual information. The privacy implications of the collection of these vast quantities of data needs to be considered.

Robots are further vulnerable to supply chain risks, from the design of the product, to its development, to the creation of the final product. One such risk involves vendors that provide critical components for robots (e.g., microcontroller).

For instance, outsourcing these components to a company that is located in a foreign country can provide the foreign country with the ability to introduce a hardware vulnerability that could be exploited by the country at a later date. Software or hardware with malware may also be used to create the robots and/or the software applications used with robots may be vulnerable to cyberattacks. Vulnerabilities in third party applications required for the monitoring and remote operation of robots may also be present. Interconnections of robots to other digital technologies, and even other robots, create new vulnerabilities. These vulnerabilities include the interception of data being transferred, the surreptitious monitoring of data, and the gaining of unauthorized access to the administrative capabilities of the robots. The vulnerabilities enable perpetrators to surveil the environment within which they operate and/or control the functions of the robots in order to modify, disable, or otherwise interfere with the normal functioning and operations of the robots.

Finally, robots may not operate as intended and/or may malfunction, resulting in damage to property, injury, serious harm, and/or death. There have been several instances of maloperations and malfunctioning of robots. In Alabama, a woman in a factory, Ajin USA plant, was crushed to death by a car-robot, when it restarted as she was trying to determine why it malfunctioned (Silverman 2017). In California, a mall security robot knocked a toddler down and ran him over in the Stanford Shopping Center (McFarland 2016). The toddler sustained minimal injury to the leg. Surgical robots have also malfunctioned causing minor and major injuries, even death (BBC 2015).

Conclusion

The security concerns regarding robots involve both the data processed, stored, communicated, and shared by the robot, and the unauthorized access and use of the robot. Data obtained, processed, and transmitted by the robots should be secured, encrypted, or otherwise obfuscated to protect the confidentiality and integrity of data. Robot security can be implemented at the design

level by creating secure firmware and software. Any default usernames and passwords, wherever present, should be changed by the users or operators of the robots. Because unauthorized access to robots can destroy, disrupt, and degrade robot capabilities and operations, robots should be developed in a manner that enables them to withstand cyberattacks.

Cross-References

► Cybersecurity: Practice

References

- Babe, A. (2017). Why South Korea is an ideal breeding ground for robots. *BBC News*, 6 Dec 2017. <http://www.bbc.com/travel/story/20171205-why-south-korea-is-an-ideal-breeding-ground-for-robots>
- BBC. (2015). Robotic surgery linked to 144 deaths in the US. <https://www.bbc.com/news/technology-33609495>
- Beiser, V. (2018). The robot assault on Fukushima. *Wired*, 26 Apr 2018. <https://www.wired.com/story/fukushima-robot-cleanup/>
- Choi, C., Oh, M., Choi, M., & Kim, S. (2020). Exploring the influence of culture on tourist experiences with robots in service delivery environment. *Current Issues in Tourism*. <https://doi.org/10.1080/13683500.2020.1735318>.
- Creswell, K., Cunningham-Burley, S., & Sheikh, A. (2018). Health care robotics: Qualitative exploration of key challenges and future directions. *Journal of Medical Internet Research*, 20(7), e10410. <https://doi.org/10.2196/10410>.
- D'Monte, L. (2015). 5 Robots that may rescue you from natural disasters. *Government Technology*, 2 June 2015. <https://www.govtech.com/em/safety/5-Robots-That-May-Rescue-You-From-Natural-Disasters.html>
- Fouraker, C. (2018). Robotic security forces on patrol in NYC prompt privacy concerns for some. *CBS New York*, 16 Oct 2018. <https://newyork.cbslocal.com/2018/10/16/knightscope-robot-security-patrol/>
- Holmes, A. (2020). Police robots keep malfunctioning, with mishaps ranging from running over a toddler's foot to ignoring people in distress. *Business Insider*, 19 Jan 2020. <https://www.businessinsider.com/police-robots-security-malfunctioning-fails-knightscope-2020-1>
- Malaea, M. (2019). Quirky Japanese hotel replaces in-room robots when they turn out to be hackable can be turned into peeping toms. *Newsweek*, 23 Oct 2019. <https://www.newsweek.com/quirky-japanese-hotel-replaces-room-robots-when-they-turn-out-hackable-can-turned-peeping-toms-1467386>
- Martin, H. (2016). Cutting edge: Robots deliver fun with hotel room service orders, and they don't expect a tip. *LA Times*, 7 Feb 2016. <https://www.latimes.com/business/la-fi-hotel-robots-20160207-story.html>
- McFarland, M. (2016). 300-Pound mall robot runs over toddler. *CNN*, 14 July 2016. <https://money.cnn.com/2016/07/14/technology/robot-stanford-mall/index.html>
- McNeill, J. B., & Machi, E. (2009). Robotics and the next steps for national security. *Heritage Foundation*. <https://www.heritage.org/node/13925/print-display>
- Parrish, M. (2017). Massive industrial robots vulnerable to being hacked. *Manufacturing.net*, 3 May 2017. <https://www.manufacturing.net/industry40/news/13116550/massive-industrial-robots-vulnerable-to-being-hacked>
- Reuters. (2020). Robots on hand to greet Japanese coronavirus patients in hotels. <https://www.reuters.com/article/us-health-coronavirus-japan-robot-hotels/robots-on-hand-to-greet-japanese-coronavirus-patients-in-hotels-idUSKBN22D4PC>
- Silverman, G. (2017). A death in Alabama exposes the American factory dream. *The Financial Times*, 5 Feb 2017. <https://www.ft.com/content/54d05c3e-e9fa-11e6-893c-082c54a7f539>
- Son, H. (2018). This bank is staffing branches with humanoid robots that dance, take selfies and push credit cards. *CNBC*, 26 June 2018. <https://www.cnbc.com/2018/06/26/this-bank-is-staffing-branches-with-humanoid-robots-that-dance-take-s.html>
- Sykes, N. (2018). How manufacturing automation is evolving. *Robotics Business Review*, 7 Mar 2018. <https://www.roboticsbusinessreview.com/manufacturing/how-manufacturing-automation-is-evolving/>

Further Reading

- European Parliament. (2018). Civil law rules on robotics. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (2018/C 252/25). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051&from=EN>
- Jordan, J. (2016). *Robots*. Cambridge, MA: MIT Press.