Cyber Security of Social Robots and the Internet of Things

Matthew Kinzler | Dr. Debbie Perouli | Marquette University

Purpose

The purpose of this research is to take the first steps in securing social robots against malicious activity.
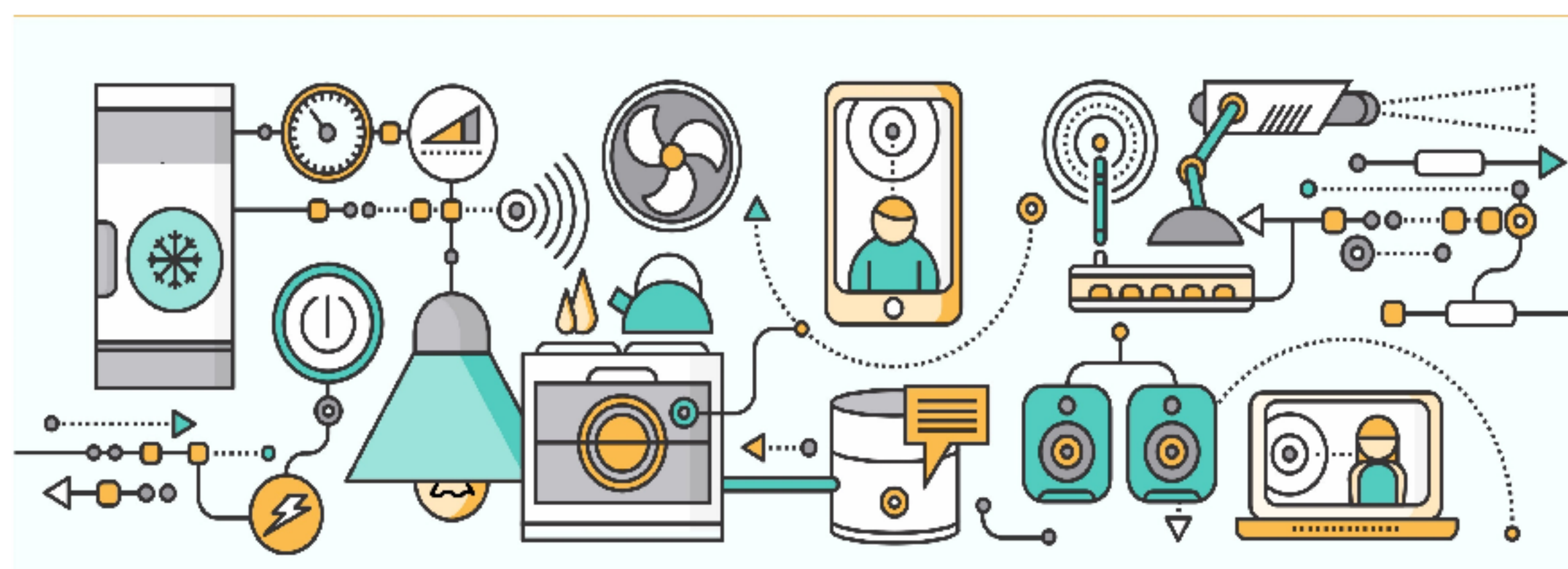
Definitions

- Social Robots – Robots designed specifically to interact with humans and other social robots
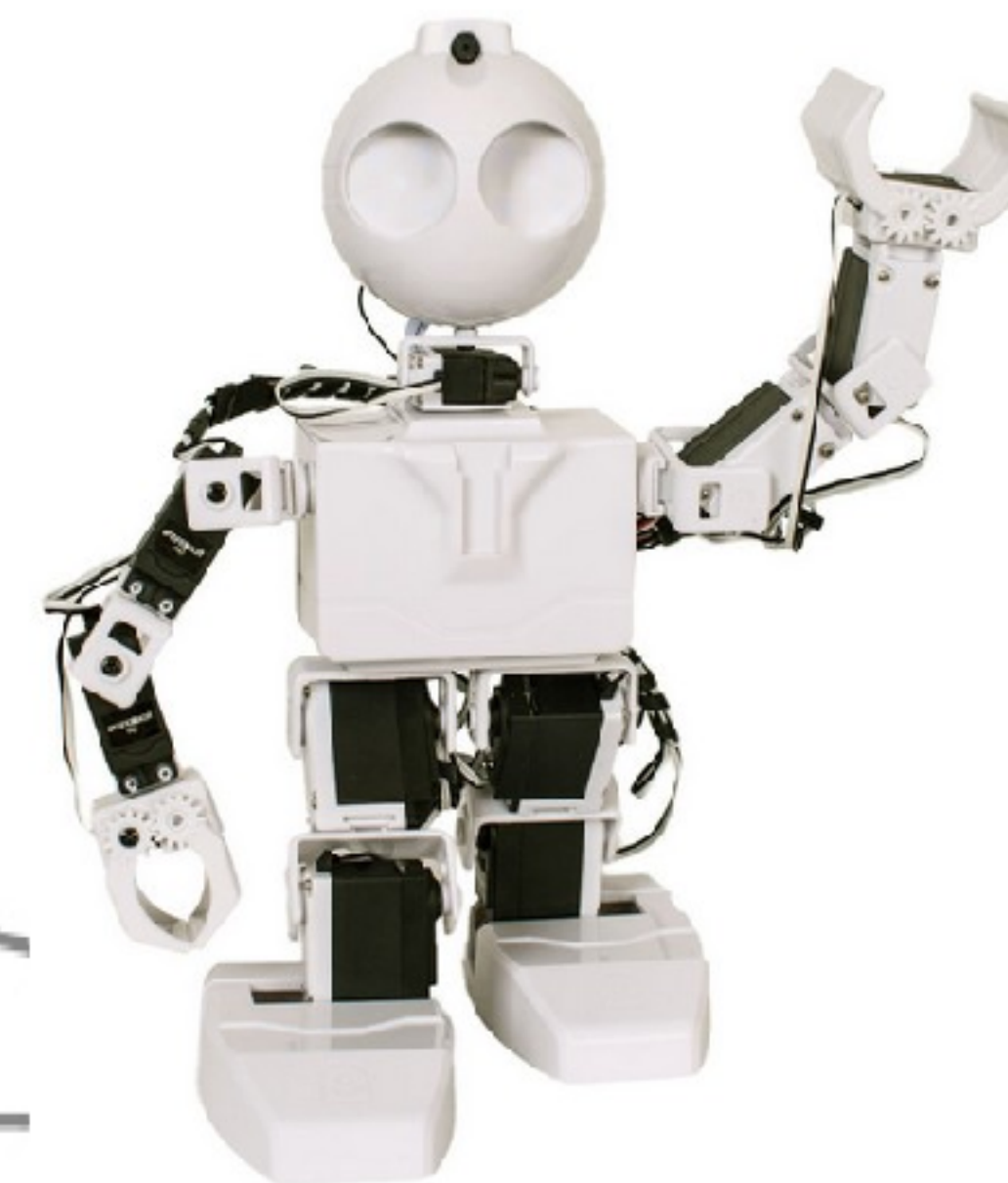
Source: www.heykuri.com

- Internet of Things (IoT) – Devices that collect data and are accessible through the internet
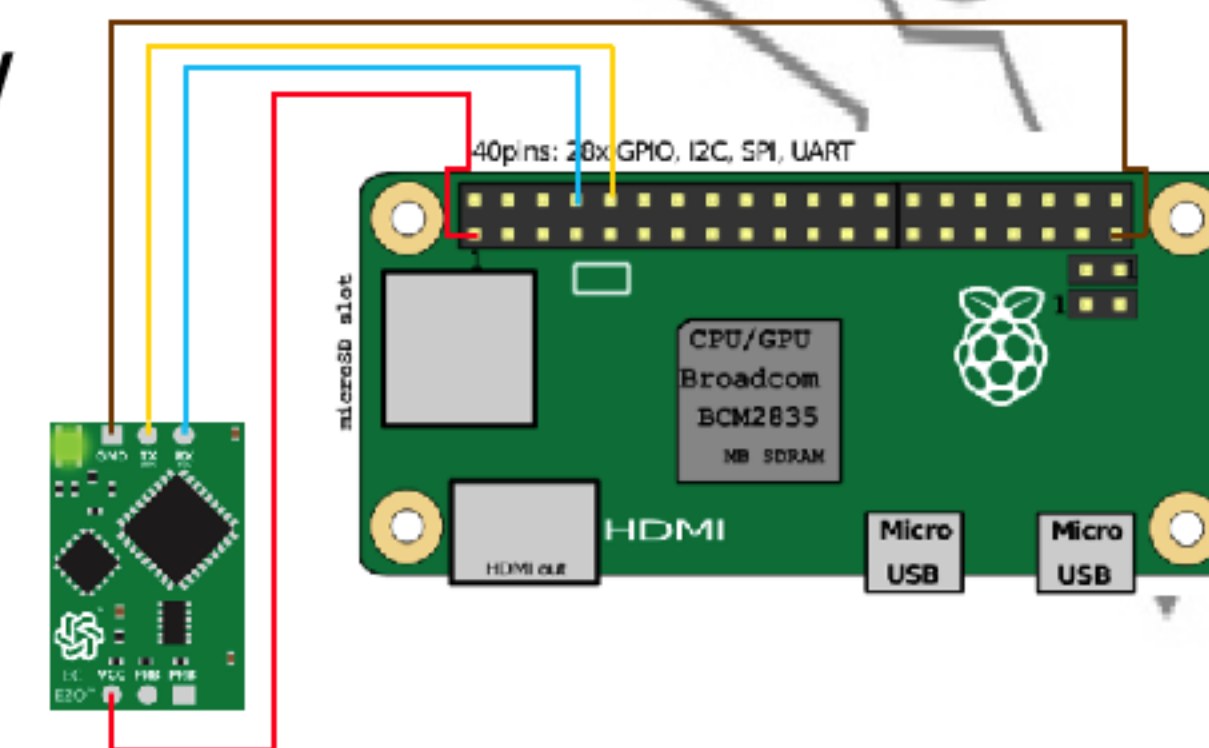
Source: www.computerweekly.com

The Research Environment

- JD-Humanoid Robot
- Made by EZ-Robot

Source: www.solvelight.com

- Raspberry Pi Zero W
- EZO Conductivity Circuit

- All of these devices are connected to each other through the cloud via Ubidots

Results

- Backup and retrieval to/from the cloud has option for HTTPS (encrypted) protocol

- Login to Raspberry Pi requires username and password

- Discovered security vulnerabilities related to the social robot

- Established connection allows for extensive options

```
help: What you see now
version: Display hw/sw version
exit: CLI exit
scan: scan ap
wifistate: Show wifi state
ifconfig: Show IP address
arp: arp show/clean
ping: ping <ip>
dns: show/clean/<domain>
sockshow: Show all sockets
tasklist: List all thread name status
memshow: Print memory information
memdump: <addr> <length>
memset: <addr> <value 1> [<value 2> ... <value n>]
memp: Print memp list
wifidriver: Show wifi driver status
reboot: Reboot EZ-B
reset: Reset to default configuration
ugf: Start firmware upgrade
time: Show system time
flash: Flash memory map
identify: Identify EZ-B with flashing LED and Audio Beep
servo: Move a servo
servospeed: Set Servo Speed
set: Set digital port state
bs: Show Highest Buffer Sizes
```

- Uses Telnet (unencrypted) with no password

- The programs run on the windows computer and send commands to the robot

- We strongly support the addition of an authentication mechanism implemented on the robot controller

Most Important References

- [1] Kali.org, 'Our Most Advanced Penetration Testing Distribution, Ever.', 2017. [Online]. Available: https://www.kali.org/ [Accessed 24 July 2017].
- [2] *EZ-Bv4 Datasheet*, EZ-Robot, 2016. [Online]. Available: https://www.ez-robot.com/Tutorials/Files/EZ-Bv4%20Datasheet.pdf. [Accessed 24 July 2017]
- [3] Denning, Tamara, et al. "A spotlight on security and privacy risks with future household robots: attacks and lessons." Proceedings of the 11th international conference on Ubiquitous computing. ACM, 2009

Acknowledgements