IoT and Security

Data Security ICT4TF022-3008

Melissa Westberg

What is IoT

- Things that are connected to the internet but sometimes have been ''dumb'' but are now ''smart''
  - Smart watches, smart TVs, smart appliances, smart pacemakers…
  - Smart homes in general, thermostats, lights…
  - Smart cars
- Sensors, surveillance cameras, baby monitors, wireless heart monitors, insulin dispensers…
- IIoT: industrial IoT
  - Used to boost up efficiency

Sources: https://www.ic3.gov/Media/PDF/Y2015/PSA150910.pdf, https://internetofthingsagenda.techtarget.com/definition/IoT-device

IoT security breach examples

- Mirai Botnet: DDoS attack used against Dyn (has DNS infrastructure services) in 2016
  - Mirai-infected computers search for more vulnerable IoT devices (many have default login information, non-unique passwords, vulnerable firmware, no security patches…) which are then used for DDoS
- FDA confirmed St. Jude Medical's implantable cardiac devices that could allow a hacker to access a device
  - Battery depletion, incorrect pacing, shocks
  - Vulnerability in the transmitter that reads the device's data and remotely shares it
- The Owlet WiFi Baby Heart monitor
  - Has sensor in baby's sock, sensor relays data wirelessly to a nearby hub. The hub can ping out an alert to parent's phone (via manufacturer's server).
  - From hub to manufacturer's server data is encrypted. The adhoc WiFi network linking hub and sensor is unencrypted and requires no authentication, i.e. the hub has its own unlocked WiFi network anyone can access.

Sources: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities, https://www.theregister.com/2016/10/13/possibly_worst_iot_security_failure_yet/?mt=1476453928163

IoT security breach examples

- The TRENDnet Webcam Hack: faulty software
  - Anyone with camera's IP address could look through the camera (and sometimes listen).
  - Credentials were transmitted in cleartext over the internet and stored on the mobile devices
- The Jeep Hack: firmware vulnerability
  - Researchers took total control over (speed up, veer off the road…) the car via vehicle's CAN bus (car's internal network, interconnects engine, transmission, sensors…)
  - First hack the multimedia system through WiFi connection (password autogenerated based on time), after connected to head unit, hack multimedia computer and control the music player. Multimedia system is undirectly connected to the CAN bus via another controller.
  - Researchers changed controller firmware (no checks or authorization needed) that allowed to take control of the CAN bus and control the car.

Sources: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities, https://www.technewsworld.com/story/webcam-maker-takes-ftcs-heat-for-internet-of-things-security-failure-78891.html, https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

What should be done?

- "Don't overconnect your systems, don't trust a locally compromised or accessible device, and do subject your code and hardware to third-party penetration testing, both in blackbox and whitebox variants".
- "Devices that cannot have their software, passwords, or firmware updated should never be implemented."
- "Changing the default username and password should be mandatory for the installation of any device on the Internet."
- "Passwords for IoT devices should be unique per device, especially when they are connected to the Internet."
- "Always patch IoT devices with the latest software and firmware updates to mitigate vulnerabilities."

Sources: https://www.technewsworld.com/story/webcam-maker-takes-ftcs-heat-for-internet-of-things-security-failure-78891.html, https://uk.pcmag.com/business/87031/the-5-worst-hacks-and-breaches-of-2016-and-what-they-mean-for-2017

What should be done?

FBI recommendations:

- Isolate IoT devices on their own protected networks
- Disable UPnP on routers
- Consider whether IoT devices are ideal for their intended purpose
- Purchase IoT devices from manufacturers with a track record of providing secure devices
- When available, update IoT devices with security patches
- Consumers should be aware of the capabilities of the devices and appliances installed in their homes and businesses. If a device comes with a default password or an open Wi-Fi connection, consumers should change the password and only allow it operate on a home network with a secured Wi-Fi router
- Use current best practices when connecting IoT devices to wireless networks, and when connecting remotely to an IoT device
- Patients should be informed about the capabilities of any medical devices prescribed for at-home use. If the device is capable of remote operation or transmission of data, it could be a target for a malicious actor
- Ensure all default passwords are changed to strong passwords

Sources: https://www.ic3.gov/Media/PDF/Y2015/PSA150910.pdf