An Exploration and Cybersecurity Evaluation of IoT Healthcare Devices

Shababa Kamreen
School of Science and Technology
Georgia Gwinnett College
skamreen@ggc.edu

Michael Eakins
METIL, IST
University of Central Florida
meakins@ist.ucf.edu

Dr. David Metcalf & Dr. Barbara Truman
METIL, IST
University of Central Florida
{dmetcalf, brtruman}@ist.ucf.edu

Objective: To examine the security risks of IoT healthcare devices based on NIST Risk Management Framework

Abstract

In 2019, it is expected that 1.9 billion smart home devices are going to be shipped for consumers [1]. These devices, ranging from mobile phones to cars, all connected to the internet, are part of a network called the Internet of Things (IoT). These can be used for a variety of purposes, from reporting back the location of a patient to a caregiver to even sending reminder alerts to a patient to get more Vitamin D. Offering a connection to the internet can cause security risks, which are a paramount concern among most people these days due to the prevalence of these devices. In regard to this, the Internet of Things in the healthcare world is a particular network to be interested in. The impact of insecure data and false information in the healthcare world, could have far-reaching consequences on patients' health and increase the possibility of their health deteriorating. Giving patients suggestions on what device to aid them to take care of their own health and having the company implement proper security policies could help to mitigate this problem. Information about health care wearables and software on sites including common search engines, Amazon, CNET, and company websites, were found to help the elderly. These same devices were evaluated based on the National Institute of Standards and Technology's Risk Management Framework to provide companies and patients with accurate information to operate in their own domains.

Methodologies

The following resources were analyzed to base the evaluation:

- **NIST Risk Management Framework** is a method that incorporates risk management processes into business functions and through the system development lifecycle.
- **Pentest-tools' Website Vulnerability Scanner** is an online tool that scans passively for website vulnerabilities.
- **Upguard's Cloud Scanner** is an online tool that checks for security risks.
- **Qualys SSL Labs' SSL Server Test** shows details of SSL web server of a website.

Acknowledgment

The support for this work was provided by the National Science Foundation REU program under Award No. 1560302. Any opinions, findings, and conclusions and recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Initial Results

Wearable Device, Company	Business Mission	Product Description	Impact of CIA Loss	Security Overview	Recommendations
Garmin vivofit Fitness Band, Garmin	To be a long-lasting company that delivers quality products through honesty, integrity, and respect	Tracks steps, calories, sleep and generates a customized goal	*Confidentiality: Moderate, Integrity: High, Availability: High*	Lacks non-repudiation and auditing with Bluetooth 4.0, Public key cryptography is used for device authentication, ANT+'s device encryption and authentication is weak	Use the last security level associated with Bluetooth and increase confidentiality
Mindme Locate, Mindme	To give dementia independence and caregivers a peace of mind through GPS tracking	Locates position of wearer, position can be seen through website	*Confidentiality:* High, *Integrity*: High, *Availability*: High	Device: SIM chip provides an extra layer of authentication, Website: HTTP protocol used, buffer overflow vulnerability due to IIS 6.0 used	Upgrade to the latest version of IIS, use HTTPS, X-XXS, X-Content Type Options, set Sender Policy Framework to -all
Leaf Health Tracker, Bellabeat	To inspire and motivate women to be the best version of themselves through technology	To track different activities, steps, calories, or reproductive activity through the tracker and app	*Confidentiality:* Moderate, *Integrity*: High, *Availability*: High	Bluetooth prior to version 4.2 uses AES-128 algorithm, Bluetooth version 4.2 and after uses P-256 Elliptic Curve with AES- CMAC. Both not protected from Man-in-the-Middle attacks [2].	Encourage users to use Bluetooth 4.2 and after for better security and provide protection against Man-in-the-Middle attacks.
Qsun, Comfable Inc	To help people live healthier in a green environment	Displays amount of Vitamin D user makes, monitors UV rays from sun	*Confidentiality:* Moderate, *Integrity*: High, *Availability*: High	Uses Bluetooth Low Energy, which can prevent tracking through changing private addresses and is not protected from Man-in-the-Middle attacks [2].	Provide protection against Man-in-the-Middle attacks
Lively Wearable, GreatCall	To provide good outcomes to help seniors live independent lives	Tracks steps and looks out for falls	*Confidentiality:* High, *Integrity*: High, *Availability*: High	Uses Bluetooth 4.1, which uses AES-128 algorithm	Make connectivity to be compatible with Bluetooth 4.2, provide secure communications to prevent eavesdropping

[1] **THE CONNECTED-HOME REPORT: Forecasts and growth trends for one of the top 'Internet of Things' markets**
Tony Danova - http://www.businessinsider.com/connected-home-forecasts-and-growth-report-2015-4

[2] D. Celebucki, M. A. Lin, and S. Graham, "A security evaluation of popular Internet of Things protocols for manufacturers," *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 2018.