An Analysis on Medical Device Recalls and Cybersecurity
Implications on Patient Safety

Rachel N. Leone  
*Boise State University*

Liljana Babinkostova  
*Boise State University*

Marion Scheepers  
*Boise State University*

Kristen Garcia  
*Boise State University*

Sulema Jimenez  
*Boise State University*

See next page for additional authors
An Analysis on Medical Device Recalls and Cybersecurity Implications on Patient Safety

Abstract
According to the Food and Drug Administration (FDA) a recall is the removal or correction of medical devices that do not abide by the laws governed by the FDA and threaten patient health and safety. A Class I recall is the most severe and shows the most significant danger of death, while Class II and III are intermediate and low levels of danger. The main issues with medical device recalls include the interference of patient health and adherence to treatment for different diseases. Software issues were the number one cause of medical device recalls in 2019. As more devices connect to the internet, issues with cybersecurity have become more prominent. Although there are currently no reported malicious attacks to these devices, it is possible to exploit these vulnerabilities to deplete batteries, affect drug dosing, or access private health data. Our goal is to compile the FDA reports from the medical device recalls and run statistical tests to determine if there is a significant increase in cybersecurity vulnerabilities. In addition, we are compiling resources from health organizations regarding protocol to respond to cybersecurity incidents in medical devices and develop a cyber-awareness framework for patients, manufacturers, and product developers. Improving the security of medical devices is vital to ensuring patient health, safety, and privacy.

Authors
Rachel N. Leone, Liljana Babinkostova, Marion Scheepers, Kristen Garcia, Sulema Jimenez, and Tabarak Alomar

This student presentation is available at ScholarWorks: https://scholarworks.boisestate.edu/under_showcase_2020/104
INTRODUCTION

According to the Food and Drug Administration (FDA) a recall is the removal or correction of medical devices that do not abide by the laws governed by the FDA and threaten patient health and safety [1]. Even though medical devices have become more advanced and are able to connect to networks and other devices, cybersecurity has become an issue while ensuring proper patient care. A recent study examined cybersecurity attacks in medical devices, then characterized the vulnerabilities based on reports from the CVE and ICS-CERT databases [3]. This analysis of FDA reports [2] are the preliminary actions to categorize medical device recalls and eventually connect them to potential cybersecurity vulnerabilities.

METHODS AND DATA

Data was collected from the FDA Medical Device Recall Database from January 2010-March 2020 by entering “software” and “hardware” reasons into the search engine and yielded approximately 1300 results. The total number of software and hardware-related device recalls is shown by year in Figure 1.

The entries from the top ten manufacturers were categorized by utilizing a keyword-based method the manufacturer’s reason for recall. Keywords were manually grouped together into categories, shown in Table 1. The proportions of these categories are shown in Figure 3.

<table>
<thead>
<tr>
<th>Category</th>
<th>Keyword Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple</td>
<td>“multiple issues”, “numerous issues”</td>
</tr>
<tr>
<td>Incorrect Data</td>
<td>“incorrect values”, “error in”</td>
</tr>
<tr>
<td>Loss of data</td>
<td>“delayed diagnosis”, “exam to fail”</td>
</tr>
<tr>
<td>Images and Results</td>
<td>“rescans”, “same image”</td>
</tr>
<tr>
<td>Patients</td>
<td>“wrong patient”, “mishandled”</td>
</tr>
<tr>
<td>Damages</td>
<td>“thermal damage”, “overheating”</td>
</tr>
<tr>
<td>Software</td>
<td>“upgrade”, “updated”</td>
</tr>
<tr>
<td>System Processing</td>
<td>“system crash”, “no access”</td>
</tr>
<tr>
<td>Saving</td>
<td>“not saved”, “confusion”</td>
</tr>
<tr>
<td>Other</td>
<td>“position sensor”, “mishandling”</td>
</tr>
</tbody>
</table>

CONCLUSION/FUTURE WORK

• Our preliminary results indicate that there are many types of medical devices and reasons for recall. The manufacturer’s reason for recall is more specific than the FDA’s reason, so patients may not understand the errors in their devices and the impact these errors can have on their safety and privacy due to the report. Therefore, using the manufacturer’s reason may provide more transparency for the patient.

• Develop a Natural Processing Language (NPL) software to categorize current and future recalls into a more manageable database for ease of patient access, while also linking these reasons for recall to the CVE and ICS-CERT classifications of software and cybersecurity malfunctions.

REFERENCES


ACKNOWLEDGEMENTS

This research was supported by NSF REU Site Grant DMS-1659867. We thank the Boise State College of Innovation and Design for their support of the project as well as our mentors Dr. L. Babinkostova, R. Erbes (Idaho National Lab), J. Radcliffe (Thermo Fisher Scientific), and Dr. M. Scheepers. We would also like to thank D. Leone, D. Valiente, and G. Frandsen for discussing our data analysis.