Maude Miner

Mining FDA's MAUDE Dataset for Security Events

Thomas Lovett, Denis Foo Kune, Kevin Fu
University of Michigan

UNIVERSITY OF MICHIGAN

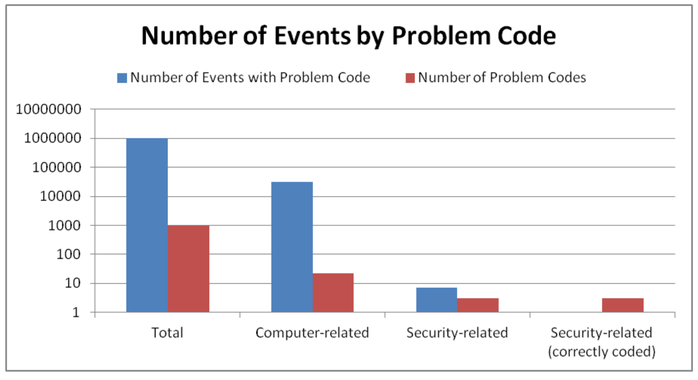
SPQR
https://spqr.eecs.umich.edu

Problem and Motivation

Security in medical devices is a growing problem[1]. The Food and Drug Administration (FDA) provides the Manufacturer and User Facility Device Experience (MAUDE) database [2] to report adverse events, including security incidents. There are 2 main problems:

1. The search capabilities are limited (mostly keywords)
2. Clinicians recording the event are not trained in security.

The second issue results in sparse (if any) use of security-related problem codes, making it difficult searches for security events harder and compounding the first problem.



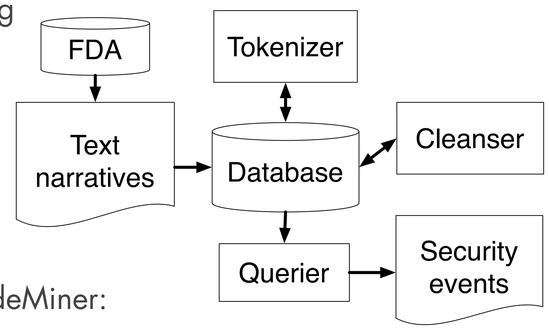
3 of 986 Device Problem Codes related to security issues:
- Application Security Issue (2882)
- Computer System Security Issue (2899)
- Unauthorized access to computer System (3025)

References:
[1] G. McGraw. Software security: building security in volume 1. Addison-Wesley Professional, 2006.
[2] U.S. Food and Drug Administration. Maude -manufacturer and user facility device experience. http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm Visited June 2013.
[3] Microsoft. Flaw in rpc endpoint mapper could allow denial of service attacks (331953). http://technet.microsoft.com/en-us/security/bulletin/ms03-010, Visited June 2013.

Approach and architecture

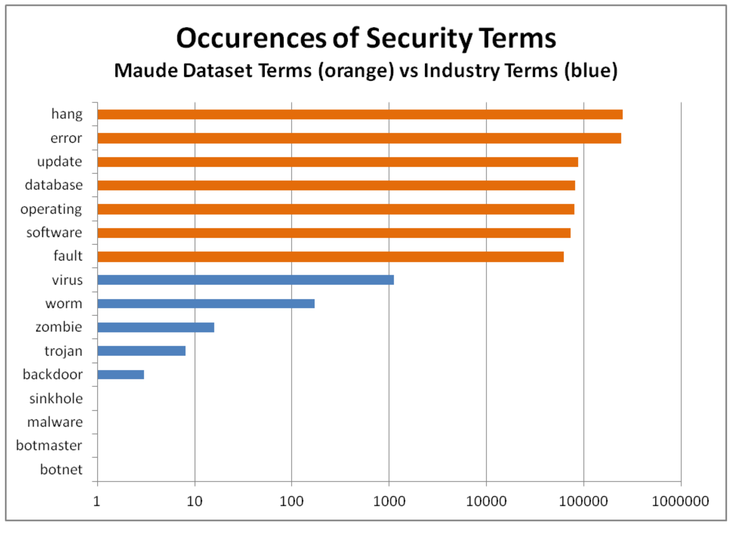
MaudeMiner: A modular command line interface for managing the MAUDE dataset. Usable and extensible for 3rd party research

- downloading
- building
- cleaning
- tokenizing
- querying



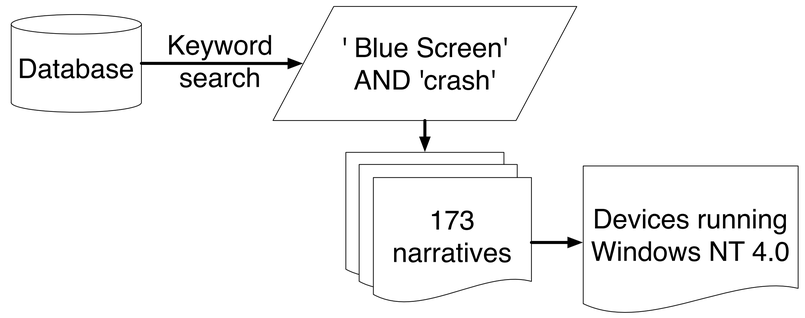
Uses for MaudeMiner:
- More advanced and customized searches
- Build corpora of computer- and security-related keywords
- Allows use of Machine Learning techniques on narratives

Security terms mean different things in medical industry:
- Trojan (condom)
- Zombie (look or feeling)
- Virus (infection)
- Worm (clamp)

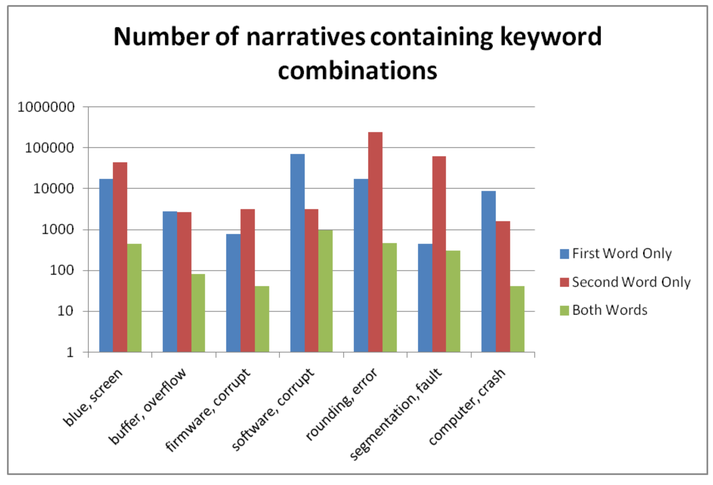


Results

We can extract events from the MAUDE dataset which could be a result of computer vulnerability. Further analysis of the identified devices is necessary to definitively determine if events are caused by security issues.



Keyword search of 'blue screen' AND 'crash' led to 50 reports of a device running Windows NT 4.0 with known and unfixable security vulnerabilities [3].



Next Steps

More advanced analysis to uncover security issues
- Statistical analysis
- Natural Language Processing ('stomach bug' vs 'computer bug')

Any opinions, findings, and conclusions or recommendations expressed in these materials are those of the author(s) and do not necessarily reflect the views of the following sponsors.
The US Department of Health and Human Services Cooperative agreement No. 90TR0003/01 and the National Science Foundation under Grant No. 1331652.

SHARPS Strategic Healthcare IT Advanced Research Projects on Security