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.

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

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].

References: