Experiences Developing an IBM Watson Cognitive Processing Application to Support Q&A of Application Security (Software Assurance) Diagnostics

SEI staff:
Mark Sherman (PI)
Lori Flynn (Tech lead)
Chris Alberts (Assurance SME)

Students:
Christine Baek
Anire Bowman
Skye Toor
Myles Blodnick
Experiences Developing an IBM Watson Cognitive Processing Application to Support Q&A of Application Security (Software Assurance) Diagnostics

October 26, 2016

© 2016 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.


IBM, BlueMix, IBM Watson, the IBM Watson Logo, and the Watson Avatar are trademarks of International Business Machines Corp.

SparkCognition, SparkSecure and their logos are trademarks of SparkCognition Corp.

CWE, Common Weakness Enumeration and the CWE logo are trademarks of MITRE Corp.

CMU Language Technologies Institute logo is a trademark of Carnegie Mellon University.

Apache Lucene, Apache Solr and their respective logos are trademarks of the Apache Software Foundation.

"Jeopardy!" and Jeopardy Productions Inc. are trademarks of Sony Corp.

DM-0004026
Can DoD Use IBM Watson to Improve Assurance?

- Acquisition programs generate voluminous documentation
- Assurance is based on assembling and reviewing relevant evidence from documents
- Finding appropriate evidence or explanations can be challenging

Q: Can typical developers build IBM Watson applications to support an assurance review?
Key Take Aways

• You do not need a PhD in AI or Natural Language Processing to build IBM Watson applications on BlueMix

• Significant automation will be required for corpus (knowledge database) preparation, potentially larger than application development

• Subject matter expert needed to help craft document structure

• End user involvement needed to guide and improve training

• IBM Watson is one of many tools to bring to bear for cognitive processing applications
Approach: Simulate a Development Process

Assemble team of assurance experts
- Determine interesting questions
- Select appropriate documents
- Define training (ground truth)

Assemble team of developers
- Experienced Python programmers
- No specific expertise in artificial intelligence or natural language processing

Two phases
- 2 weeks of 3 SMEs specifying corpus
- 11 weeks of 4 student developers building application and corpus
Application Performance

Better **Recall** and **Precision**:
Example: “What is the risk of INT33-C”

INT33-C – Risk Overview

INTC33-C. Ensure that division and remainder operations do not result …
https://www.securecoding.cert.org/…/c/INT33-C. =Ensure+that+division+and+remaind…
Lessons Learned From Project

Theory

Practice
Government use rights apply. IBM Watson software (and any dependencies) must be licensed from IBM.

SparkCognition is an IBM Watson business partner (independent software vendor) and has licensed the project materials from CMU for use in their products.
We Want to Thank and Acknowledge Collaborators

SparkSecure team at SparkCognition

IBM Watson team at IBM

Prof. Eric Nyberg, Language Technologies Institute, School of Computer Science, CMU

And our student interns: Christine Baek, Anire Bowman, Skye Toor and Myles Blodnick