Introducing Sallie, the World's First Embedsec Training Bot and the Latest Addition to the Salvum© Security Engine

QVLx

Executive Summary

The Salvum© Security Engine welcomes a new feature, and her name is Sallie. Sallie is a bot that provides friendly training to users on embedded security principles and concepts pertinent to the Salvum environment.

Sallie was designed to reduce the time and effort needed to get up to speed on the Salvum platform as well as to learn core embedsec concepts that empower teams to succeed.

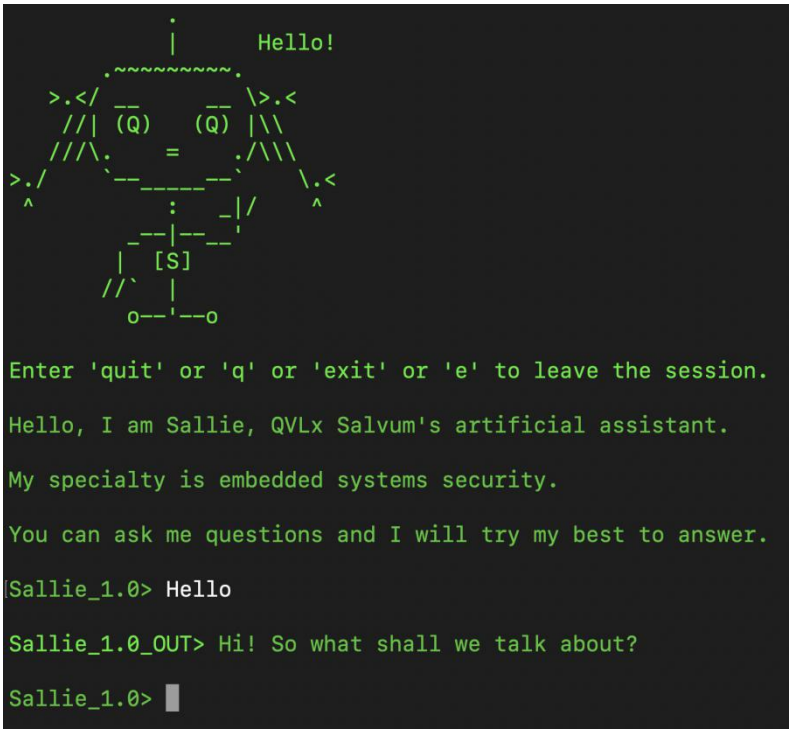

Figure 1. Sallie Console Demo

Sallie Design

The Sallie bot was built with a few key design considerations:

- Is only included by user preference.
- Written in pure Safe Rust.
- Does not use machine learning.
- User input and data do not persist.
- Developed to resemble human interaction.

Sallie is a derivative of the Eliza natural language processing program. She has diverged from Eliza in several aspects such as improved synonym handling, but the general concept is still the same.

Eliza was created by Joseph Weizenbaum at the MIT Artificial Intelligence Laboratory in the mid sixties. Eliza simulates conversation through pattern matching and substitution in a clever manner that displays a convincing illusion of deep human understanding to the user. During her time, Eliza duped many people into thinking she was sentient and that she could pass the Turing test.

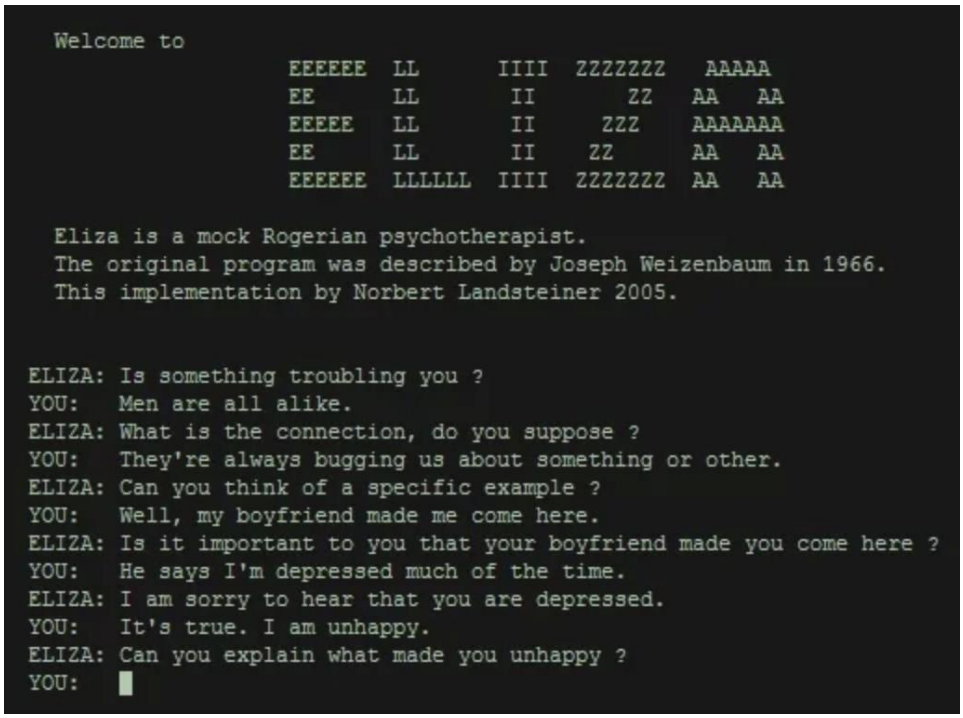

Figure 2. Eliza Console Demo

Using the foundation created nearly six decades ago, QVLx adds a descendant of Eliza to the Salvum security stack for users that wish to have some interactive guidance along their journey.

Implications

In addition to Sallie's role within Salvum, there are implications for the mechanics behind the bot regarding the use of artificial intelligence on embedded systems.

Modern advances in robotics and edge computing have resulted in a growing demand for on-board artificial intelligence processing, facilitated by dedicated hardware accelerators. Yet progress is not without problems in machine learning use.

ML, whether implemented in hardware or software, presents security and determinism challenges. ML is inherently difficult to verify, often being treated as a black box. ML consumes multidimensional data meaning that data is aggregated wherever and whenever ML is being performed. This leaves an attractive target for threat actors to carry out reversal, poisoning, and injection attacks.

In safety critical contexts such as the certification standards, the difficulty in verifying and validating ML algorithms means they must be constrained to lower criticality levels or excluded entirely. OEMs are taking steps to perform the verification and validation of AI accelerating hardware as well as develop deterministic chipsets, but this progress

is in early stages.

For security critical situations, there are currently no standard protection profiles or set of principals regarding security verification of AI. This security verification is referring to the verification of the AI itself, not its ability to provide security functions. Some of the responsibility of verification has been accepted by OEMs in the case of AI coprocessors, but work on that front needs maturation. As for software AI, verification is something that falls upon developers to do and is non-trivial.

Embedded systems developers with safety or security restrictions require new advancements in artificial intelligence capabilities to accommodate security and real-time safety needs. In time, OEMs and software vendors will provide the proper verification around these needs. The algorithm used in Eliza and Sallie does not have many practical use cases on an embedded system in and of itself, but the simplicity with which it was

designed may be a good starting point. There are times when developers don’t necessarily need large, complex AI or learning-based algorithms on their systems. These systems would benefit from using simpler algorithms to meet edge computing design goals. Simpler algorithms are easier to verify, more deterministic, and provide less attack surface. In the words of Leonardo De Vinci, simplicity is the ultimate sophistication.

Hopefully this article, in addition to revealing a Salvum feature, provides some points to ponder.

About QVLx

QVLx is a disruptive supplier of critical embedded systems expertise, products, and innovation. Our company helps customers develop complex, robust, and elegant solutions to meet their most demanding requirements in excellence.

QVLx is headquartered in Huntsville, Alabama.

For more information, visit qvlx.com

Or contact: **security@qvlx.com** **or** **(256)-607-4044**