QVLx

whitepaper

Salvum© and the Dawn of Disruptive Security

Unveiling the world's first embedded systems security engine

www.qvlx.com

Executive Summary

There are times when an embedded system requires the highest degree of protection. By purchasing products and services from hardware vendors, operating system providers, and specialized security firms, responsible parties can meet their most stringent requirements. This is costly but necessary if they want to reach utmost fortification.

Most embedded systems either don't require quite as high of a level of rigor or responsible parties are unable to allocate sufficient budget for security due to other higher priority expenses. As a result, many embedded systems remain unprotected and are exposed to simple attacks. Furthermore, an astonishing number of these devices serve critical purposes.

QVLx Salvum© Security Engine was developed to ensure that unprotected systems have access to an acceptable baseline of system hardening and provide an additional layer of refinement for already-fortified systems.

Salvum is the first in a line of QVLx products aiming to transform the security landscape by granting widespread access to commercial security assessment and protection capability.

In this paper, we will detail how to:

- significantly cut costs of protecting exposed embedded systems.
- provide an additional layer of security for hardened systems.
- empower traditional security professionals with embedsec capability and training.
- reduce time to meet security requirements by substantial margin.
- gift cross-platform, productivity-enhancing tools to embedded systems developers.

A Modern Problem

There are billions of embedded computing devices in the world today and many of which carry out critical functions. While ubiquitous chips bring an increase in productivity and higher quality of life, they also present a proportional increase in collective attack surface size. This risk is further exacerbated by the vulnerable nature of embedded systems:

- Systems are typically fielded such that they are physically accessible to attackers.
- Systems are typically updated less frequently than other computer variants.
- Systems typically have power, memory, and other limitations.

The continuous contributions of hardware vendors, operating system providers, and security communities ensure that the latest computing devices have the capability to thwart most attackers. However, only a subset of the embedded system landscape is comprised of the latest devices and leveraging relevant countermeasures requires some arcane knowledge.

Without a dedicated budget or in-house embedsec expertise, most stakeholders need a solution to meet security needs that is easy to use and affordable. The embedded systems market needs a disruptive technology that makes asset protection available to *everyone*.

A Novel Solution

QVLx joins the collective effort of other commercial, government, and open communities to protect a range of embedded devices with the development of the Salvum© Security Engine.

Salvum is a novel framework for penetration testing, hardening, and refining embedded systems both at development and runtime phases. It is designed based on specifications derived from NIST SP 800-115 recommended practices and built with modular components using object-oriented programming principles.

At the core of Salvum is a security-hardened shell which serves as the executive, managing the module ecosystem and providing supporting functionality to the user. Modules, classified as either Applets or Apps, provide the bulk embedsec capability to the collective engine. Applets provide the basal functionality that makes Salvum a rich and vibrant productivity studio. Apps are divided into red and blue categories, respectively for their offensive and defensive foci. Offensive capability is only to be used on systems owned by the user and this is enforced in policy. Modules are either developed in-house or sourced through communities. The entire core of Salvum as well as the majority of modules are are written in pure, Safe Rust. This was done foremost for security but also performance, portability, and extensibility.

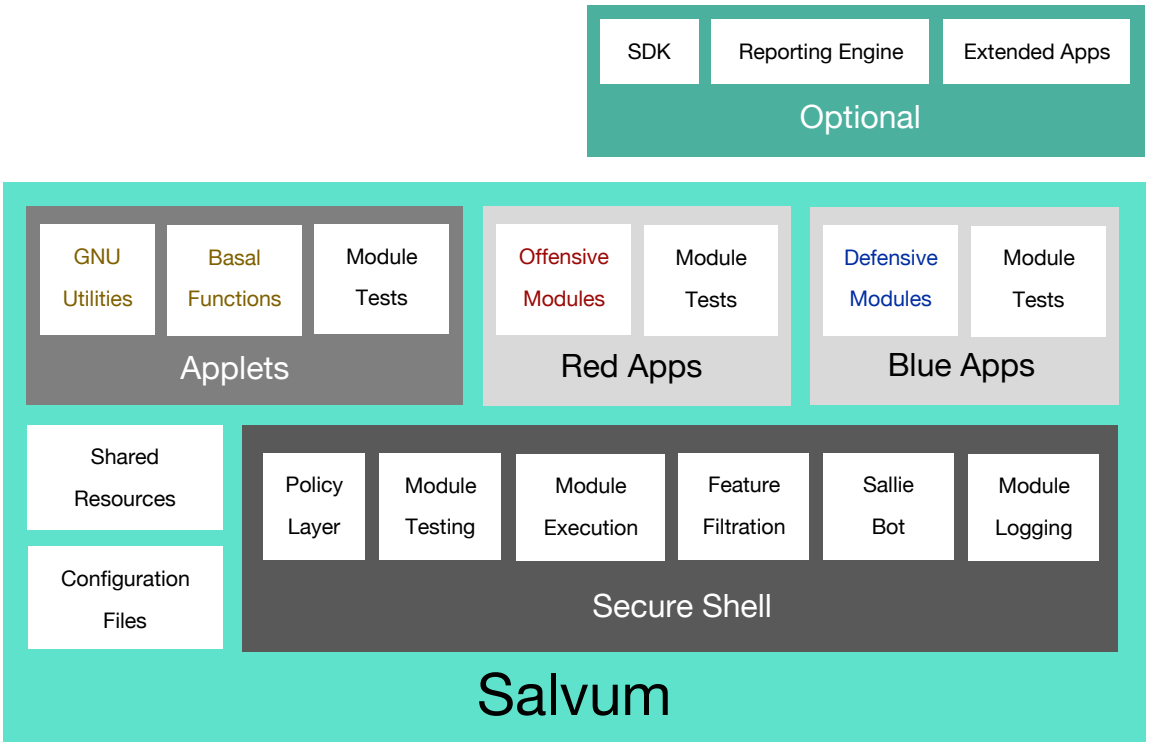

Figure 1. Salvum Architecture

Your Salvum

One of the primary design goals of Salvum is customization of the environment to the exact requirements and preferences of the end user.

This is achieved through the following features:

- Interface freedom providing multiple means of navigation and module invocation.
- Configuration mechanism allowing inclusion, exclusion, and policy control of modules.
- Optional SDK allowing for development of custom modules.
- Feature filtration on large, complex modules for user-specified functionality reduction.
- Configurable module aliasing for further tailoring user experience.
- Optional reporting engine for user-specified data interpretation.

Security Power

Salvum offensive and defensive security functionality is provided by Red and Blue Apps. Here are a few of the capabilities that these Apps provide:

- Audited and quantum-resistant cryptography.
- Hashing algorithms with no known successful attacks.
- Creative, non-cryptographic obfuscation methods.
- Detection of DoS attacks, steganography, rootkits, advisories, and more.
- Cryptosecure pseudorandom and true random number generators.
- File scanning for security features, encryption, IP addresses, passwords, email addresses and more.
- Static and dynamic binary analysis for vulnerabilities.
- Decompilation, dissasembly, parsers, and other reversal methods.
- Curated vulnerability, FCC ID, cryptographic key, hash, and password databases.
- Decompression, unpacking, and firmware extraction methods.
- UART, JTAG, IP packet sniffing, and other forms of debugging/snooping tools.
- Source code analysis, linting, input sanitization, and dependency checking.
- Perform MITM, spoofing, exploit injection, DoS, and other packaged attacks.
- Easy TFTP, FTP, and PXE netloading.
- Entropy, header magic, and embedded signature analysis modules.
- Loopback filesystem mounting and digital forensics.
- Crafted Linux kernel hardening mechanisms with Yocto and Buildroot integration.
- Analysis tools specifically for LynxOS, QNX, and VxWorks.
- Cracking utilities for passwords, hashes, CRCs, ECCs, and more.

Team Reinforcement

Salvum Applets provide a nexus of functionality to bolster development productivity. Using refined utilities, teams reach development and security goals in less time, cutting cost.

Example ways that Salvum Applets accelerate a team's delivery:

- Full suite of GNU utilities but with visual, functional, and security modifications.
- High-throughput compilation tools for C and C++.
- Calculation/conversion, text editors, string manipulation, and visual analysis tools.
- Secure console web browser, Stack Overflow querying, Wikipedia searching tools.
- Host hardware information, visual GNU debugger, ELF and raw binary dumping utils.
- Sallie, a bot that trains your team in embedded security and how to use the engine.

Salvum was developed carefully to run on most x64 hosts and its optimized runtime allows for seamless integration into common IDEs such as Eclipse and Visual Studio. Our provided host hardening resources ensure that only protected systems interact with your embedded target, so you can purify your boards with peace of mind.

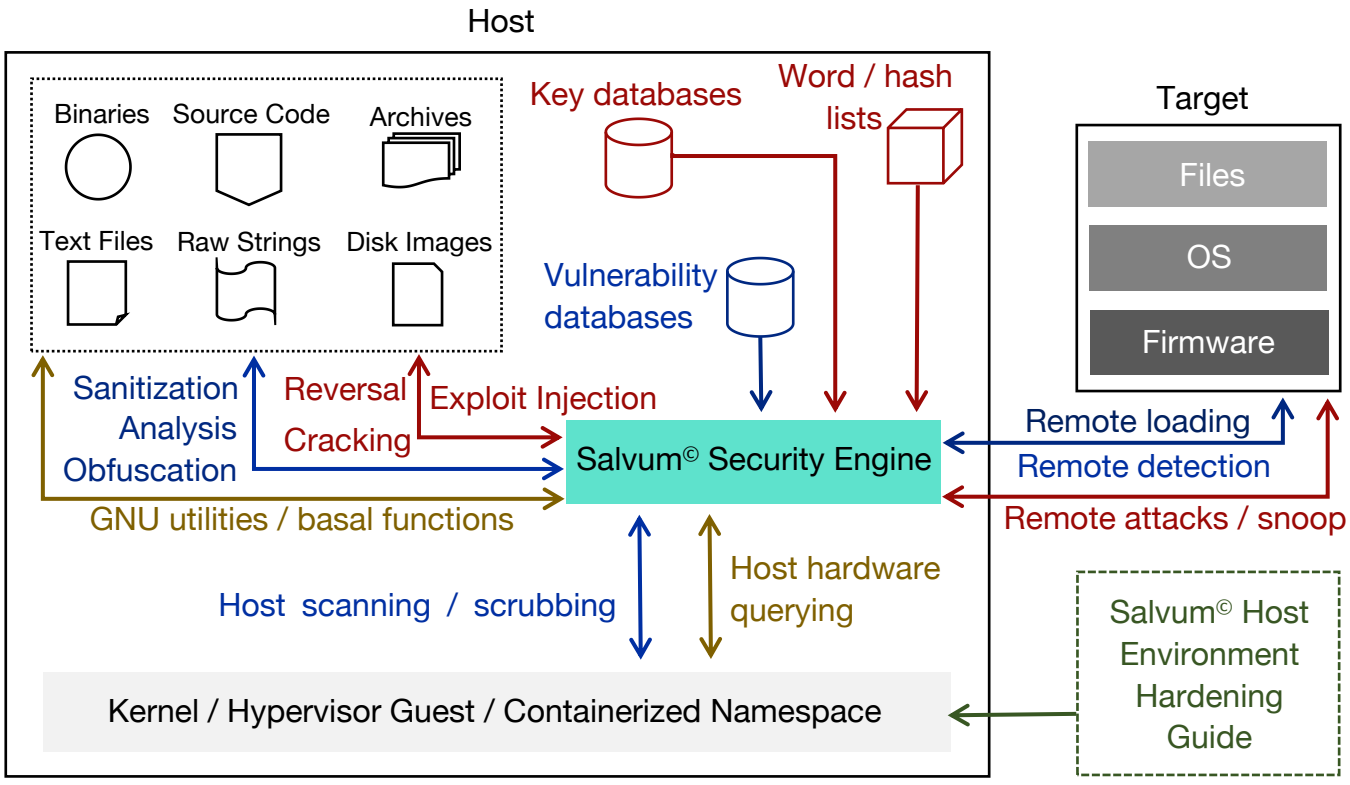

Figure 2. Salvum Example Scenario

Common Misconceptions

It is important to dispel a few common misconceptions around the Salvum© Security Engine in order to further highlight its value to the embedded security cause.

Misconception 1: *Salvum is a distro*

Salvum is not an OS distribution of any kind. It is a highly refined collection of software components that provide the functionality that then runs on top of an OS of your choice. It is also not a virtual machine. Salvum succeeds where both of these concepts fall short. While some distros do provide packaged functionality, they still require the user to understand a great deal about what tools to use and how to use them. They also require maintenance and bring with them extraneous elements. Salvum is tailored to user needs and provides assistance and guidance. Regarding virtual machines, VMs have performance implications that do not apply to the Salvum workspace.

Misconception 2: *Salvum is redundant*

Salvum is hand-crafted software that provides functionality unlike what is available with current security distros. It is possible to achieve the stand-alone functionality of certain modules if they are originally open sourced, but it will not replicate Salvum. Many of the open sourced modules in Salvum have been modified and improved. In addition, outdated tools have been refactored and rebuilt for modern systems. Furthermore, complex utilities have been wrapped with Rust and made with user experience as an important objective. Salvum also contains many custom modules written from scratch that can't be found anywhere else.

Misconception 3: *Salvum is dangerous*

Salvum's provided offensive capabilities are intended only for Red Team exercises to strengthen security. Hence, they must be used exclusively on systems on the same direct network as the user's Salvum installation. We have enforced this in the policy layer of the Salvum shell. We have added various other rules to the policy layer such restricting access to sensitive top-level directories unless whitelisted for a specific module, the zeroization of sensitive information such as passwords in RAM, and ability to de-elevate shell privilege if desired. We have also added security measures at the module level such as enforced bounding of iterative commands. The Rust language also provides security measures that Salvum has no choice but to adhere to. Salvum is built from the ground up with security at all levels as the most important objective. This is also why we provide host-hardening guidance, to ensure that precious embedded targets are only in contact with a highly trusted hosts.

Salvum inbound.

For further inquiries about the Salvum© Security Engine, Salvum© SDK, Salvum© Reporting Engine, or Salvum© Extended Apps, or QVLx Services please contact our team:

Email: security@qvlx.com **Phone:** (256)-607-4044

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