OSEHRA
Open Source Electronic Health Record Alliance

Cyber Security and Open Source Community Call Summary

April, 2016

Seong K. Mun, PhD
Don Hewitt
OSEHRA
Arlington, Virginia

Cybersecurity Workgroup

- **Ad Hoc group to address questions posed by VA**
  - OSEHRA Cybersecurity Workgroup - https://www.osehra.org/groups/cybersecurity-and-open-source
  - Weekly Call Meetings held to discuss issues
  - Summary in this briefing
- **Will be followed by establishment of a VA Technical Working Group (TWG) on VistA Security**
  - Will operate under OSEHRA's VA contract
  - Community participation will be invited

Key Questions from VA

1. **Does the open source community have a focus on cyber security?**
2. **Are projects to enhance cybersecurity proposed to OSEHRA by the open source community? If so, have any been completed?**
3. **Are there lessons learned from Red Hat/LINUX WRT cybersecurity that might be applicable to health IT?**
4. **What is the relationship of OSEHRA certification to cybersecurity?**

(Q1) Focus on Cyber Security

- **OSEHRA has not (yet)**
- **Implementer has ultimate responsibility for security**
  - Open source code delivered "as-is"
  - Community focus on tools
- **Some examples of open source projects in greater OS community**
  - http://www.open-scap.org/

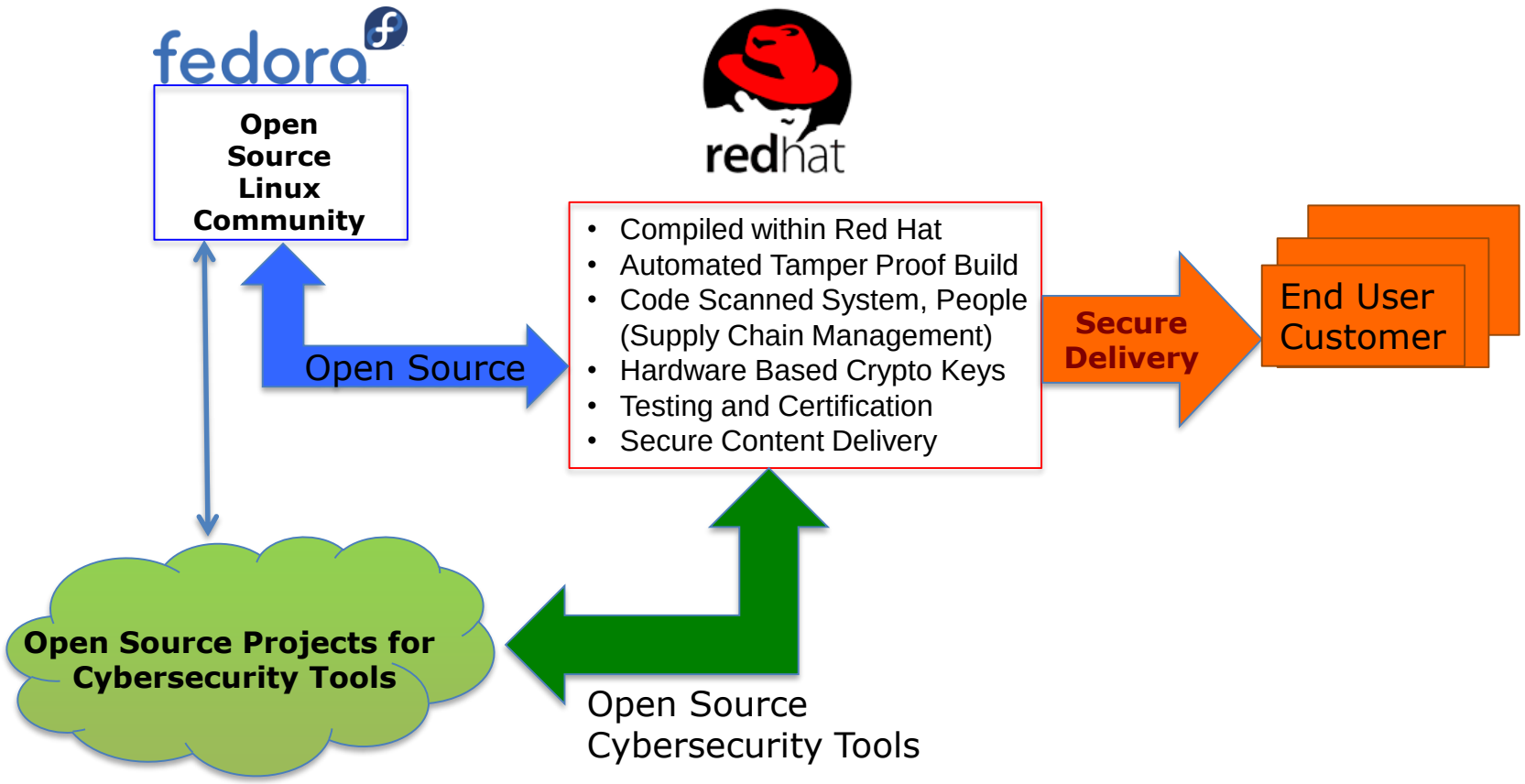
(Q2) Open Source Projects

- **Previous special project for vulnerability remediation**
  - M2M Broker Vulnerability
  - Joint effort, closed project group under non-disclosure
  - Precedent and process established
- **No project proposals for explicit security upgrades**
- **VA has proposed an open source project for a code scanning tool (similar to HP Fortify) for M code**
  - OSEHRA recommends enhancing the existing Xindex tool rather than starting from scratch
  - Most effective approach would be a funded community open source project

(Q3) – Red Hat Reporting

- **Are there lessons learned from Red Hat/LINUX WRT cybersecurity that might be applicable to health IT?**

Securing Open Source Code - Red Hat



Securing VistA - VA

Open Source EHR Community

- Open Code Review
- OSEHRA Certification

Open Source

VA: OI&T

- Compiled within VA Network
- VA Testing and Certification
- Automated Tamper Proof Build
- Code Scanned System, People (Supply Chain Management)
- Hardware Based Crypto Keys
- Secure Content Delivery

Secure Delivery

Open Source Projects for Cybersecurity Tools

Open Source Cybersecurity Tools

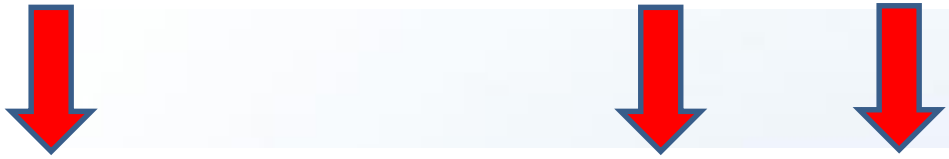
OS Community Innovation → Productization → OS Commercial Product

(Q4) Certification

What is the relationship of OSEHRA Certification to cyber security?

Brief answer: OSEHRA Certification is intended as a prerequisite for, not a replacement of, the in-depth testing required for specific implementations. As such, while specific tools may be run during code review, OSEHRA does not intend to certify the security of code. *However…*

(Q4) Certification Components



	Name / Number Space	Dependency / SAC	Open Source License	Documentation	Regression	Code Review	Functional Testing	Test Installation
Level 1	Pass	Pass	OSI-Approved	None	Existing Tests Pass	Large # Non-critical Issues	Large # Non-critical Issues	Large # Non-critical Issues
Level 2	Pass	Pass	Core is Apache 2	Basic	Existing + Some R. Tests	Small # Non-critical Issues	Small # Non-critical Issues	Small # Non-critical Issues
Level 3	Pass	Pass	Core+ is Apache 2	Substantial	Existing + >= 50% Coverage	No Issues	No Issues	No Issues
Level 4	Pass	Pass	All Apache 2	All Required	Existing + >= 90% Coverage	No Issues	No Issues	No Issues

(Q4) SAC Checking

- **Standards and Conventions Compliance**
  - Critical aspect of security
  - Dependent upon quality / breadth of SAC rule base
  - Example: scope checking
- **Susceptible to use of scanning tools**
  - Fortify (but not for M code)
  - Xindex (covers M code, but currently limited)

Current Status

- **The XINDEX tool developed by VA is the only current MUMPS code scanning tool in use. XINDEX is a Mumps routine which parses and analyzes all the routines in VistA install. The analysis includes a variety of useful information, including:**
  - Errors and warnings for the code based on MUMPS language and VA SAC (The Department of Veterans Affairs M Programming Standards and Conventions)
  - List of all calls to other routines
  - List of calls within the routine
  - Global and naked global usage in the routine
  - Local variable usage in the routine
- **OSEHRA utilized XINDEX as part of its certification process on VA Gold Disk support project.**

Challenges

- **MUMPS expertise increasingly scarce**
  - Declining even within VA
  - Scattered pockets of expertise in community
- **Code base continually evolving**
  - Continuing development and bug fixes
  - Fileman being changed during intake

(Q4) Code Review

- **Major advantage of open source**
  - More eyes on code is better
  - Security through obscurity is a myth
- **Proper facilitation is key**
  - Bugs
  - Possible improvements
  - Possible (or definite) vulnerabilities
- **Documented issues and results**

(Q4) Regression Testing

- **Continuous Unit Testing**
  - Emergent best practice
  - Critical part of defense in depth
  - Required for higher OSEHRA certification levels
- **M-Unit available for M code**
  - Newest version in OSEHRA repository
  - Certified to OSEHRA Level 4™

(Q4) Summary

- **No overt security certification by OSEHRA**
- **Substantial contribution to security of incoming open source code**
  - Use of automated scan tools
  - Open code review
  - Requirement for unit tests
- **As tools improve (e.g. Xindex), OSEHRA contribution to security will increase**

OSEHRA
Open Source Electronic Health Record Alliance

Contact:

Don Hewitt
hewittd@osehra.org
(571) 858-3376