RED HAT SECURITY ROADMAP

Mark Thacker
mthacker@redhat.com
Technical Product Manager, Red Hat
April 2017

DISCLAIMER

The content set forth herein does not constitute in any way a binding or legal agreement or impose any legal obligation or duty on Red Hat.

This information is provided for discussion purposes only and is subject to change for any or no reason.

AGENDA

Red Hat and Security in the Community

What we are seeing as trends in :

1. Creating secure foundations
2. Enabling hybrid cloud deployments
3. Automating security compliance

Where else to go for more information - especially here at Summit

Q&A

RED HAT AND SECURITY

RED HAT AND SECURITY?

Red Hat is not a security company, but....

We build security into everything we ship and deliver security capabilities

Over 40 sessions, labs, lightning talks with security content at this Summit!

RED HAT SUPPLY CHAIN SECURITY

- Community leadership
- Package selection
- Manual inspection
- Automated inspection
- Packaging guidelines
- Trusted builds

- Quality assurance
- Certifications
- Signing
- Distribution
- Support
- Security updates/patches

SECURITY THROUGHOUT THE STACK

It all comes together for comprehensive solutions

1. CREATING SECURE FOUNDATION
2. ENABLING HYBRID CLOUD DEPLOYMENTS
3. AUTOMATING COMPLIANCE

CREATING SECURE FOUNDATIONS

The foundation drives the security of the rest of the stack

Networking / Firewall

- NFTables firewall for stateful firewalls with online policy change
- IPSec and MACSec L2 for encrypted network communications

Cryptographic protection

- Wide variety of strong, peer-reviewed and FIPS certified crypto algorithms for privacy
- Encrypted data at rest and in-flight throughout the Red Hat software stack
- Deprecation of old crypto algorithms to remove attack vectors

Preventing intrusions and attacks

- SELinux mandatory access controls to prevent breaches (i.e. Shellshock)
- Security evaluation of open source code during development and before shipping
- Secure Boot for verified integrity of boot image
- Trusted Platform Module (TPM) 2.0 support for hardware based key storage

TRENDS IN CREATING SECURE FOUNDATIONS

- New TLS 1.3 and other cryptographic algorithms
  - While respecting the need for binary compatibility with existing releases
- Unified crypto policies across all apps on a system for easier management
  - Example : Disable an algorithm system or site-wide without breaking the stack
- Hardware root of trust
  - Attestation standards for proving a tamper-proof system
  - Trusted Platform Modules using PKCS#11 for broader crypto integration
  - Disk crypto key storage (LUKS and NBDE) in TPM for protecting against disk theft
  - More applications using TPM 2.0 and Virtual TPMs for the VMs and Containers
- Methods for executing only ‘white listed’ utilities and applications to reduce risk
  - Software ID Tags that are package specific
- Automatic disk decryption in secured manner (see NBDE)
- USB Guard for specific device authorization per device / device class

IDENTITY MANAGEMENT

It’s not a separate product, it’s a core capability

Identity Management is a core part of the Red Hat stack

- Centralized Linux authentication and authorization
- Integrates with integration into Active Directory
- Centralized management of system services (host name, services, etc)
- Container deployment of Identity Management server

Certificate Services

- Provides PKI and X.509v3 certificates for encrypted and authenticated communications

Directory Server

- Provides standards-based LDAP identity for Linux and Unix IDs

TRENDS IN IDENTITY MANAGEMENT

- Better integration with middleware identity management
  - Beyond OpenStack
- Automatic enrollment of systems into Identity Management upon deployment
  - Using Ansible and other tools
  - RHEL Engineering maintained modules
- Hardware Security Module use
  - TPM and dedicated hardware devices
  - Ideal for secret store and access through Custodia
- Better integration of PKI across whole stack
  - What about LetsEncrypt? Smartcard and PKI

1. CREATING SECURE FOUNDATION
2. **ENABLING HYBRID CLOUD DEPLOYMENTS**
3. AUTOMATING SECURITY COMPLIANCE

HYBRID CLOUD PLATFORMS

Security flows from the foundation up the stack

Red Hat Virtualization, Red Hat OpenStack Platform and Red Hat OpenShift Container Platform*

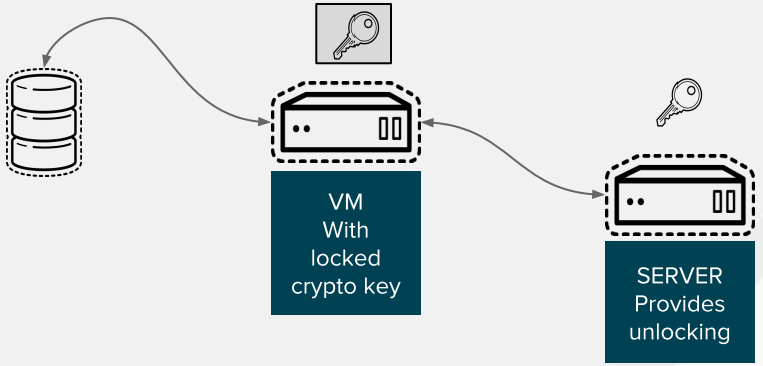
- SVirt provides automatic SELinux protecting VMs and host from exploiting each other
- MACSec L2 and IPSec encrypted communications between guests and hosts
- Automatic firewall configuration
- Content scanning upon deployment to prevent non-compliant instances from running
- Signing of Container images to allow verification of trust back to build time
- Secure, multi-tenancy hosting
- Isolation of process, memory and filesystems to maintain separate boundaries
- Read-only Atomic Host for Containers

*Exact features vary by product

STORAGE SECURITY IN THE HYBRID CLOUD

Network Bound Disk Encryption

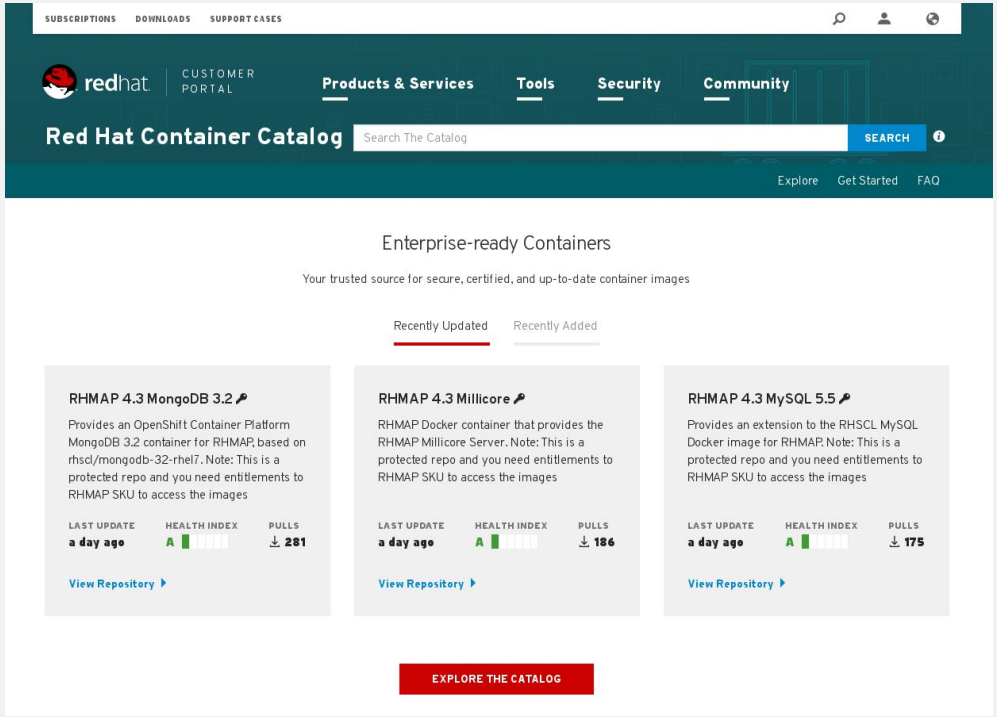
- LUKS encrypted volumes for transparently encrypting data at rest across flexible software-defined disks
- Typically at boot time, someone needs to type in a password (not convenient or even possible always)
- Client system maintains local encryption key, but it's wrapped with a public key from the server and can only be unlocked if the server is present
- The stateless server provides public key to help client unwrap the encryption key and the client system continues its boot process, hands-free!



TRENDS FOR HYBRID CLOUD

- OverlayFS support of SELinux
  - Stronger mandatory access controls for Containers file systems
- Use of Custodia as a secrets protocol for Containers?
  - Avoid hard coding secrets, or a specific storage vault, into the Container
- OpenShift reduced attack vectors
  - Deletes old memory-backed volumes to reduce risk
  - Service Containers for privileged process that are still controlled
- Trusted Execution Environments (SGX, SVE)
  - Encrypted memory for protection of VM/Container from host itself
- NBDE support for non-boot volumes
  - Including Red Hat storage solutions

TRUSTING THE CLOUD - THE CONTAINER HEALTH INDEX



- Trusted Container Images
- Container Health Index
  - Letter grade A - F
  - Age of Image
  - Unapplied updates
- Red Hat security expertise
- Unique, easy to use

1. CREATING SECURE FOUNDATION
2. ENABLING HYBRID CLOUD DEPLOYMENTS
3. AUTOMATING COMPLIANCE

AUTOMATING SECURITY COMPLIANCE

Are you sure you are running a secure system?

- OpenSCAP Scanning of a system
- CloudForms automatic prevention of execution of out-of-compliance Containers
- Red Hat Insights service for applying our expert knowledge to your whole datacenter
- Common Criteria and FIPS certification of solutions
- Security Patch Remediation and Response
- Rapid responses to known vulnerabilities (see 2016 Risk Report)
- Vulnerability API allowing you to query our database

TREND TOWARDS SMART RESPONSES TO BRANDED ISSUES

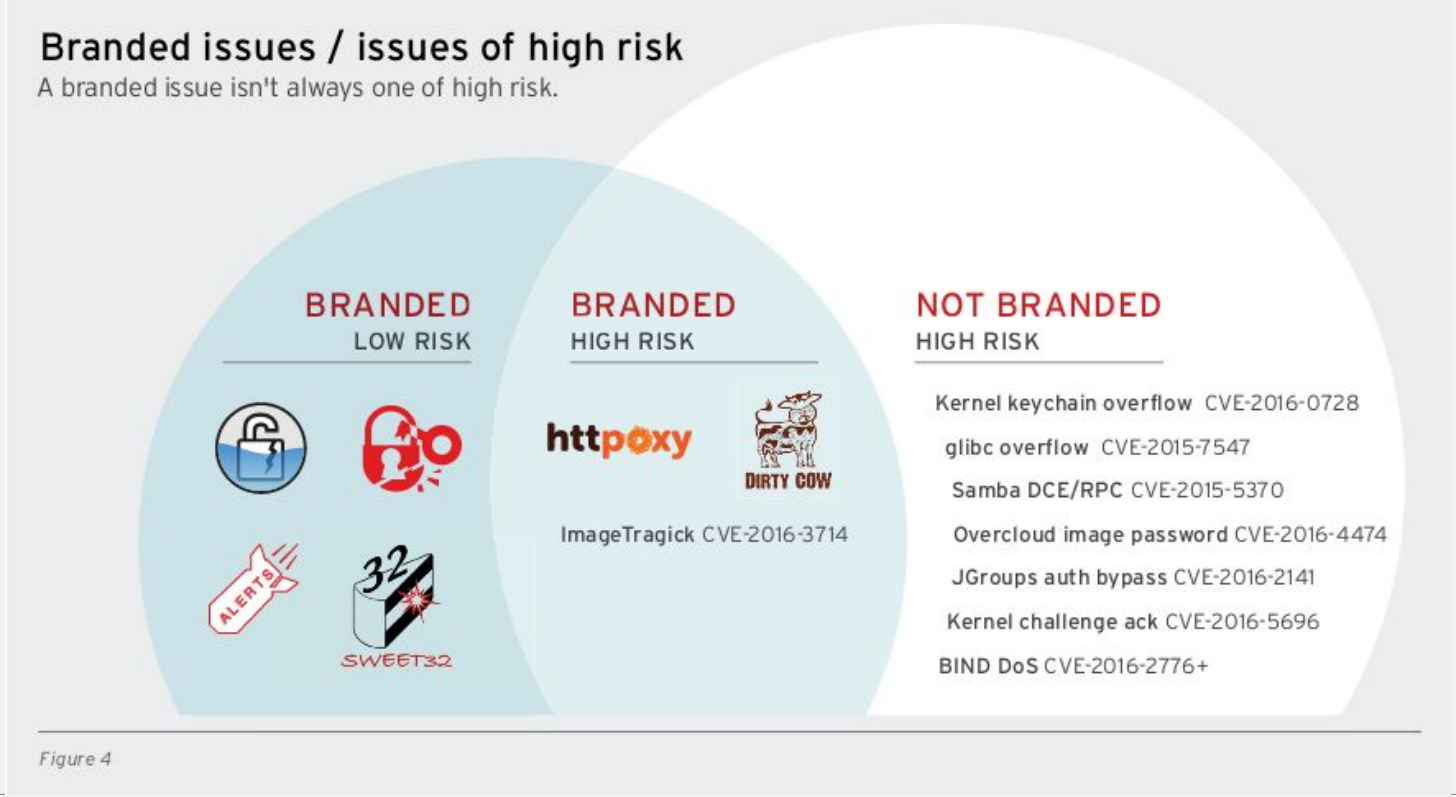


Figure 4

TRENDS IN AUTOMATING SECURITY COMPLIANCE

- Common Logging
  - Collection of data, normalize and display trends
  - Across Red Hat Enterprise Linux, OpenStack Container Platform, etc.
- Session recording and playback
  - Required by some customers, may be a requirement for certification
- More OpenSCAP profiles
  - For other industries, for more container sources and formats
- Achieving NIST Certifications for OpenSCAP tools in RHEL 7
- Reduced cycle time for certifications
- Revisions to Common Criteria certifications
- Increased coverage of products being patched in 1 day

IN CONCLUSION...

REMINDER OF WHAT WE TALKED ABOUT

Red Hat and Security in the Community

What we are seeing as trends in :

- Creating secure foundations
- Enabling hybrid cloud deployments
- Automating security compliance

Where else to go for more information - especially here at Summit

Q&A

WHERE TO GO AT SUMMIT 2017

Remember over 40 security sessions to choose from!

Partner Pavilion (Hall A)

- DevSecOps booth (412)
- Ask The Expert bar (600)
- Product Security Team (CEE booth)
- Booth Theatre
  - Security in RHEL
  - Container Catalog & Trusted Content
  - Automated Security Response
  - Automating Security Compliance
  - 2016 Risk Report

Sessions (a sampling)

- Red Hat Enterprise Linux Roadmap
- Red Hat Container Catalog LT
- Roadmap for Security-Enhanced Red Hat OpenStack Platform
- Fury and Sound : A Mock Disaster
- DevSecOps the Open Source Way
- Easily Secure Your.. Applications with Keycloak
- The Security of Cryptography
- Mobilizing and Securing JBOSS

WHERE TO LEARN MORE

Report a Security Concern

- SecAlert@redhat.com

Product Documentation

- access.redhat.com

Product Security Center

- access.redhat.com/security

Customer Security Awareness Program

- access.redhat.com/articles/2968471

2016 Risk Report

- www.redhat.com/en/resources/2016-product-security-risk-report

RED HAT SUMMIT

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos

LEARN. NETWORK.
EXPERIENCE
OPEN SOURCE.