
# RED HAT SECURITY ROADMAP 2019

Mark Thacker, Principal Technical Product Manager

Red Hat
May 2019

# 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

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

# SECURITY THROUGHOUT THE STACK + LIFECYCLE


**DESIGN**

- RED HAT® CONSULTING Guided Transition
- RED HAT® SERVICES
- RED HAT® TRAINING

**BUILD**

- RED HAT® OPENSHIFT Container Platform
- RED HAT® MIDDLEWARE
- 3scale BY RED HAT®

**RUN**

- RED HAT® ENTERPRISE LINUX®
- RED HAT® CoreOS
- RED HAT® VIRTUALIZATION
- RED HAT® OPENSTACK® PLATFORM
- RED HAT® STORAGE

**MANAGE & AUTOMATE**

- RED HAT® ANSIBLE® Automation
- RED HAT® SATELLITE
- RED HAT® CLOUDFORMS

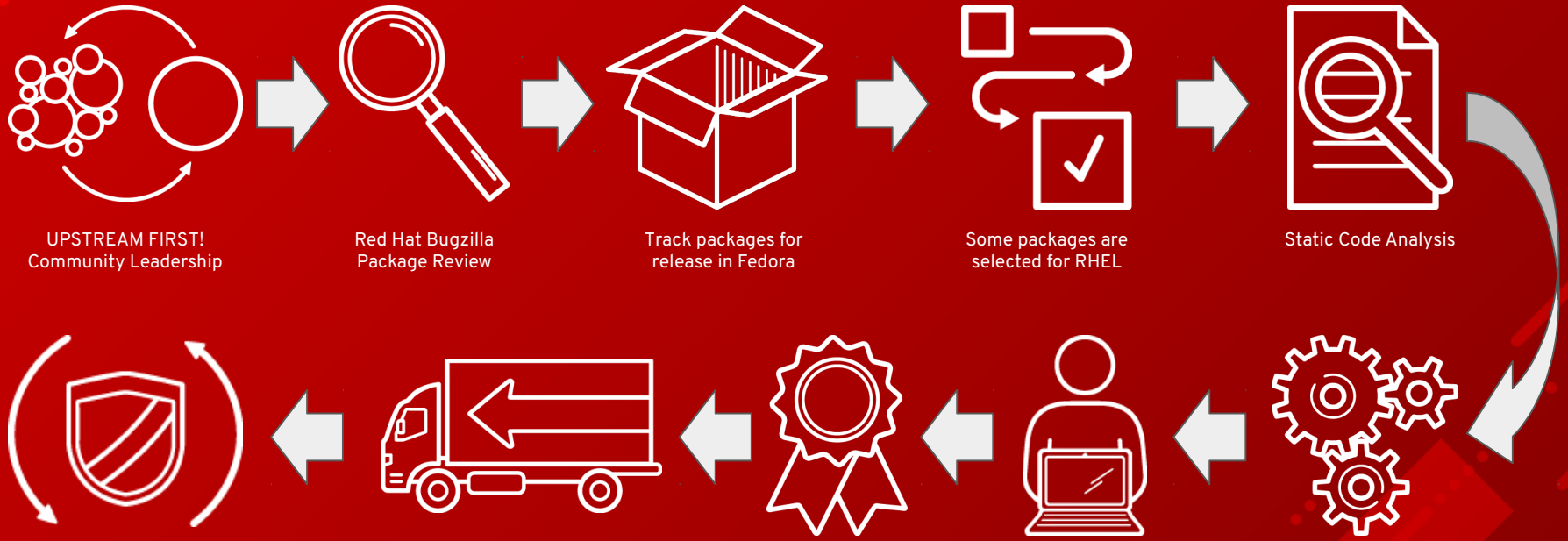
**ADAPT**

- RED HAT® INSIGHTS
- RED HAT SECURITY ADVISORIES

TESTED, CERTIFIED, STABLE, AND SUPPORTED OPEN SOURCE SOFTWARE

# RED HAT SUPPLY CHAIN SECURITY

## Reducing Risk and Making Open Source Consumable by the Enterprise



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

## Preventing intrusions and attacks

- SELinux mandatory access controls to prevent breaches with bare metal, VMs and Containers
- USBGuard prevents mounting of rogue / suspect USB devices
- UEFI Secure Boot for verified integrity of boot image
- Trusted Platform Module (TPM) 2.0 support for hardware based key storage
- Smartcard and HSM support for tamper proof digital certificate storage

## 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

## Networking / Firewall

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

# TRENDS IN CREATING SECURE FOUNDATIONS

- Advanced cryptographic algorithms
  - While respecting the need for binary compatibility with existing releases (i.e. TLS 1.3)
  - Post-Quantum Computing cryptography research (a.k.a. Watch this space)
  - More products with FIPS compliance & regular FIPS validation of products
- Unified crypto policies across all apps on a system for easier management
  - Disable an algorithm system or site-wide without breaking the stack
- Hardware root of trust
  - Attestation standards for proving a system hasn't been tampered with
  - 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, Virtual TPMs & other HSMs for the VMs and Containers
- Methods for executing only 'white-listed' utilities and applications to reduce risk
  - Leveraging Software ID (SWID) Tags across all of Red Hat portfolio
- Automatic disk decryption in secured manner (see NBDE)
  - Better integration into Gluster and Ceph



*See booth for example

# IDENTITY MANAGEMENT & AUTHENTICATION

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 for users, groups
- Integrates with integration into Active Directory
- Centralized management of system services (host name, services, etc)
- Smartcard authentication across Linux & Windows systems

## 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 & AUTHENTICATION

- Better integration of Identity Manager 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, Virtual TPM and other dedicated hardware devices
  - Consistent, Easier Smartcard support
- 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

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

### Control

- Content scanning upon deployment to prevent non-compliant instances from running
- Signing and scanning of Container images to allow verification of trust back to build time
- SELinux mount points for isolation of container block devices and file systems
- Red Hat CoreOS (minimized, immutable OS) powering OpenShift 4.x

### Defend

- SVirt provides automatic SELinux protecting VMs, Containers and host from exploiting each other
- Security Context Controls and non-root Containers for limiting risk and exploits
- Automatic firewall and VPN encrypted (MACSec L2, TLS & IPSec) communications between guests and hosts
- Automatic firewall configuration
- Isolation of users and root processes and namespaces from each other for strong protection

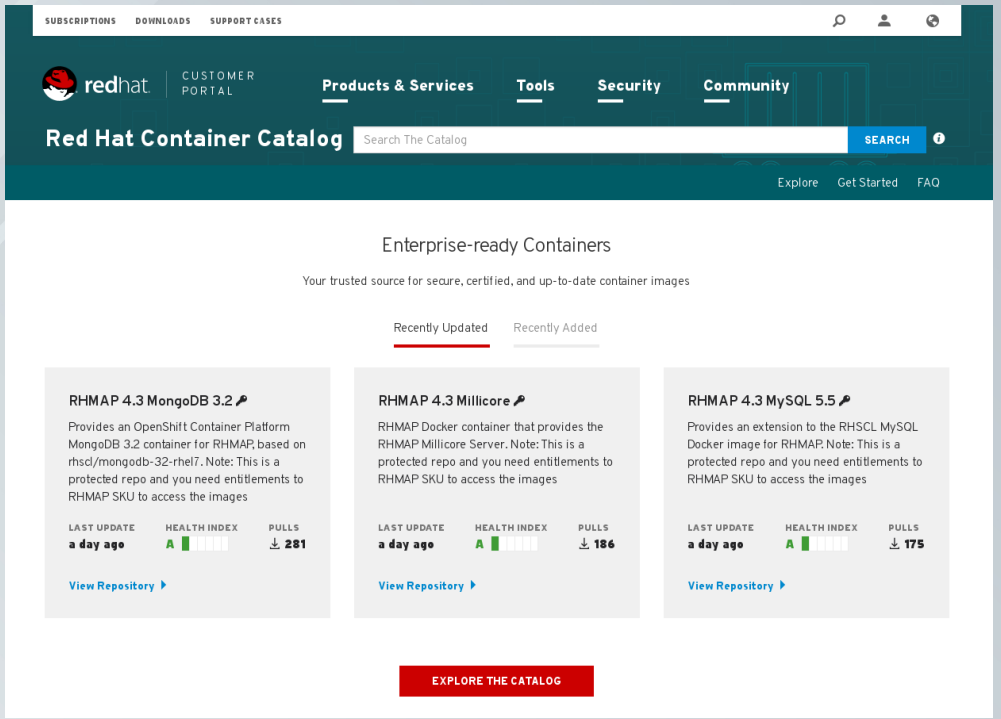
### Extend

- Partners for PKI, identity, encryption and storage integration - extensible scanning API

# TRENDS FOR HYBRID CLOUD

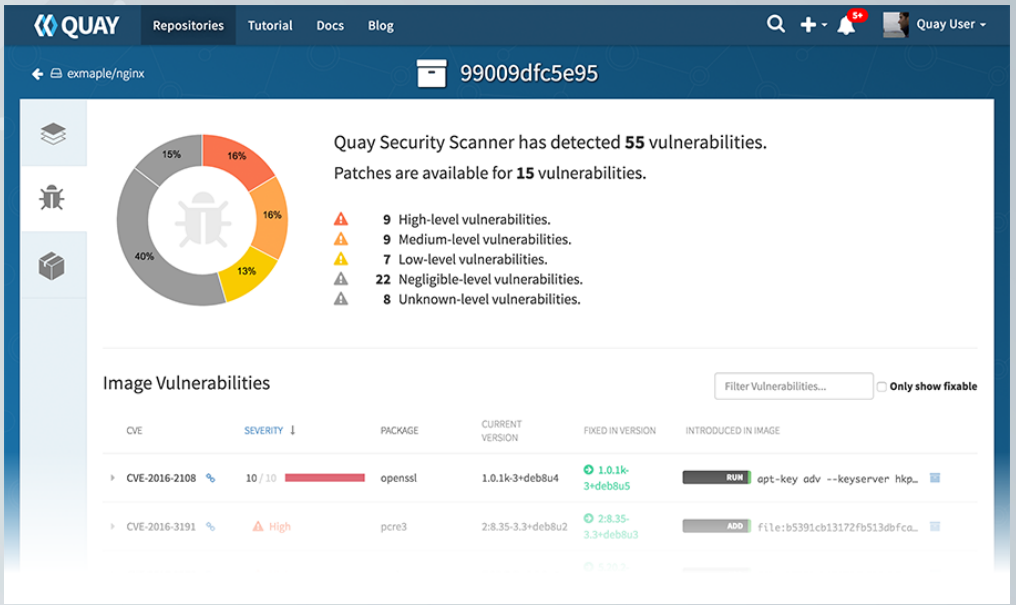
- Boot-time image verification and measurement
  - Using TPM for both RHEL and OpenStack - see Keylime
- Better secrets management for Containers
  - Avoid hard coding secrets, or a specific storage vault, into the Container
  - New Vault Operator from CoreOS
- OpenShift reduced attack vectors
  - Non-privileged Containers by default (no root daemon running)
  - Selective extensions of container security policy, avoiding the need for root (Udicia)
- Trusted Execution Environments (AMD SVE and others)
  - Encrypted memory for protection of VM/Container from host itself
  - Secure delivery and execution of encrypted payload
  - Better scale of solutions and better support for virtual TPM for cloud use

# TRUSTING THE CLOUD - THE CONTAINER HEALTH INDEX




- Trusted Container Images
- Letter grades A through F
  - Age of Image
  - Unapplied updates
  - Signed status
- Updated, maintained
- Unique, easy to use

# COREOS VULNERABILITY SCANNER - CLAIR




- Part of CoreOS acquisition
- Integrates with Quay container private registry
- Continuously scans your own container images
- Easily identify issues

1. CREATING SECURE FOUNDATION
2. ENABLING HYBRID CLOUD DEPLOYMENTS

# 3. AUTOMATING COMPLIANCE

# AUTOMATING SECURITY COMPLIANCE

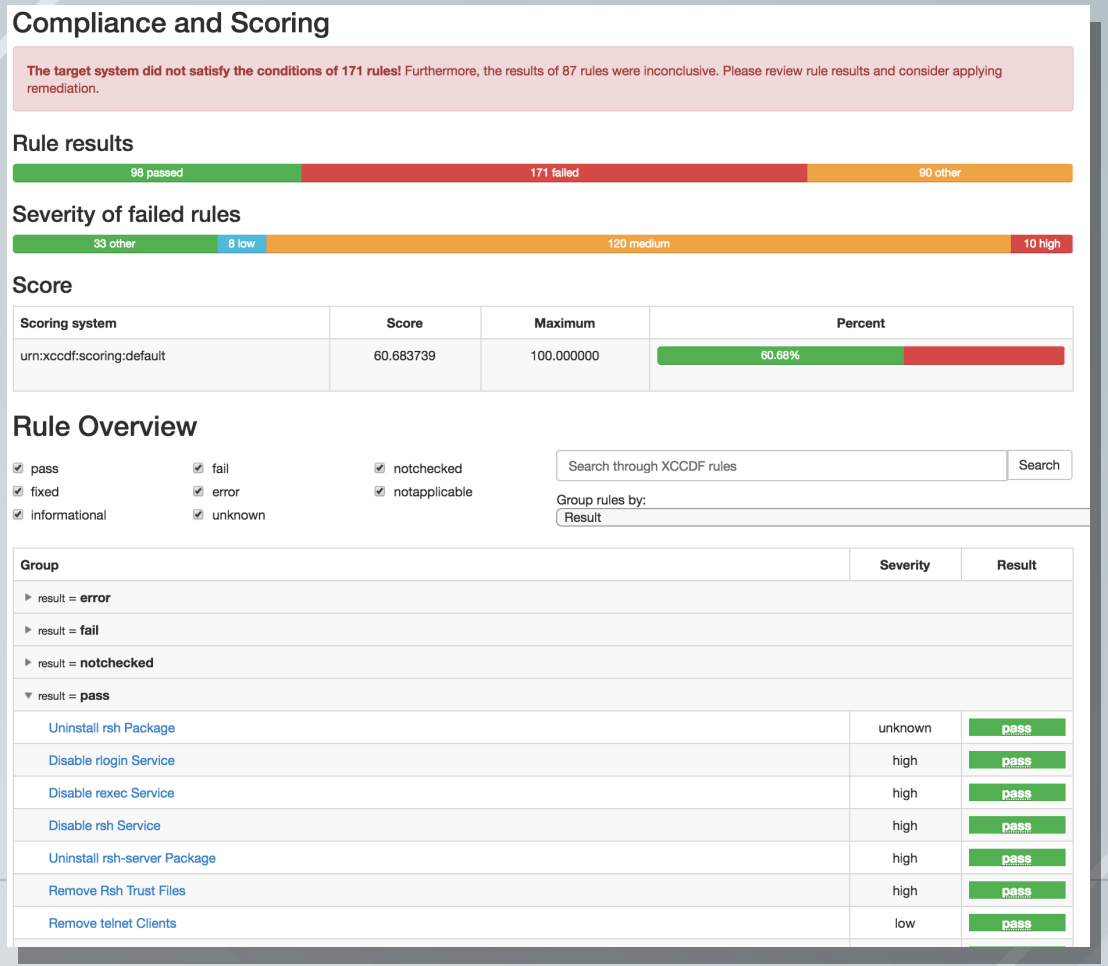
Are you sure you are running a secure system?

- OpenSCAP compliance scanning of a system
  - Both CVE exposure detection & security configuration validation
  - Automation of remediation w/Ansible, per-system or w/Satellite
  - Variety of compliance standard profiles : DISA STIG, PCI-DSS, USGCB...
- Compliance at install-time for RHEL
- Red Hat Insights service for proactive health & security monitoring
- Common Criteria and FIPS certification of solutions
  - Enterprise Linux, Certificate Server, JBOSS, etc.
- Security Patch Remediation and Response
- Vulnerability API allowing you to query our database

# TRENDS IN AUTOMATING SECURITY COMPLIANCE

- Service-based compliance
  - Making compliance just as easy to use as a service as the rest of your cloud
- Automation of scanning and remediation
  - RHEL System Roles, OpenSCAP Ansible remediation
- Common Logging
  - Collection of data, normalize and analysis of audit and log
  - 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 and easier contributions
  - Open Control efforts, ANSSI, FedRamp
  - Compliance as Code upstream (github.com/complianceascode)
- Reduced cycle time for certifications (FIPS & Common Criteria)

# OpenSCAP Scanner Example



## Compliance and Scoring

**The target system did not satisfy the conditions of 171 rules!** Furthermore, the results of 87 rules were inconclusive. Please review rule results and consider applying remediation.

### Rule results

98 passed | 171 failed | 90 other

### Severity of failed rules

33 other | 8 low | 120 medium | 10 high

### Score

| Scoring system | Score | Maximum | Percent |
|---|---|---|---|
| urn:xccdf:scoring:default | 60.683739 | 100.000000 | 60.68% |

### Rule Overview

pass, fail, notchecked, fixed, error, notapplicable, informational, unknown

Search through XCCDF rules — Search

Group rules by: Result

| Group | Severity | Result |
|---|---|---|
| result = **error** | | |
| result = **fail** | | |
| result = **notchecked** | | |
| result = **pass** | | |
| Uninstall rsh Package | unknown | pass |
| Disable rlogin Service | high | pass |
| Disable rexec Service | high | pass |
| Disable rsh Service | high | pass |
| Uninstall rsh-server Package | high | pass |
| Remove Rsh Trust Files | high | pass |
| Remove telnet Clients | low | pass |

# IN 2018:

redhat.

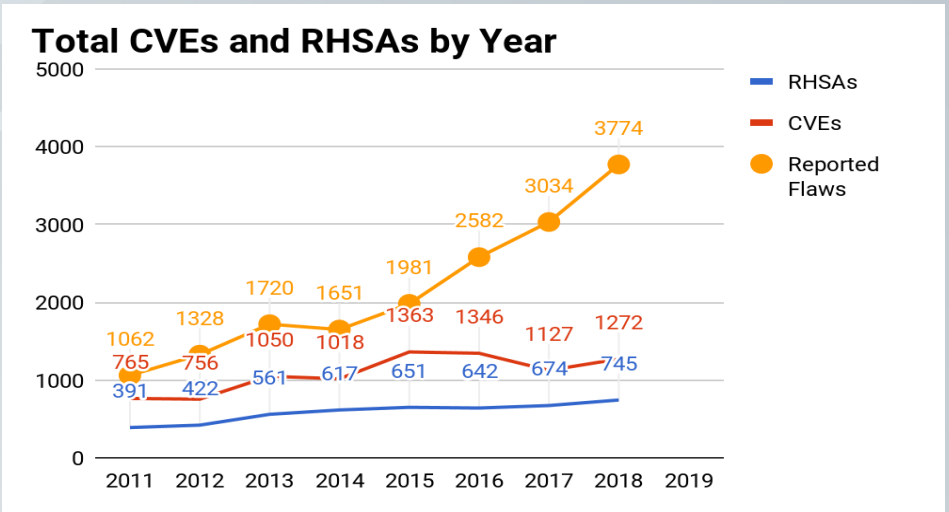
**745** Red Hat SECURITY ADVISORIES

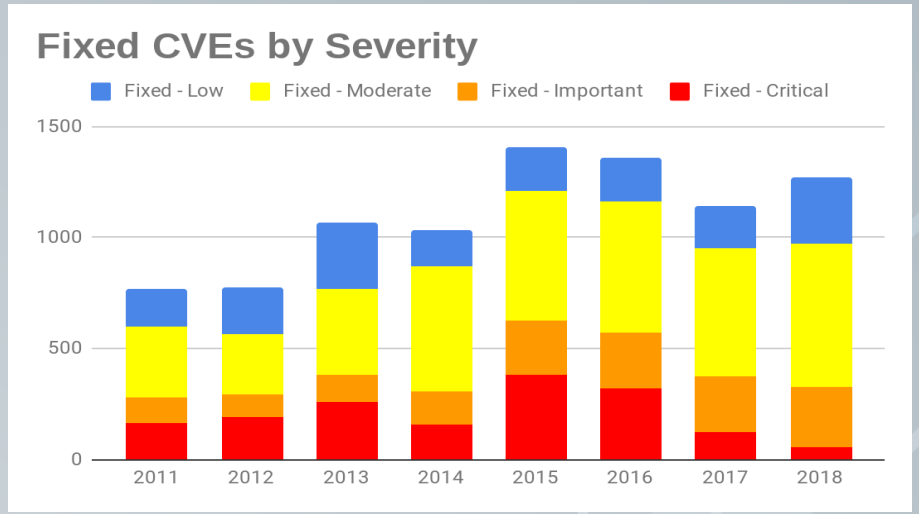
**1,272** CVEs ADDRESSED

Source: 2018 Red Hat Product Security Risk Report, February 2019. red.ht/2018riskreport

# VULNERABILITY METRICS

A snapshot of Red Hat Product Security response over the years




https://www.redhat.com/security/data/metrics/

# 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

Q&A

# 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


# THANK YOU


linkedin.com/company/Red-Hat


facebook.com/RedHatinc

youtube.com/user/RedHatVideos


twitter.com/RedHat

Mark Thacker
mthacker@redhat.com