RED HAT SECURITY ROADMAP 2018

Mark Thacker, Principal Technical Product Manager
Nathaniel McCallum, Principal Software Engineer
Brian Atkisson, Sr. Principal System Engineer
Red Hat
May 2018
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
   a. Network Bound Disk Encryption Use Case
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 50 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

Upstream > Community projects > Red Hat solutions > Red Hat customers
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
- Multi-factor authentication

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
  - More products with FIPS compliance

- **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, vTPM and other dedicated hardware devices
  - Ideal for secret store and access through Custodia
  - Broader Smartcard support
- Better integration of PKI across whole stack
  - What about LetsEncrypt? Smartcard and PKI
NETWORK BOUND DISK ENCRYPTION AT WORK
STORAGE SECURITY IN THE HYBRID CLOUD

Network Bound Disk Encryption

- **Addresses disk theft & the midnight reboot problem**
- 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!
RED HAT IT REQUIREMENTS

- Enterprise Security
  - Data Encryption at Rest
  - Secure data transport

- Operations
  - Avoid manual operator intervention
  - Automatable
  - Consistent solution across all Infrastructure
  - Offline and emergency data recoverability
  - Multisite and Highly Available

- Identity and Access Management
  - Avoid key escrow solutions
  - Open source and standards-based
  - Avoid proprietary solutions
NETWORK BOUND DISK ENCRYPTION OVERVIEW

- Clevis (client-side)
  - Decryption Automation Framework
  - Integration with LUKS (dracut, systemd, GNOME)
  - Uses pins (plugins) for encryption policies:
    - Tang
    - HTTPS-based escrows
    - TPM2 (upstream)
    - Shamir’s Secret Sharing (combine policies into meta-policies)

- Tang (server-side; escrow alternative)
  - Small, Fast, Stateless
  - Foundational Infrastructure
  - ECMR Key Exchange
    - No transport encryption required! (No Chicken & Egg!)
CLEVIS POLICY EXAMPLE*

* Not all features currently implemented.
# TANG VS. ESCROW

<table>
<thead>
<tr>
<th></th>
<th>Escrow</th>
<th>Tang</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Provisioning</td>
<td>Online</td>
<td>Online or Offline</td>
</tr>
<tr>
<td>Client Authentication</td>
<td>Required</td>
<td>Anonymous</td>
</tr>
<tr>
<td>Transport Encryption</td>
<td>Required</td>
<td>Optional</td>
</tr>
<tr>
<td>State</td>
<td>Secure Storage/Backups</td>
<td>None*</td>
</tr>
<tr>
<td>Performance</td>
<td>Slow</td>
<td>Fast</td>
</tr>
<tr>
<td>Deployment</td>
<td>Difficult, Manual</td>
<td>Easy, Automatable</td>
</tr>
<tr>
<td>Chain of Trust</td>
<td>Required</td>
<td>Optional</td>
</tr>
</tbody>
</table>

* Not yet implemented.
NBDE IN THE DATA CENTER

● Initial use-case
  ○ Red Hat IdM servers
  ■ Both bare metal and RHV VMs in 6 data centers across the globe (24 hosts)
  ○ Tang (NBDE) servers

● Now standard for bare metal systems
  ○ All new systems deployed with LUKS+NBDE

● Future
  ○ Data LUNs
  ■ Application data storage from storage appliances
  ○ Red Hat Storage
  ○ SSS and policy-based decryption
RED HAT IT POLICY

LUKS

pwd
Admin

tang
a.srv.local

tang
b.srv.local

tang
c.srv.local

tang
d.srv.local

pins
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 of Container images to allow verification of trust back to build time
- Secure, multi-tenancy hosting
- Read-only Atomic Host for Containers

Defend

- SVirt provides automatic SELinux protecting VMs and host from exploiting each other
- Automatic firewall and VPN encrypted (MACSec L2 and IPSec) communications between guests and hosts
- Automatic firewall configuration
- Isolation of users and root processes from each other for strong protection

Extend

- Partners for PKI, identity, encryption and storage integration

*Exact features vary by product.

See Red Hat Security Roadmap for Hybrid Cloud
TRENDS FOR HYBRID CLOUD

● Boot-time image verification and measurement
  ○ Using TPM for both RHEL and OpenStack

● OverlayFS support of SELinux
  ○ Stronger mandatory access controls for Containers file systems

● 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
  ○ Deletes old memory-backed volumes to reduce risk
  ○ Service Containers for privileged process that are still controlled

● Trusted Execution Environments (Intel SGX, AMD SVE, ARM TrustZone)
  ○ Encrypted memory for protection of VM/Container from host itself
  ○ 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
- 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
  - 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
- Red Hat Satellite for automating of patch installation
- Common Criteria and FIPS certification of solutions
- 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
  - OpenControl efforts, easier YAML input, variety of remediation tools
  - Other platforms? Give us your feedback: Windows OpenSCAP community
- 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
- 50 other

Severity of failed rules
- 33 other
- 8 low
- 100 medium
- 10 high

Score
- Scoring system: unix.cccdf.scoring:default
  - Score: 60.86739
  - Maximum: 100.000000
  - Percent: 60.89%

Rule Overview

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

Search through XCCDF rules

Group rules by:
- Result

<table>
<thead>
<tr>
<th>Group</th>
<th>Severity</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>result = error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>result = fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>result = notchecked</td>
<td></td>
<td></td>
</tr>
<tr>
<td>result = pass</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Uninstall nsh Package: unknown
- Disable rsync Service: high
- Disable nexec Service: high
- Disable nsh Service: high
- Uninstall nsh-server Package: high
- Remove Reh Trust Files: high
- Remove telnet Clients: low
TREND TOWARDS SMART RESPONSES TO BRANDED ISSUES

Branded issues / issues of high risk
A branded issue isn't always one of high risk.

BRANDED
LOW RISK

BRANDED
HIGH RISK

NOT BRANDED
HIGH RISK

Kernel keychain overflow CVE-2016-0728
Glibc overflow CVE-2015-7547
Samba DCE/RPC CVE-2015-5370
Overcloud image password CVE-2015-4474
JGroups auth bypass CVE-2016-2141
Kernel challenge ack CVE-2016-5696
BIND DoS CVE-2016-2776+

Figure 4
SPECTRE AND MELTDOWN PATCHES

<table>
<thead>
<tr>
<th>Release</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 7</td>
<td>7.4z, 7.3 EUS, 7.2 AUS &amp; SAP, 7.4-ALT, 7.5-ALT</td>
</tr>
<tr>
<td>RHEL 6</td>
<td>6.9z, 6.7 EUS, 6.6 AUS, 6.5 AUS, 6.4 AUS, 6.2 AUS</td>
</tr>
<tr>
<td>RHEL 5</td>
<td>5.11 ELS, 5.9 AUS</td>
</tr>
<tr>
<td>RHEV / RHV</td>
<td>3, 3 ELS, 4</td>
</tr>
<tr>
<td>OpenStack Platform</td>
<td>6, 7, 8, 9, 10, 11, 12</td>
</tr>
</tbody>
</table>

- Broad coverage of Red Hat Platforms on Jan 3 (early break of embargo)
- Container base images updated within SLA
- Only vendor who delivered support on RHEL 5 / Linux Kernel 2.x
RED HAT PRODUCT SECURITY OVER THE YEARS

Total CVEs and RHSAs by Year

Total CVEs Fixed by Severity

#redhat #rhsummit  
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
  - Network Bound Disk Encryption Use Case
- 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 2018

Remember over 50 security sessions to choose from!

Sessions (a sampling)

- The Red Hat Security BoF: Ask Us (Almost) Anything
- Getting Strategic About Security
- Defend Yourself Using Built-in RHEL Security Technologies
- Automating Security & Compliance For Hybrid Environments
- Path To Success With Your Red Hat Identity Management Deployment

- Booth: Hat: IT Optimization
  - NBDE with TPM demo
  - USBGuard demo
  - Identity Management demo
  - Product Security Team
- Practical SCAP
- Deploying SELinux Successfully in Production Environments
- Red Hat Security Roadmap for Hybrid Cloud
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

+ plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos