SECURITYWEEK NETWORK:

- Information Security News
- Infosec Island
- Suits and Spooks

Security Experts:

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe (Free)
- Security White Papers
- ICS Cyber Security Conference
- Contact Us

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - White Papers
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
  - Whitepapers
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance
  - Risk Management
  - Compliance
  - Privacy
  - Whitepapers
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - White Papers
  - Network Security
  - Application Security
- Management & Strategy

Disrupting the Disruptor: Security of Docker Containers

By David Holmes on April 15, 2015

Docker Security: How Secure are Containers and Will Security be a Hurdle to Container Adoption?

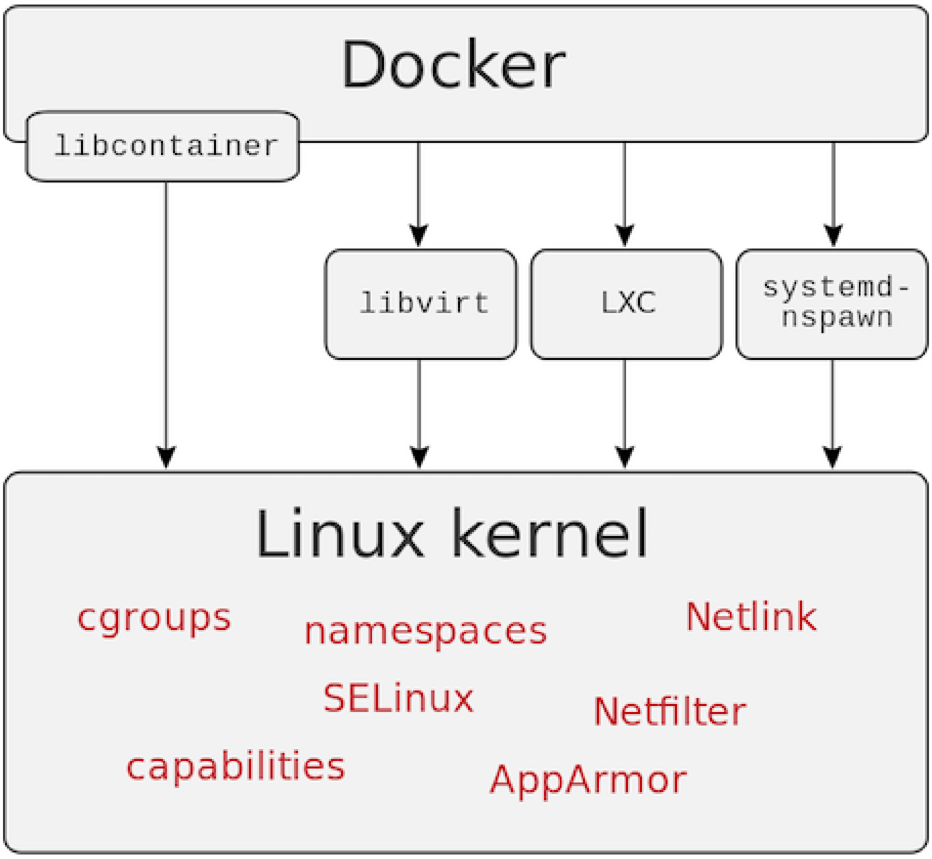
In 1897, physiologist René Quinton completely replaced the blood of a live, abandoned dog with seawater in an experiment to prove the theory that the chemistry of mammalian blood is formulated from ocean water, with which it shares many properties including salinity and acidity. Ancient life forms co-opted other primitive life forms in a symbiotic state to harvest oxygen from seawater. When the advanced life forms moved out of the ocean, they brought forward those primitives with them to maintain the seawater within themselves. Isn’t it bizarre that, millions of years later, we still carry around our own seawater and all its supporting apparatus?

In the digital age, we have brought forward similar primitives into our computing clouds: virtual versions of desktop operating systems from the 90s: Windows, BSD and Linux. It’s bizarre because these bulky, inefficient virtual guest operating systems are just supporting apparatus for an application.

But now a form of virtualization called containers may obsolete virtual operating systems. Containers are host processes that have advanced support for multi-tenancy and privilege isolation. Applications can run inside a container more efficiently than inside a whole virtual operating system.

And just as VMware rode the wave of operating system virtualization to fame and fortune, there’s a new company named Docker riding the popularity of containers. Docker is fast becoming synonymous with container technology and as a result is the new open-source debutante that everyone wants to date.

So will containers replace traditional operating system virtualization in the same way that virtualization has replaced much of the physical, bare-metal world? And how secure are containers, anyway? Will that be a stumbling block to container adoption?



A recent Gartner analysis of Docker security largely gives Docker security a thumbs up (while noting shortcomings in management and maturity). Because the overall concept of cloud security has already been accepted, the argument now is just about the level of protection. We're probing the mechanics of the immune system, not deciding whether the concept lives or dies. The Gartner analysis for Docker security reiterates some of the main points from Docker's own security page.

- **Virtualization security** has migrated into the host operating system. Linux and Microsoft kernels have been providing more support for virtualization in every release. The LXC (Linux container) and *userspace* file systems secure the containers at the host operating system level. This helps traditional virtualization as well and enables containers to focus on efficiency.

- A **container system** has a smaller threat surface than the traditional virtualization system. Because containers consolidate redundant shared resources, there will be fewer versions of Apache (and its entire mod ecosystem) to attack, and fewer processes to manage. A smaller attack surface is always a good thing.

- **Process security controls** will be applied to containers. Process security is an ancient black art: easy to misconfigure, often disabled, and it often doesn't do what you think it should. But the underlying technology should only get better.

On a fundamental level, container security is equivalent to hypervisor security. If you can suspend your disbelief about security to the point where you accept the additional layer of risk because there is no "air gap," then you've got to be good with both hypervisors and containers. Sure, Docker is not as mature as VMware, but that's just one parameter in your equation—as container security matures, the reduced threat surface may lead to fewer vulnerabilities than full virtual machines.

Docker is already supported by the major cloud infrastructures: Google, Amazon Web Services, IBM, and now Microsoft. The promise of container efficiency is leading some to predict that containers will eventually replace traditional virtualization systems. The ability to spin up containers in a second or less means they will proliferate to deliver their value and then disappear, allowing the underlying operating system to boost the efficiency of the application's circulatory system.

Perhaps there is a Dr. Quinton right now running an experiment to see how effectively containers may replace the traditional virtual system. And just to fully close the loop and put your mind at ease, in the dog experiment, the dog whose blood was replaced with seawater was incredibly ill—close to death, actually—but then fully recovered in a week’s time. Happy ending.

David Holmes is an evangelist for F5 Networks' security solutions, with an emphasis on distributed denial of service attacks, cryptography and firewall technology. He has spoken at conferences such as RSA, InfoSec and Gartner Data Center. Holmes has authored white papers on security topics from the modern DDoS threat spectrum to new paradigms of firewall management. Since joining F5 in 2001, Holmes has helped design system and core security features of F5's Traffic Management Operating System (TMOS). Prior to joining F5, Holmes served as Vice President of Engineering at Dvorak Development. With more than 20 years of experience in security and product engineering, Holmes has contributed to security-related open source software projects such as OpenSSL. Follow David Holmes on twitter @Dholmesf5.

Previous Columns by David Holmes:

In Memoriam: Goodbye to RC4, an Old Crypto Favorite
What's the Disconnect with Strict Transport Security?
How "Let's Encrypt" Will Challenge The CA Industry
Should You Be Worried About BGP Hijacking your HTTPS?
Stack Ranking the SSL Vulnerabilities for the Enterprise

Tags:

INDUSTRY INSIGHTS Cloud Security

2 Comments SecurityWeek provides information security news and analysis.

1 Исследовательс...

Recommend Share Sort by Best

Join the discussion…

Ismo · 7 months ago

Precise and informative write up. Can container technology replaces the use of servers in a complex network.

Reply · Share ›

Sergio Arcos · 7 months ago

I don't agree with some of your statements. Virtualization haven't replace bare metal, it's just a complementary tool, like containers are. You must use them wisely to get a better benefit.

Reply · Share ›

ALSO ON **SECURITYWEEK PROVIDES INFORMATION SECURITY NEWS AND ANALYSIS.** WHAT'S THIS?

T-Mobile 'Incredibly Angry' Over Breach via Credit Bureau

1 comment • a month ago

Optimist911 — Anger doesn't help, unless he turns into a green, heavily muscled giant who can run roughshod over the problem and …

vBulletin Website Offline After Hacker Attack

1 comment • 15 days ago

Nick — Precisely what happened here isn't clear yet, but one of the common ways that a site is hacked is first by getting PHP code …

Flaw Allows Hackers to Find Ubiquiti Devices Exposed to Web

1 comment • 11 days ago

WhatADouche — Not to be confused with Ubiquiti Hosting, a spammer haven.

The Harsh Truth of the Cybersecurity Talent Gap

2 comments • 21 days ago

KimOsoba — Spot on run thru of the "history of IT talent" of the 2000s. As a someone who has spent the past 15 years working in …

Subscribe Add Disqus to your site Privacy DISQUS

Google™ Custom Se Search

Subscribe to SecurityWeek

Enter Your Email Address Subscribe

Most Recent Most Read

- Attacks Revive Debate on Encryption, Surveillance
- Docker Boosts Security for Containerized Applications
- Changing the Economics of Cybersecurity
- State-Sponsored Attackers Use Web Analytics for Reconnaissance
- Anonymous Hackers Declare War on IS: Video
- Libpng Library Updated to Patch Vulnerabilities
- Thousands of Sites Infected With Linux Encryption Ransomware
- Conficker Worm Shipped With Police Body Cameras
- Gmail to Warn When Messages Take Unencrypted Routes
- Researcher Hijacks Android Phone via Chrome Vulnerability

Popular Topics

Information Security News
IT Security News
Risk Management

- Cybercrime
- Cloud Security
- Application Security
- Smart Device Security

Security Community

- IT Security Newsletters
- IT Security White Papers
- Suits and Spooks
- ICS Cyber Security Conference
- CISO Forum
- InfosecIsland.Com

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group
- Cyber Weapon Discussion Group
- RSS Feed
- Submit Tip
- Security Intelligence Group

About SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us

Wired Business Media