Dhiru Kholia

+91 9689327876
dhiru@openwall.com
kholia
@DhiruKholia

Open Source & Research Work

John the Ripper

- Authored over 1024 commits in John the Ripper (JtR) repository, resulting in addition of more than 128 plugins, for cracking Apple Keychain, ZIP, PDF, and MS Office files among lot other things ▸
- My Apple DMG cracking plugin for JtR was used to recover the forgotten password of the CTO of WhiteHat Security ▸

Miscellaneous

- Discovered a critical cryptographic flaw in the Audible DRM (Digital Rights Management) scheme, and found ways to bypass Audible's content downloading protections. This work was accepted in REcon 2016 conference [1]. Worked with Amazon to fix these problems.
- Presented a research paper on Dropbox security in USENIX WOOT '13 titled "Looking inside the (Drop) box" ▸ Listed on Dropbox's Special Thanks page ▸ [2].
- Independently rediscovered a critical cryptographic flaw (CBC padding oracle attack) in Oracle's O5LOGON authentication protocol (CVE-2012-3137). Published Ettercap, JtR, and Nmap plugins to demonstrate, and exploit the vulnerability ▸
- Reverse engineered various authentication schemes used in Cisco's proprietary protocols. This work enables auditing of proprietary authenticated networking protocols, and also improves multi-vendor interoperability ▸ Cisco's PSIRT acknowledged, and appreciated this reversing work.
- Created an Ettercap plugin to demonstrate the first practical man-in-the-middle downgrade attacks on Kerberos servers. These attacks work against the latest versions of Active Directory & MIT Kerberos servers, and allow a speed-up of over 4000x while brute-forcing the network authentication hashes offline. Also published various other Ettercap plugins for dissecting, and auditing network authentication traffic. Member of the Ettercap organization on GitHub ▸
- I have contributed patches to Metasploit, Nmap, Go, CPython, and Wireshark projects. I also have commit access to FFmpeg, JtR, and DynamoRIO projects.

Skill Set

Languages	Python, C, Go, Java, JavaScript, Bash
Cloud	OpenStack, Google Cloud Platform (GCP), Amazon Web Services (AWS)
Virtualization	KVM, Docker, Xen, VMware ESX, VirtualBox
Miscellaneous	IDA Pro, Android Reversing, Hardware Security, SELinux, AppArmor, JVM, Burp Suite, GDB, Coverity, Wireshark ▸
Certifications	RHCA ▸ RHCSS, CCNA, SCJP, CEH

Work Experience

May 2016 - current **Red Hat**, *Senior Product Security Engineer*, Pune.

- I handle security response for Red Hat products, especially Red Hat Enterprise Linux. I also do proactive application design reviews, source code reviews, and pentesting.

April 2014 - Jan 2016 **Spotify**, *Product Security Engineer*, Stockholm.

- Full-stack security work including internal corporate security (anti-phishing, endpoint security, security awareness training), incident response, handling incoming bug bounty reports, code reviews, web application fuzzing, threat modeling, protocol fuzzing, SecOps, deployment, and configuration reviews.
- Wrote AppArmor profiles to sandbox backend applications, and Docker containers heavily. This work was a part of an in-house security anomaly detection engine built around the Elastic Stack.
- Used AddressSanitizer (ASan) to find and fix bugs which were lurking in production code for almost 10 years!
- Created an anti-phishing bot to classify and automatically respond to incoming email reports. This bot allows us to detect phishing attacks, and move faster against the attackers. Led internal anti-phishing training efforts using ThreatSim platform.

March 2013 - April 2014 **Red Hat**, *Product Security Engineer*, Pune.

- Found, and helped in fixing more than 120 proactive hardening bugs in Fedora within two weeks by developing open-source automated analysis tools which are an order of magnitude faster than the existing ones.
- Wrote exploits for multiple security bugs. E.g. OpenStack DoS tool for bug #1175906, a wide impact exploit for CVE-2013-2215, user tracking exploit (CVE-2012-5639) for OpenOffice, code-execution using source itself (CVE-2013-5106).
- Convinced the Fedora committee to use stronger compilation flags, disable prelink, and enable format-security in Fedora. While eliminating string format vulnerabilities completely, I filed close to 400 bugs, and contributed patches to Go language to improve its DWARF parsing functionality ▸
- Did code review of multiple Python packages included in RHEL 7, and found a remote code execution bug (RCE) in powerpc-utils-python package (CVE-2014-8165) ▸
- Collaborated with multiple upstream projects to improve their security posture - persuaded PHP upstream to fix six-month old hardening bugs in a single day, got my patch for enabling the usage of AddressSanitizer accepted in Ruby MRI and CPython projects ▸
- Started and led the work on having "Reproducible Builds" (deterministic builds) for Fedora. This is one of the foundational steps required in establishing end-to-end trust in software ▸

Dec 2011 - March 2013 **sTec Inc**, *Software Engineer*, Pune.

- Developed a WUI (Web User Interface) for an enterprise class SSD caching solution, named EnhanceIO, using Python, C, CherryPy, Django, and jQuery.
- Improved the packaging of our product by using PyInstaller, reduced the number of files by 95% (five thousand to a few hundred), and installation time by 80%.
- Found and fixed critical security bugs (e.g. RCE, XSS) before the product shipped. Monitored new security vulnerabilities, and took proactive actions to mitigate potential risks.
- Developed solid debugging skills by resolving multiple memory usage, correctness, and performance bugs in the code base.

Apr 2011 - Sep 2011 **Google Summer of Code (GSoC)**, *Software Developer*, Vancouver, Canada.

- Extended John the Ripper password cracker to support cracking of non-hashes like OpenSSH private key passphrases, RAR files, and PDF files under the mentorship of Solar Designer. Went on to become a major contributor to the JtR project ▸

Sep 2009 - Jul 2011 **UBC Computer Science**, *Research & Teaching Assistant*, Canada.

- Worked on cutting-edge projects like, execution mining (generating parallel data flow graphs for huge virtual machine execution datasets using Amazon Cloud Services), smaFS (a versioning file system), Request Broker (a backend server for a web based time-traveling debugger written using Python Twisted), password cracking using GPUs, and VEC (video encoding on the cloud done using Celery, Django and Amazon S3).
- In the execution mining project, we reduced the processing time of an execution mining data set from 12 hours to 50 minutes by using 200 CPU cores on Amazon Cloud.
- Assisted teaching of CPSC 260 - Object Oriented Program Design, CPSC 221 - Basic Algorithms & Data Structures, and CPSC 313 - Computer Hardware & Operating Systems courses.

Jan 2009 - Aug 2009 **PTC Inc**, *Systems Engineer*, Pune.

- Lead build, release engineer, and system administrator for the Precision LMS project. Precision LMS is a web-based training solution for PTC's software products, written using the Java stack.
- Implemented and supported the setup of Nagios for monitoring, Apache for load balancing, hardened web servers, facilitated Java application and web server performance tuning exercises. Took the initiative in migrating the legacy Perl codebase to PHP. Did initial debugging of load balancing problems, JVM crashes, database and application performance problems.

Jul 2006 - Dec 2008 **SETLabs, Infosys**, *Software Engineer, R&D*, Pune.

- Discovered a critical flaw in the employee attendance tracking software, developed an exploit for the same, and successfully demonstrated submitting proxy attendance for employees.
- Led the GridOS project, which builds efficient OS guest images. Optimized bootup time of Fedora to under 4 seconds by re-writing SysVinit. Built 98% smaller, faster, and more secure custom Linux kernels.
- Co-authored a research paper on optimal strategy for migrating VMs for improving consolidation ratio. We proposed a new migration strategy based on time-windows instead of the popular event-based approach ▸

Publications

[1] Dhiru Kholia. Audible DRM scheme. *REcon, Montreal, Canada*, 2016.

[2] Dhiru Kholia and Przemysław Węgrzyn. Looking inside the (Drop) box. In *the Proceedings of the 7th USENIX Workshop on Offensive Technologies (WOOT)*, Berkeley, CA, 2013. USENIX.

Education

Aug 2002 – May 2006 **B.E. in Electronics and Telecommunication**, *University of Pune*, Pune.

First Class With Distinction, College Topper, Ranked among top 1% in the University.