

Alexander Scheel

Alexander Maurice Scheel
alexander.m.scheel@gmail.com
cipherboy.com – personal website
he/him

3035 Whisperwood Dr. Apt. 347
Ann Arbor, MI 48105
C: (507) 206-8310

GitHub – cipherboy
Pagure – cipherboy
Fedora Project – cipherboy
LinkedIn

[Overview]

- Interests in algorithm, protocol, and application development.
- Algorithmic specialties include cryptography, boolean satisfiability, and graph theory.
- Research interests include logical cryptanalysis of hash functions.

[Experience]

Red Hat – Software Engineer – Red Hat Certificate System September 2018 – *present*

- Primary maintainer of [JSS](#) a [NSS](#) wrapper for Java
- Major projects include developing [javax.net.ssl](#) support, extending Java Cryptography Architecture (JCA) compatibility, and low-level algorithm enablement.
- Development team lead; frequent cross-team and cross-organization contributions.
- Contributor to many open source ecosystems including Dogtag PKI, FreeIPA, OpenSCAP, NSS, MIT Kerberos, fapolicyd, rpminspect, and FreeRADIUS.
- Fedora and RHEL maintainer contributing to efforts such as the Stewardship and Java Maintenance SIGs.

Red Hat – Intern – OpenSCAP June 2018 – August 2018

- Simplified SME contribution experience to the [Compliance as Code](#) project.
- 95 accepted [pull requests](#) to Compliance as Code and 25 accepted [pull requests](#) to OpenSCAP and SCAP Workbench.

Red Hat – Intern – Identity Management June 2017 – August 2017

- Focused on enabling [Channel Bindings](#) in MIT Kerberos.
- Over 20 accepted pull requests across MIT Kerberos, gssproxy, ding-lib, python-gssapi, and libverto.
- Contributed to improving Kerberos interactions with SSH and NFS (Red Hat Bugzillas [#1199363](#), [#1477231](#), and [#1463665](#)).

ISEAGE – Lab Staff October 2016 – May 2018

ISEAGE is a security research lab at ISU which runs five Cyber Defense Competitions each year under the direction of Dr. Doug Jacobson.

- Developed scenario VM images, exploitable backdoors, and competition anomalies for use in an isolated environment.
- Competition roles include Competition Director, Red Team (volunteer hackers) Lead and Green Team (usability testing) Lead.
- Multiple responsibilities including lab leadership, sponsorship activities, and infrastructure development.

IBM Cloud Managed Services – Intern May 2016 – August 2016

CMS is a portion of IBM providing managed services on top of a diverse cloud platform for hundreds of companies.

- Automated compliance and security; improved developer workflow and auditing of compliance with Nessus and AppScan on Source.
- Technical mentorship under Steven J. Munroe. Optimizations for SHA-3 on Power8+ assembly with vector instructions.

[Projects]

Open-Source Contributor 2010–always

- Contributes to several open source projects including [CryptoMiniSat](#), [Gitea](#), [Let's Encrypt Boulder](#), [cryptofuzz](#), and [Apache Tomcat](#).
- Publishes [over 75 open-source projects](#) including [cmsh](#), [p](#), [sharg](#), [SSSa libraries](#), and many others.
- Former [Ubuntu Forums](#) contributor with over 600 posts.

Collisions in Hash Functions 2017 – 2018

- Research under Dr. Eric W. Davis (Rozier) and Dr. Clifford Bergman.
- Modeling collisions in hash functions as 3-CNF-SAT problems.
- Deriving metrics of utilities of collisions to evaluate impact of a collision.
- Analyzing breadth of collision malleability.
- Improving bounds for second preimage attacks.
- Contributing to [open access](#) and [open source](#) research.
- "Measuring Hash Trustworthiness via Collision Utility Metrics: Logical Cryptanalysis of MD4"
A. Scheel and E. Rozier (unpublished)

Cryptopals 2016–present

Cryptographic challenges which attacking insecure assumptions. Completed 54 out of 56 problems in Go.

crypto-collection 2016–2017

Various cryptographic algorithms with cross-architecture implementations in C.

COMS 309 – EduTLS 2016

TLS 1.2 library implemented in C++ as part of an API-based web framework.

[Education]

Iowa State University (2015 – 2018) @ 3.75 GPA

- Honors College Project: Collisions in Hash Functions (see above)
- Degrees: Computer Science and Mathematics
- Honors: [ΦBK](#) Junior Inductee, Spring 2017
- Honors: *magna cum laude* & Honors Program

[Awards]

ACM ICPC – North Central North America region

- Fall 2017: 1st in site, 4th place overall

ΦBK Junior Inductee, Spring 2017

ISEAGE Cyber Defense Competitions

- ISU CDC: 5th place – Fall 2016
- ISU CDC: 4th place – Spring 2016
- National CDC: 1st place – 2016
- ISU CDC: 2nd place – Fall 2015

[Buzzwords]

Programming Languages:

C, Java, Python, Go, C++, Bash, Ansible, rpmspec, SQL, HTML5, CSS3, JSX, React, JavaScript, PHP

Operating Systems: Fedora, RHEL, CentOS, Ubuntu, Debian, occasionally Gentoo

Orchestration: Podman, Docker, KVM, libvirt, AWS, GCE, DigitalOcean, RHEV

Project Management: Git, [GitHub](#), [Pagure](#), Gitea

Protocols and Encodings: TLS, Kerberos, ASN.1, XML, JSON, YAML

Editors: Atom, Brackets, Gedit, Vi, Emacs, Nano, Eclipse, Word, Google Drive

Daemons: Apache httpd, Apache Tomcat, MySQL, MariaDB, PostgreSQL, SSH, Nginx, FreeRADIUS, Kerberos

References available upon request