Michael K. Mabey

(480) 788–3411 ◇ mmabey@asu.edu ◇ mikemabey.com
LinkedIn

EDUCATION

Ph.D. Computer Science — Information Assurance *(expected) Dec 2017*
Arizona State University Tempe, AZ
Committee: Gail-Joon Ahn (Co-Chair), Adam Doupé (Co-Chair), Stephen S. Yau, Jooyung Lee, Ziming Zhao
Research Topics: Web environment forensics, Email forensics, Chrome OS forensics

M.S. Computer Science — Information Assurance *Aug 2011*
Arizona State University Tempe, AZ
Committee: Gail-Joon Ahn (Chair), Stephen S. Yau, Dijiang Huang
Thesis: Collaborative Digital Forensics: Architecture, Mechanisms, and Case Study

> In order to catch the smartest criminals in the world, digital forensic examiners need a means of collaborating and sharing information that is not prohibitively difficult to use and that complies with standard operating procedures and the rules of evidence. In this thesis I present the design and implementation of the Collaborative Forensic Framework (CUFF) which is a cloud-based forensic analysis environment that facilitates collaboration among examiners and their trusted colleagues. CUFF makes a positive impact on forensic examiners' efficiency by helping them leverage their network of subject matter experts while also tapping into the scalability and power of the cloud.

B.S. Computer Science — Information Systems *May 2009*
Utah State University Logan, UT

EXPERIENCE SUMMARY

Research Assistant *Nov 2009 – Present*
Security Engineering for Future Computing (SEFCOM) Lab, ASU Tempe, AZ

Civilian Reserve/Intern *May 2016 – Aug 2016*
Arizona Department of Public Safety Phoenix, AZ

Teaching Assistant *Aug 2010 – Dec 2015*
Arizona State University Tempe, AZ

SAT/ACT Instructor *Sep 2015 – Oct 2015*
Minerva Learning, LLC Chandler, AZ

Summer Intern *Jul 2015 – Sep 2015*
Arizona Cyber Threat Response Alliance (ACTRA) Phoenix, AZ

Teaching Assistant (Instructor of Record) *Aug 2011 – Dec 2014*
Arizona State University Tempe, AZ

Student Trainee (Civilian) *Jun 2013 – Aug 2013, Jun 2014 – Aug 2014*
US Army Fort Meade, MD

Graduate Student Summer Intern *May 2011 – Jul 2011*
Sandia National Laboratories Albuquerque, NM

Graduate Student Recruitment Specialist/Webmaster *Jul 2006 – Aug 2009*
Electrical & Computer Engineering Department, USU Logan, UT

Technician Aid *Sep 2006 – Aug 2009*
Electrical & Computer Engineering Department, USU Logan, UT

Store Attendant *Jun 2005 – Sep 2008*
Electrical & Computer Engineering Department, USU Logan, UT

Lab Technician *May 1997 – Aug 2002*
KWM Electronics Co. West Jordan, UT

HONORS AND AWARDS

- DoD Information Assurance Scholarship Program (IASP) Recipient (5 years) *2012 – 2017*
- Inducted into Eta Kappa Nu (HKN) Engineering Honors Society *Nov 2010*
- Eagle Scout, Boy Scouts of America *2002*

RESEARCH INTERESTS

- Digital Forensics
  - Web and Email Forensics
  - Forensics on Non-Traditional Devices
- Cyber Security
  - Threat Intelligence Sharing
  - Web Security

RESEARCH EXPERIENCE

Research Assistant *Nov 2009 – Present*
Security Engineering for Future Computing (SEFCOM) Lab, ASU Tempe, AZ
Lab Directors: Gail-Joon Ahn, Adam Doupé, Ziming Zhao

- Projects:
  - Created a method for identifying extensions installed on **Chrome OS** by analyzing the encrypted files on the hard drive. Wrote an accompanying crawler in **Python** (and using **Ansible**, **Celery**, **MySQL**, **sshfs**, and **OpenStack**) to download all extensions on the Chrome Web Store and analyze them.
    Publications: [J1, P2, BL2, BL3]
  - Helped design and implement a cloud-based version of the International Capture the Flag (iCTF) competition, allowing educators to more easily host their own CTF competitions. Used **Ansible**, **Vagrant**, **Amazon EC2**, and **Python** for the implementation and deployment.
    Publications: [C1]
  - Developed a forensic acquisition approach for web email that reestablishes persistent cookie sessions stored by a browser, and automated the process using **Python** and **Selenium**.
    Publications: [C3]
  - Designed and implemented the core components of a modular, highly scalable, collaboration-centric digital forensic framework built on the **OpenStack** cloud architecture. Functions of the components included distributed job scheduling, storage management, and concise evidence representation and transmission.
    Publications: [C4, BC1, P4]
- Other experience:
  - Maintained fifteen servers for the lab, including a public-facing router, an **OpenVPN** server, a reverse-proxy web server with **TLS** certificate management, an **OpenStack** cloud, switches transmitting **VLAN**-tagged traffic, and a **GitLab** server.
- Sponsors:
  - Department of Defense Information Assurance Scholarship Program (IASP)
  - Department of Energy
  - National Science Foundation

PUBLICATIONS

Peer–Reviewed Conference Proceedings

[C1] Erik Trickel, Francesco Disperati, Eric Gustafson, Faezeh Kalantari, **Mike Mabey**, Naveen Tiwari, Yeganeh Safaei, Adam Doupé, and Giovanni Vigna. "Shell We Play A Game? CTF-as-a-service for Security Education". In: *2017 USENIX Workshop on Advances in Security Education (ASE 17)*. USENIX Association, August 2017.

[C2] Wonkyu Han, **Mike Mabey**, and Gail-Joon Ahn. "Simulation-based validation for smart grid environments". In: *Proceedings of the 2013 IEEE 14th International Conference on Information Reuse and Integration, IEEE IRI 2013*. IEEE Computer Society, 2013, pp. 14–21.

[C3] Justin Paglierani, **Mike Mabey**, and Gail-Joon Ahn. "Towards Comprehensive and Collaborative Forensics on Email Evidence". In: *Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on*. October 2013, pp. 11–20. DOI: 10.4108/icst.collaboratecom.2013.254125.

[C4] **Mike Mabey** and Gail-Joon Ahn. "Towards Collaborative Forensics: Preliminary Framework". In: *Information Reuse and Integration (IRI), 2011 IEEE International Conference on*. August 2011, pp. 94–99. DOI: 10.1109/IRI.2011.6009527.

Peer–Reviewed Journal Papers

[J1] **Mike Mabey**, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. "dbling: Identifying extensions installed on encrypted web thin clients". In: *Digital Investigation* 18 (August 2016), S55–S65. ISSN: 17422876. DOI: 10.1016/j.diin.2016.04.007.

[J2] Wonkyu Han, **Mike Mabey**, Gail-Joon Ahn, and Tae Sung Kim. "Simulation-Based Validation for Smart Grid Environments: Framework and Experimental Results". In: *Integration of Reusable Systems*. Ed. by Thouraya Bouabana-Tebibel and Stuart H Rubin. Vol. 263. Advances in Intelligent Systems and Computing. Springer International Publishing, 2014, pp. 27–44. ISBN: 978-3-319-04716-4. DOI: 10.1007/978-3-319-04717-1_2.

Peer–Reviewed Book Chapters

[BC1] **Mike Mabey** and Gail-Joon Ahn. "Towards Collaborative Forensics". In: *Information Reuse and Integration in Academia and Industry*. Ed. by Tansel Özyer, Keivan Kianmehr, Mehmet Tan, and Jia Zeng. Springer Vienna, 2013, pp. 237–260. ISBN: 978-3-7091-1537-4. DOI: 10.1007/978-3-7091-1538-1_12.

Invited Talks

[T1] **Mike Mabey**. "dbling: Identifying Extensions Installed on Encrypted Web Thin Clients". August 2016.

Poster Presentations

[P1] Erik Trickel, Faezeh Kalantari, Yeganeh Safaei, Lakshmi Srinivas, Naveen Tiwari, **Mike Mabey**, Sukwha Kyung, and Wonkyu Han. *Capture the Flag in the Cloud*. *Symposium on Information Assurance Research and Education, ASU*. October 2016.

[P2] **Mike Mabey**, Jeremy Whitaker, Gail-Joon Ahn, and Adam Doupé. *Towards Forensics for Web Thin Clients*. *Symposium on Information Assurance Research and Education, ASU*. November 2015.

[P3] Jeremy Whitaker, **Mike Mabey**, Gail-Joon Ahn, and Adam Doupé. *Forensic Analysis on Mobile Devices*. *Symposium on Information Assurance Research and Education, ASU*. October 2014.

[P4] **Mike Mabey**, Justin Paglierani, and Gail-Joon Ahn. *Towards Collaborative Forensics*. *Workshop on Information Assurance Research and Education, ASU*. April 2012.

[P5] James Bridges, Kasimir Gabert, and **Michael Mabey**. *Cyber Tracer*. *University Day, Sandia National Laboratories*. July 2011.

TEACHING INTERESTS

- Computer and Network Forensics
- Advanced Topics in Digital Forensics
- Information Assurance
- Security Toolkit Programming with Python
- Cryptography
- Software Security

TEACHING EXPERIENCE

Invited Lectures

- "IoT Security" — CSE 465, ASU. Invited by Dr. Stephen S. Yau *Nov 2016*
- "Introduction to Cryptography" — CSE 465, ASU. Invited by Dr. Stephen S. Yau *Sep 2016*

Teaching Assistant *Aug 2010 – Dec 2015*
Arizona State University Tempe, AZ

- CSE 465 Information Assurance with Dr. Gail-Joon Ahn: Fall 2010, Fall 2015.
- CSE 469 Computer and Network Forensics with Dr. Gail-Joon Ahn: Spring 2015.
- FSE 100 Introduction to Engineering with Dr. Ryan Meuth: Spring 2014.
- CSE 423/424 Capstone I and CSE 485/486 Capstone II with Dr. Debra Calliss: Spring 2014.
- CSE 467 Data & Information Security with Dr. Gail-Joon Ahn: Spring 2011.

SAT/ACT Instructor *Sep 2015 – Oct 2015*
Minerva Learning, LLC Chandler, AZ

- Individual tutor for a high school student preparing for the PSAT.

Teaching Assistant (Instructor of Record) *Aug 2011 – Dec 2014*
Arizona State University Tempe, AZ

- CSE 465 Information Assurance: Fall 2014.
- FSE 100 Introduction to Engineering: Fall 2011 – Fall 2013 (5 semesters).

ACADEMIC ACTIVITIES

Fulton Undergraduate Research Initiative (FURI) Mentor

- Adric Rukkila B.S. in Computer Science at ASU *Sep 2016 – May 2017*
  Topic: Leveraging Cloud Service APIs for Forensic Data Collection

Undergraduate Honors Thesis Mentor

- Samantha Juntiff B.S. in Computer Science at ASU *Spring 2015*
  Thesis: Squeegee: Integrating Forensic Tools for Collaborative Forensic Analysis

TECHNICAL STRENGTHS & QUALIFICATIONS

Programming Languages	Python, C/C++, HTML, CSS, LaTeX
Forensic Tools	FTK, Sleuth Kit & Autopsy, dd, HxD, etc.
Protocols & APIs	JSON, XML, AMQP, REST, STIX, RabbitMQ
Network Administration/Security	OpenVPN, ufw, lighttpd, Caddy, Wireshark
Operating Systems	Windows, Linux, Chrome OS
Cloud Architectures	OpenStack, Amazon EC2
Databases	MySQL, SQLite

SERVICE

Department

- Admin Team: UCSB International Capture the Flag (iCTF) *2017*
  Publications: [C1]
- Team Leader: ASU team in the UCSB iCTF *2009, 2010, 2014, 2015*
- Panelist: PhD Open House Student Panel *Feb 2014, Feb 2015*

Profession

- Conference Proceedings Subreviewer:
  - ACM CODASPY *2013, 2014, 2015, 2016, 2017*
  - SACMAT *2014*
  - ASIACCS *2014*
- Student Volunteer:
  - ACM CODASPY *2017*
  - ACM CCS *2014*
- Student Program Committee Member:
  - IEEE Security & Privacy *2016*

Technical Blog Posts

[BL1] **Mike Mabey**. *How eCryptfs Affects Filename Lengths*. https://mikemabey.com/blog/2017/08/ecryptfs_filenames.html. August 2017.

[BL2] **Mike Mabey**. *How to check out an old version of Chromium OS*. https://mikemabey.com/blog/2016/02/check_out_old_chromium.html. February 2016.

[BL3] **Mike Mabey**. *Fixing repo init to check out Chromium OS code*. https://mikemabey.com/blog/2015/01/fixing_repo_init_chromium_os.html. January 2015.

[BL4] **Mike Mabey**. *Getting into Developer Mode on the HP Pavilion 14 Chromebook*. https://mikemabey.com/blog/2013/05/getting_into_developer_mode.html. May 2013.

[BL5] **Mike Mabey**. *Debian on Android and my quest for a full-fledged terminal Python IDE*. https://mikemabey.com/blog/2012/06/debian_on_android.html. June 2012.

[BL6] **Mike Mabey**. *OpenVPN Update: Fixed!* https://mikemabey.com/blog/2012/06/openvpn-update-fixed.html. June 2012.

PROFESSIONAL EXPERIENCE

Civilian Reserve/Intern *May 2016 – Aug 2016*
Arizona Department of Public Safety Phoenix, AZ

- Updated the content, layout, and topics of the security policy for the Arizona Counter Terrorism Information Center (ACTIC) for clarity and to be in compliance with recommendations from the Department of Homeland Security. Created training slides to accompany the new security policy.

Summer Intern *Jul 2015 – Sep 2015*
Arizona Cyber Threat Response Alliance (ACTRA) Phoenix, AZ

- Designed an operationalized workflow for Arizona Infragard member organizations to share **threat intelligence** through a common **STIX/TAXII** platform.

Student Trainee (Civilian) *Jun 2013 – Aug 2013, Jun 2014 – Aug 2014*
US Army Fort Meade, MD
Grade: GG-09 Step 1 *Service*: Excepted *Tenure*: Permanent

- Summer internships in connection with DoD IASP scholarship.

Graduate Student Summer Intern *May 2011 – Jul 2011*
Sandia National Laboratories Albuquerque, NM

- Helped design a dynamic malware analysis framework built on **OpenStack**, allowing incident responders to define customizable analysis environments and use arbitrary analysis tools for triage or manual analysis.
- Wrote **Python** scripts to automate the setup process for using a SheevaPlug computer as a wireless intrusion detection agent running **Kismet**.

Graduate Student Recruitment Specialist/Webmaster *Jul 2006 – Aug 2009*
Electrical & Computer Engineering Department, USU Logan, UT

- Primary responsibilities included maintaining and augmenting the department website using **PHP**, **MySQL**, and other basic web technologies like **CSS**, **JavaScript**, and an **SMTP** server.
- Completed multiple graphic design projects for the department using **GIMP**, **Adobe Photoshop**, and **Adobe Illustrator**.
- Replaced a **MS Access** database by porting the old data to a **MySQL** server and creating a set of **Python** programs with the **Dabo** framework that interfaced with the database.
- Created a testing environment using an **Apache** web server, **PHP**, **MySQL**, and **SVN**.
- Gathered statistics on web visitors, inquiries from students, and applicants' credentials for the purpose of improving the department's graduate student recruitment processes.
- Responded to inquiries from potential domestic and international graduate students.

Technician Aid *Sep 2006 – Aug 2009*
Electrical & Computer Engineering Department, USU Logan, UT

- Built and maintained computers for department faculty and student labs.
- Installed and configured various software on Windows machines for faculty, staff, and students.
- Created and restored backup images of lab computers using **Norton Ghost** and **Acronis TrueImage**.
- Protected lab computers using **Faronics Deep Freeze**.

Store Attendant *Jun 2005 – Sep 2008*
Electrical & Computer Engineering Department, USU Logan, UT

- Maintained equipment and instruments in the labs for electrical engineering students.
- Performed store duties including maintaining inventory, serving customers, cleaning rooms, and running errands.

Lab Technician *May 1997 – Aug 2002*
KWM Electronics Co. West Jordan, UT

- Worked closely with CEO/Head Engineer to build prototypes of electronic devices.
- Used various soldering techniques on both through-hole and surface-mount parts.

PROFESSIONAL MEMBERSHIPS

- IEEE (Student Member)
  - Cybersecurity Community
  - Internet of Things Community
- IEEE Computer Society
- Python Software Foundation (Basic Member)

PROFESSIONAL DEVELOPMENT

- Preparing Future Faculty (GRD 791 at ASU) *Aug 2015 – May 2016*
  The Preparing Future Faculty (PFF) program is a year-long series of seminars, discussions, and activities designed to expose graduate students and postdocs more fully to the realities of teaching, research, and service in higher education.

REFERENCES

Please feel free to contact any of my references.

Gail–Joon Ahn
Director, Center for Cybersecurity and Digital Forensics
Professor of Computer Science and Engineering
Fulton Entrepreneurial Professor
School of Computing, Informatics and Decision Systems Engineering
Ira A. Fulton Schools of Engineering, Arizona State University
Brickyard Engineering (BYENG) Bldg, Room 486
699 S. Mill Avenue
Tempe, AZ 85281
Phone: (480) 965-9007
Fax: (480) 965-2751
http://www.public.asu.edu/~gahn1/
gahn@asu.edu

Adam Doupé
Assistant Professor of Computer Science and Engineering
School of Computing, Informatics and Decision Systems Engineering
Ira A. Fulton Schools of Engineering, Arizona State University
Brickyard Engineering (BYENG) Bldg, Room 472
699 S. Mill Avenue
Tempe, AZ 85281
Fax: (480) 965-2751
http://adamdoupe.com
doupe@asu.edu

Frank J. Grimmelmann
President & CEO/Intelligence Liaison Officer
Arizona Cyber Threat Response Alliance (ACTRA)
Phone: (623) 551-1526
Fax: (623) 551-4221
fgrimmelmann@actraaz.org

Stephen S. Yau
Director, Information Assurance Center
Professor of Computer Science and Engineering
School of Computing, Informatics and Decision Systems Engineering
Ira A. Fulton Schools of Engineering, Arizona State University
Brickyard Engineering (BYENG) Bldg, Room 488
699 S. Mill Avenue
Tempe, AZ 85281
Phone: (480) 965-2647
Fax: (480) 965-2751
http://dpse.eas.asu.edu/yau/
yau@asu.edu