

# Michael K. Mabey

(480) 788-3411 ♦ mmabey@asu.edu ♦ mikemabey.com



LinkedIn

## EDUCATION

---

### **PhD Computer Science – Information Assurance**

*(expected) Dec 2017*

Arizona State University

Tempe, AZ

*Committee:* Gail-Joon Ahn (Chair), Stephen S. Yau, Jooyung Lee, Adam Doupé, 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 work 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

*Lab Directors:* Gail-Joon Ahn, Adam Doupé

### **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

<b>Graduate Student Recruitment Specialist/Webmaster</b> Electrical & Computer Engineering Department, USU	<i>Jul 2006 – Aug 2009</i> Logan, UT
<b>Technician Aid</b> Electrical & Computer Engineering Department, USU	<i>Sep 2006 – Aug 2009</i> Logan, UT
<b>Store Attendant</b> Electrical & Computer Engineering Department, USU	<i>Jun 2005 – Sep 2008</i> Logan, UT
<b>Lab Technician</b> KWM Electronics Co.	<i>May 1997 – Aug 2002</i> West Jordan, UT

### HONORS AND AWARDS

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

### RESEARCH INTERESTS

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

### RESEARCH EXPERIENCE

<b>Research Assistant</b> Security Engineering for Future Computing (SEFCOM) Lab, ASU <i>Lab Directors:</i> Gail-Joon Ahn, Adam Doupé	<i>Nov 2009 – Present</i> Tempe, AZ
<ul style="list-style-type: none"> <li>Projects: <ul style="list-style-type: none"> <li>Researched forensic techniques for <b>Chrome OS/Chromium OS</b> by creating tools in <b>Python</b> and using <b>libvirt</b> to interface with a <b>KVM/QEMU</b> hypervisor. (In progress) <i>Publications:</i> [J1], [P2], [BL1], [BL2]</li> <li>Developed a web email forensic acquisition approach that reestablishes persistent cookie sessions stored by a browser, and automated the process using <b>Python</b> and <b>Selenium</b>. <i>Publications:</i> [C2]</li> <li>Designed and implemented the core components of a modular, highly scalable, collaboration-centric digital forensic framework built on the <b>OpenStack</b> cloud architecture. Functions of the components included distributed job scheduling, storage management, and concise evidence representation and transmission. <i>Publications:</i> [C3], [BC1], [P4]</li> </ul> </li> <li>Sponsors <ul style="list-style-type: none"> <li>Department of Defense Information Assurance Scholarship Program (IASP)</li> <li>Department of Energy</li> <li>National Science Foundation</li> </ul> </li> </ul>	

### PUBLICATIONS

<b>Peer-Reviewed Conference Proceedings</b>
[C1] Wonkyu Han, <b>Mike Mabey</b> , and Gail-Joon Ahn. "Simulation-based validation for smart grid environments". In: <i>Proceedings of the 2013 IEEE 14th International Conference on Information Reuse and Integration, IEEE IRI 2013</i> . IEEE Computer Society, 2013, pp. 14–21.
[C2] Justin Paglierani, <b>Mike Mabey</b> , and Gail-Joon Ahn. "Towards Comprehensive and Collaborative Forensics on Email Evidence". In: <i>Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on</i> . October 2013, pp. 11–20. DOI: 10.4108/icst.collaboratecom.2013.254125.

- [C3] **Mike Mabey** and Gail-Joon 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). The Proceedings of the Sixteenth Annual DFRWS Conference, 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. (Extended version of [C1]). 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. (Extended version of [C3]). 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". Presentation given at the Sixteenth Annual DFRWS Conference on paper [J1]. 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       | · Security Toolkit Programming with Python |
| · Advanced Topics in Digital Forensics | · Cryptography                             |
| · Information Assurance                | · 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**

Arizona State University

*Aug 2010 – Dec 2015*

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**

Minerva Learning, LLC

*Sep 2015 – Oct 2015*

Chandler, AZ

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

**Teaching Assistant (Instructor of Record)**

Arizona State University

*Aug 2011 – Dec 2014*

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  
*Topic:* Leveraging Cloud Service APIs for Forensic Data Collection

*Sep 2016 – Present***Undergraduate Honors Thesis Mentor**

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

*Spring 2015***TECHNICAL STRENGTHS & QUALIFICATIONS**

---

**Programming Languages**Python, C/C++, HTML, CSS,  $\LaTeX$ **Forensic Tools**

FTK, Sleuth Kit &amp; Autopsy, dd, HxD, etc.

**Protocols & APIs**

JSON, XML, AMQP, REST, STIX/TAXII, Protocol Buffers

**Network Administration/Security**

OpenVPN, Wireshark, ufw, Apache, lighttpd

**Operating Systems** Windows,  Linux,  Chrome OS**Databases**

MySQL, SQLite

**SERVICE**

---

**Department**

- Team Member: Development team for UCSB International CTF (iCTF) *2017*
- 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 Program Committee Member:
  - IEEE Security & Privacy *2016*
- Student Volunteer:
  - ACM CCS *2014*

## Technical Blog Posts

- [BL1] **Mike Mabey**. *How to check out an old version of Chromium OS*. <http://mikemabey.blogspot.com/2016/02/how-to-check-out-old-version-of.html>. February 2016.
- [BL2] **Mike Mabey**. *Fixing repo init to check out Chromium OS code*. <http://mikemabey.blogspot.com/2015/01/fixing-repo-init-to-check-out-chromium.html>. January 2015.
- [BL3] **Mike Mabey**. *Getting into Developer Mode on the HP Pavilion 14 Chromebook*. <http://mikemabey.blogspot.com/2013/05/getting-into-developer-mode-on-hp.html>. May 2013.
- [BL4] **Mike Mabey**. *Debian on Android and my quest for a full-fledged terminal Python IDE*. <http://mikemabey.blogspot.com/2012/06/debian-on-android-and-my-quest-for-full.html>. June 2012.
- [BL5] **Mike Mabey**. *OpenVPN Update: Fixed!* <http://mikemabey.blogspot.com/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 AZ 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

- 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 in triage or manual analysis mode.
- 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 **Adobe Photoshop**, **Adobe Illustrator**, and **GIMP**.
- 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 &amp; 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 TruImage**.
- Protected lab computers using **Faronics Deep Freeze**.

**Store Attendant***Jun 2005 – Sep 2008*

Electrical &amp; 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)
- IEEE Computer Society

**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](mailto:gahn@asu.edu) [✉](#)

### **Adam Doupe**

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](mailto: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](mailto: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](mailto:yau@asu.edu) [✉](#)