

# Michael K. Mabey

(480) 788-3411 ♦ [mmabey@ieee.org](mailto:mmabey@ieee.org) ♦ [mikemabey.com](http://mikemabey.com) ♦

♦ [github.com/mmabey](https://github.com/mmabey) ♦ [bitbucket.org/mmabey](https://bitbucket.org/mmabey) ♦



LinkedIn

## EDUCATION

### Ph.D. Computer Science — Information Assurance

Dec 2017

Arizona State University

Tempe, AZ

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

*Dissertation:* Forensic Methods and Tools for Web Environments

### 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 ♦

### B.S. Computer Science — Information Systems

May 2009

Utah State University

Logan, UT

## EXPERIENCE

### Computer Scientist (Civilian)

Dec 2017 – Present

US Army, NETCOM, Data Science Directorate

Phoenix, AZ

*Grade:* GS-0854-11 Step 1

*Service:* Competitive

*Tenure:* Conditional, Full-Time

- Interfaced with ASU faculty to collaborate on data analytic capabilities for monitoring the DoD Information Network (DoDIN) and conducting defensive cyber operations (DCO).

### Research Assistant

Nov 2009 – Dec 2017

Security Engineering for Future Computing (SEFCOM) Lab ♦, ASU

Tempe, AZ

*Lab Directors:* Gail-Joon Ahn, Adam Doupé, Ziming Zhao, Yan Shoshitaishvili

*Sponsors:* Department of Energy, National Science Foundation

- 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.
- 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**.
- 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.

### 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-0199-09 Step 1

*Service:* Excepted

*Tenure:* Permanent, Full-Time

- Summer internships in connection with DoD IASP scholarship.

## Graduate Student Summer Intern

Sandia National Laboratories

May 2011 – Jul 2011

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

Electrical & Computer Engineering Department, USU

Jul 2006 – Aug 2009




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**.

## PUBLICATIONS (SELECTED)

- [1] **Mike Mabey**, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. "Challenges, Opportunities, and a Framework for Web Environment Forensics". In: *Advances in Digital Forensics XIV: 14th IFIP WG 11.9 International Conference, New Delhi, January 3-5, 2018, Revised Selected Papers*. (In press). 2018.
- [2] Erik Trickle, 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.
- [3] **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.
- [4] 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.
- [5] **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.

## TECHNICAL STRENGTHS & QUALIFICATIONS

<b>Research Interests</b>	Digital Forensics, Cyber Security
<b>Programming Languages</b>	Python, Bash, C/C++, HTML, CSS, $\text{\LaTeX}$
<b>Forensic Tools</b>	FTK, Sleuth Kit & Autopsy, dd, HxD, etc.
<b>Protocols &amp; APIs</b>	JSON, XML, AMQP, REST, STIX, RabbitMQ
<b>Network Administration/Security</b>	Ansible, OpenVPN, ufw, lighttpd, Caddy, Wireshark
<b>Operating Systems</b>	 Windows,  Linux,  Chrome OS
<b>Cloud Architectures</b>	OpenStack, Amazon EC2
<b>Databases</b>	MySQL, SQLite

## AWARDS AND ACTIVITIES

- DoD Information Assurance Scholarship Program (IASP) Recipient (5 years) 2012 – 2017
- Team Leader — ASU team in the UCSB International CTF 2009, 2010, 2014, 2015
- Inducted into Eta Kappa Nu (HKN) Engineering Honors Society Nov 2010
- Eagle Scout, Boy Scouts of America 2002