

David Eargle

Information Systems Management Researcher

dave@daveeargle.com |  deargle (<https://github.com/deargle>) |  <https://daveeargle.com>

Updated 2021/09/25

Currently

I am an Assistant Professor in the Organizational Leadership and Information Analytics group at the Leeds School of Business, University of Colorado Boulder

2017-present

I also have a courtesy appointment as Assistant Professor in the Department of Information Science at the University of Colorado Boulder

2017-present

Research Interests

- Human side of Information Systems Security (Behavioral InfoSec)
- Dark Side of Information Technology, including online group polarization
- Neuroscience applications to Human-Computer Interaction and Information Security
- Machine learning and visualization approaches to performing literature reviews

Teaching Interests

- Cybersecurity management
- Descriptive, Predictive, and Prescriptive Business Analytics
- Programming for business majors (Python, R); Databases; Cloud Computing, Web and app development

Education

Ph.D., Information Systems and Technology Management

2017

Katz Graduate School of Business, University of Pittsburgh, Pittsburgh, Pennsylvania, USA.

Dissertation: "Security Messages: Or, How I Learned to Stop Disregarding and Heed the Warning" (pdf)

(<https://daveeargle.com/assets/papers/dissertation.pdf>)

- Two papers exploring whether integrating human facial expressions of fear and threat into security messages can help invoke attention and more secure behavior. A third paper exploring the degree to which various magnitudes of monetary cost impact work/study performance-security tradeoff behaviors.
- Used online lab study methods (amazon mturk) and fMRI; used deception protocols.

Master of Information Systems Management

2013

Bachelor of Science, Information Systems

Marriott School of Management, Brigham Young University, Provo, Utah, USA.

Magna Cum Laude with University Honors

Other Work Experience

Academic Research Assistant

2011-13

Department of Information Systems at Brigham Young University

- Duties included literature reviews, online lab experiment app development and server administration

Digital Forensics Analyst Intern

2012

Paraben Corporation, Ashburn, VA

- Consulted with police chiefs to create tools to log officer access to mobile forensic terminals
- Created a powershell tool to improve quality control for production of Paraben Data Recovery USB sticks
- Completed level 2 mobile forensics training

Network and Systems Administrator

2011-12

Better Logic LLC, Orem, UT

- Set up a VMWare vSphere ESXi server and migrated several bare-metal systems to be virtualized on it.
- Configured Bacula on the hypervisor



Web Developer

2010-12

Center for Teaching and Learning, BYU

- Core developer for syllabus section of Learning Suite, BYU's Learning Management System

Scholarship metrics

-  My Google scholar profile (<https://scholar.google.com/citations?user=Nw7ibigAAAAJ&hl=en>)
-  ORCID (<https://orcid.org/0000-0002-4056-8114>)
- 728 citations per Google Scholar (641 citations since 2016)
- 10 H-index per Google Scholar

Journal Publications

- Vance, A., **Eargle, D.**, Eggett, D., Straub, D., Ouimet, K. "Do Security Fear Appeals Work When They Interrupt Tasks? A Multi-Method Examination of Password Strength," *MIS Quarterly*, forthcoming. Forthcoming
- Kirwan, C., Bjornn, D., Anderson, B., Vance, A., **Eargle, D.**, Jenkins, J. 2020. "Repetition of Computer Security Warnings Results in Differential Repetition Suppression Effects as Revealed With Functional MRI," *Frontiers in Psychology*, 11, pp. 1-10. 2020
- Veen, Hendrik van, Nathaniel Saul, **David Eargle**, and Sam Mangham. "Kepler Mapper: A Flexible Python Implementation of the Mapper Algorithm." *Journal of Open Source Software* 4, no. 42 (2019): 1315. 2019
- Anderson, B.B., Vance, A., Kirwan, C.B., Jenkins, J. and **Eargle, D.** "From warnings to wallpaper: Why the brain habituates to security warnings and what can be done about it." *Journal of Management Information Systems*, 33, 3 (2016), 713-743. doi: 10.1080/07421222.2016.1243947 2016
- Anderson, B.B., Jenkins, J., Vance, A., Kirwan, C.B. and **Eargle, D.** "Your memory is working against you: How eye tracking and memory explain habituation to security warnings." *Decision Support Systems*, 92 (2016), 3-13. doi: 10.1016/j.dss.2016.09.010 2016
- Jenkins, J., Anderson, B., Vance, A., Kirwan, B. and **Eargle, D.** "More harm than good? How security messages that interrupt make us vulnerable." *Information Systems Research*, 27, 4 (2016), 880-896. **Awarded ISR's "Best Published Paper" for 2016.** doi: 10.1287/isre.2016.0644 2016

Conference
Publications

- Anderson, B., Vance, A., Kirwan, B., **Eargle, D.** and Jenkins, J. "How users perceive and respond to security messages: A NeuroIS research agenda and empirical study." *European Journal of Information Systems*, 25, 4 (2016), 364-390. doi: 10.1057/ejis.2015.21 2016
- Anderson, B., Kirwan, B., **Eargle, D.**, Jensen, S. and Vance, A. "Neural correlates of gender differences and color in distinguishing security warnings and legitimate websites: A neurosecurity study." *Journal of Cybersecurity*, 1, 1 (2015), 109-120. doi: 10.1093/cybsec/tyv005 2015
- Vance, A., Anderson, B.B., Kirwan, C.B. and **Eargle, D.** "Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG)." *Journal of the Association for Information Systems*, 15, 10 (2014), 679-722. 2014
- Larsen KR, Gefen D, Petter S, **Eargle D.** (2020) "Creating Construct Distance Maps with Machine Learning: Stargazing Trust." In *Conference of the Association for Information Systems (AMCIS 2020)*. Online. Awarded AMCIS' "**Best Completed Paper**" for **2020**. 60% acceptance rate. 2020
- A Vance, **D Eargle**, JL Jenkins, CB Kirwan, BB Anderson. (2019) "The Fog of Warnings: How Non-Essential Notifications Blur with Security Warnings." In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, 2019. <https://www.usenix.org/conference/soups2019/presentation/vance> 2019
- Kirwan, C.B., Anderson, B., **Eargle, D.**, Jenkins, J., and Vance, A. (2019, October). Attentional habituation to non-essential computer notifications generalizes to security warnings: an fMRI study. Program No. 665.##. *Neuroscience 2019 Abstracts*. Washington, DC: Society for Neuroscience, 2019. Online. 2019
- Anderson, B., Kirwan, B., **Eargle, D.**, Jenkins, J., Vance, A., "Neural Evidence of Generalization of Software Notifications to Security Warnings," *Security and Human Behavior Workshop*, Harvard University, June 2019 2019
- Kirwan, C.B., Anderson, B., **Eargle, D.**, Jenkins, J., and Vance, A. (2019, June). Using fMRI to Measure Stimulus Generalization of Software Notification to Security Warnings. Retreat on NeuroIS, Vienna, Austria. *Information Systems and Neuroscience*, 93-99. 2019
- Eargle, D.**, Galletta, D., Shadi, J., Dimitar, K., and Shivendu, S. "The Chaos of Order: Sequence and Mindlessness Effects in Obtaining Successive App Permissions." In *Workshop on Information Security & Privacy*. Seoul, South Korea: AIS SIGSEC and IFIP TC11.1. (2017). 2017
- Eargle, D.**, Galletta, D. and Jenkins, J. "How much is your security worth? Applying a risk tradeoff paradigm to explain the bimodal nature of user elaboration over interruptive security messages." In *Workshop on Information Security & Privacy*, Dublin, Ireland: AIS SIGSEC and IFIP TC11.1 (2016). 2016
- Eargle, D.**, Galletta, D. and Cranor, L. "On the use of motivational components as attention hooks in security message interface design: Avoiding "tl;dr"." In *Dewald Roode Workshop on Information Systems Security Research*, Albuquerque, New Mexico: IFIP WG8.11/WG11.13 (2016). 2016

- Eargle, D.**, Galletta, D., Kirwan, C. B., Vance, A., and Jenkins, J. 2016. "Integrating Facial Cues of Threat into Security Warnings – an fMRI and Field Study." Paper presented at the Americas Conference on Information Systems (AMCIS), San Diego, California. 2016
- Galletta, D., **Eargle, D.**, Shadi, J., Kunev, D. and Singh, S. "Integrating social and economic models of responding to privacy messages in mobile computing: A research agenda." In *Workshop on Information Security & Privacy*, Fort Worth, Texas: AIS SIGSEC and IFIP TC11.1 (2015). 2015
- Eargle, D.**, Godfrey, J., Miao, H., Stevenson, S., Shay, R., Ur, B. and Cranor, L. "Poster: You can do better – motivational statements in password-meter feedback." In *Symposium on Usable Privacy and Security (SOUPS '15)*, Ottawa, CA: (2015). 2015
- Eargle, D.**, Galletta, D., Kirwan, C.B. and Vance, A. "Integrating facial threat signals into security messages: An extension of media naturalness theory to an information security context." In *Dewald Roode Workshop on Information Systems Security Research*, Newark, Delaware: IFIP WG8.11/WG11.13 (2015). 2015
- Anderson, B., Kirwan, B., Jenkins, J., **Eargle, D.**, Howard, S. and Vance, A. "How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study." In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, Seoul, South Korea: ACM (2015). 2015
- Eargle, D.**, Taylor, R., Sawyer, L. and Gaskin, J. "Acquiring IS skill through habitual use." In *2014 47th Hawaii International Conference on System Sciences (HICSS)*: (2014), pp. 3-12. 2014
- Eargle, D.**, Galletta, D. and Siegle, G. "Using fearful facial facial expressions to increase the effectiveness of protective security messages: Proposing an fMRI and field study." In *The Dewald Roode Workshop on Information Systems Security Research*, IFIP WG8.11/WG11.13, Newcastle, UK: (2014). 2014
- Anderson, B., Vance, A., Kirwan, B., **Eargle, D.** and Howard, S. "Why users habituate to security warnings: Insights from fMRI." In *The Dewald Roode Workshop on Information Systems Security Research*, IFIP WG8.11/WG11.13, Newcastle, UK: (2014). 2014
- Anderson, B., Vance, A., Kirwan, B., **Eargle, D.** and Howard, S. "Users aren't (necessarily) lazy: Using NeuroIS to explain habituation to security warnings." In *International Conference on Information Systems*, Auckland, New Zealand: AIS (2014). 2014
- Vance, A., **Eargle, D.**, Ouimet, K. and Straub, D. "Enhancing password security through interactive fear appeals: A web-based field experiment." In *2013 46th Hawaii International Conference on System Sciences (HICSS)*: (2013), pp. 2988-2997. 2013
- Vance, A., Anderson, B., Brock, K. and **Eargle, D.** "Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG)." In *JAIS workshop*, Gmunden Retreat on NeuroIS, Gmunden, Austria: (2013). 2013
- Eargle, D.**, Vance, A.O. and Lowry, P.B. "How moral intensity and impulsivity moderate the influence of accountability on access policy violations in information systems." In *Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy*: (2013). 2013
- Anderson, B., Vance, A., **Eargle, D.** and Kirwan, C.B. "Your memory is working against you: How eye tracking and memory explain susceptibility to phishing." In *The Dewald Roode Workshop on* 2013

- Information Systems Security Research, IFIP WG8.11/WG11.13: (2013).
- Anderson, B., Vance, A. and **Eargle, D.** "Is your susceptibility to phishing dependent on your memory?" In Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy, Milan, Italy: (2013). 2013
- Vance, A., **Eargle, D.**, Ouimet, K. and Straub, D. "How interactivity can enhance the effectiveness of fear appeals: A web-based field experiment of password security." In The Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.13, Provo, UT: (2012). 2012
- Eargle, D.**, Vance, A., Allen, G., Barrick, D., Bearnson, T. and Tialin, T. "Justifying breaking the glass: How accountability can deter unauthorized access." In WISP 2012 Proceedings, Orlando, Florida: AIS SIGSEC and IFIP TC11.1 (2012). 2012
- Anderson, B., Vance, A., Hansen, J., Kirwan, B., **Eargle, D.**, Hinkle, L. and Weagel, A. "Neural correlates of gender differences in distinguishing malware warnings and legitimate websites: A NeuroIS study." In IFIP WG8.11/WG11.13, Provo, UT: (2012). 2012

Works in progress

See <https://daveeargle.com/projects> for links to resources for these works in progress.

1. **A Spoonful of Sugar: Blending Online News Source and Content to Counter Ideological-Alignment News Biases and Encourage Political Group Depolarization**
 With: Valerie Bartelt, Zlatana Nenova, Dennis Galletta
 Anecdotes suggest that political group polarization may impact readers' perceptions of news articles so strongly that readers may call articles "fake news" solely based on their ideological alignment with the publication source, regardless of the article's content. While researchers have explored confirmation bias in social media, studies have not yet teased out the differential effects of reader ideological alignment with article content ("content-friendliness") and source ("source-friendliness") on attitudes, beliefs, and intended behaviors. Using a mixed design, 133 MTurk participants read and reacted to polarizing news articles, with article-content being presented as if from random sources.

2. **The Fog of Warnings: How Non-essential Notifications Blur with Security Warnings**
 With: Anthony Vance, Bonnie Anderson, Brock Kirwan, Jeff Jenkins
 Through a series of lab and field experiments, the impact of exposure to system notifications of varying degree of visual similarity to security messages is assessed using objective methods such as reaction times and fMRI response data.
 Targeting MISQ Submission October 2021
Conference version
 A Vance, D Eargle, JL Jenkins, CB Kirwan, BB Anderson.
 (2019) "The Fog of Warnings: How Non-Essential Notifications Blur with Security Warnings." In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). Santa Clara, CA:

USENIX Association, 2019.
<https://www.usenix.org/conference/soups2019/presentation/vance>

3. **How much is your security worth? Applying a risk tradeoff paradigm to explain the bimodal nature of user elaboration over interruptive security messages**

With: Dennis Galletta

Why do employees disregard computer security messages, opening the organization to potential information security breaches? One research perspective assumes that humans who fall prey to such attacks solely use automatic information processing, and therefore, user interfaces (such as Google Chrome browser security popups and overlays or Microsoft Word security dialogs) must be better designed to capture and hold attention, and to educate users, to the end that users more carefully consciously evaluate their information security decisions. However, this research project takes the view that employees also make monetary cost-benefit approaches to adhering to or disregarding security messages. It gathers data using a series of online deception-protocol website experiments, wherein users are exposed to security messages that interrupt an ostensible primary task. Psychometric measures of attention, including mouse-cursor tracking and reaction times, are captured and used to predict security behaviors. The monetary "cost" of disregarding a security message is experimentally varied, and its impact on prompting attention and security behaviors is examined. Survey data and focus group data is also captured to probe users' thought processes.

Targeting MISQ submission in first quarter 2022

4. **Creating Construct Distance Maps with Machine Learning: Stargazing Trust**

With: Kai Larsen, David Gefen, Stacie Petter

A design-science approach to creating a tool to graph the nomological space of all survey items used in information systems literature. Applies methods from the domain of topological data analysis to visually graph the nomological space, based on predicted "distances" between item pairs generated by a machine learning predictive model trained on a sampling of survey item-pair relationships (distances) coded by domain experts. Besides leading to insights into already-used IS constructs, the resulting tool can be used to identify placement of new survey items in context in the nomological space.

Ongoing research.

AMCIS Citation

Larsen KR, Gefen D, Petter S, Eargle D. (2020) "Creating Construct Distance Maps with Machine Learning: Stargazing Trust." In Conference of the Association for Information Systems (AMCIS 2020). Online. Awarded AMCIS' "Best Completed Paper" for 2020. 60% acceptance rate.

5. **When Bots Attack: Threat Modeling and Mitigations of Attacks Against Online Behavioral Experiments**

With: Todd M. Gureckis, Jordan W. Suchow

Psychology and behavioral data is increasingly shifting to being collected online, instead of in brick-and-mortar lab rooms. However, panic has arisen about the degree to which such data is impacted by “bots”, or by malicious actors gaming the system in order to maximize participation payouts. This paper applies models from cybersecurity – specifically, the NIST Cybersecurity Framework’s Five Functions – to systematically evaluate the threat of bots, and to show the process by which controls can be developed to mitigate identified threats. Several cross-industry controls are suggested, including the development of machine learning models to detect anomalous participant behavior, aggregated across participating researchers’ data. The behavioral research community can use these models to defend collected data, and to argue for cross-industry grants to develop novel approaches.

Ongoing research

Teaching Experience

Leeds School of
Business, University of
Colorado

In four years:

- Taught 4 unique courses
- Taught at 3000, 4000 (including honors students), and 5000 (graduate, including MBAs) levels

Courses:

Information Security Management (graduate)

- Taught within the Masters of Business Analytics—Security track.
- Compared to the undergraduate offering, this course’s lectures have a stronger focus on specific security behaviors that generate data amenable to machine learning – e.g., post mortem reports from Mandiant and the House Oversight Committee (Equifax, OPM)

Information Security Management (undergraduate)

- Exploration of human, organizational, and technical domains of information security management.
- Self-created hands-on Google Cloud virtual machine labs to teach students to “think like attackers”

Security Analytics

- A projects-based class focused on applying machine learning to security-related data. Topics include malware classification (binomial and multinomial), modeling using mobile sensor data, network traffic parsing (PCAPS => netflows) and malicious IP, domain classification
- A focus on using python-sklearn – on reading documentation and source code
- Also a focus on “open data science” – on hosted Jupyter notebooks, on using Git and Github to store and share code projects. Also on sharing and programmatically consuming shared data.
- Labs have students host models behind API endpoints (Flask app). Models are also deployed to AWS and GCP’s machine learning platforms.

2017-Present

Business Analytics

- Descriptive: querying, and ETL/wrangling data with Alteryx
- Predictive: supervised vs unsupervised machine learning algorithms
- Used Alteryx and DataRobot AutoML
- Covering topics such as association rules, k-means clusters, regressions, correlations, and text mining

Course Evaluation Metrics:

The table below shows course evaluation metrics for each semester-course I have taught at CU Boulder. The "Course Overall" and "Instructor Overall" columns also include college averages parenthetically, when available.

AY Year	Term	Course	Level	Enrolled	Course Overall (college avg.)	Instructor Overall (college avg.)
2017-18	Fall	Infosec Management	ugrad	19	5.5/6.0 (4.6)	5.8/6.0 (5.1)
	Spring	Business Analytics	ugrad	41	3.8/6.0 (4.7)	4.2/6.0 (4.2)
2018-19	Fall	Infosec Management	ugrad & grad (incl. MBAs)	45	4.6/6.0 (4.5)	4.6/6.0 (5.0)
		Business Analytics	ugrad	45	3.6/6.0 (4.5)	4.0/6.0 (5.0)
2019-20	Fall	Infosec Management	ugrad	39	5.2/6.0 (4.5)	5.4/6.0 (5.0)
		Infosec Management	grad (incl. MBAs)	10	5.8/6.0 (4.5)	5.7/6.0 (5.0)
	Spring	Security Analytics with Python	grad (incl. MBAs)	6	4.9/5.0 ^{1,2}	4.9/5.0 ^{1,2}
2020-21	Fall	Infosec Management	ugrad (honors)	33	4.4/5.0 (4.3) ¹	4.4/5.0 (4.3) ¹
		Infosec Management	grad (incl. MBAs)	13	4.7/5.0 (4.3) ¹	4.7/5.0 (4.3) ¹
	Spring	Security Analytics with Python	grad	14	4.7/5.0 (4.4) ¹	4.7/5.0 (4.4) ¹

¹ Average of all available metrics. Typical course and instructor overall evaluation metrics not collected by CU during these semesters because of Covid.

² Due to the mid-semester move to remote learning, college FCQ results for spring 2020 are not available.

- Taught relational database structures and data querying in MySQL and R to Juniors and Seniors from various departments

Introduction to Information Systems Management

2015

- Full responsibility for a class of 60 undergraduate students from various departments of the University of Pittsburgh's College of Business Administration.
- Complete direction over course curriculum, policies, and syllabus.

Microsoft Excel workshops for Katz Graduate students

2013-2015

- Taught four beginner-to-advanced-level Microsoft Excel workshops to part-time Katz MBA students

Department of
Information Systems,
Marriott School of
Management, Brigham
Young University

Spreadsheets for Business Majors

2013

Full responsibility for four college-level class sections on computer spreadsheet skills, with total enrollment of over 270 across four sections. Mix of online plus in-class teaching. Oversight of three teaching assistants.

External Service

JMIS Website Editor

2014 to Present

Web administrator for the Journal of Management Information Systems' web presence (<https://jmis-web.org>), working directly with Editor in Chief Vladimir Zwass.

AIS IS Theory Wiki Editor

Fall 2011 to Present

Systems administrator and managing editor for the Information Systems Theory Community Wiki, <https://is.theorizeit.org>, affiliated with the Association for Information Systems.

psiTurk Project Leader

June 2016 to present

Lead developer for an open platform for science on Amazon Mechanical Turk, hosted on github. Used by researchers around the world.

Ad Hoc Reviewer

ISR, MISQ, EJIS, ECIS, ICIS, HICSS, CAIS, WISP, and The Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.13.

University Service

Director of Security Analytics track within the Masters of Business Analytics degree at Leeds – University of Colorado Boulder

Fall 2017 to Present

- Developed a proposal for a track with a pioneering collaboration between the school of business and school of engineering at CU Boulder
- Supervise graduate students who enrolled in the track across their three semesters in the program.
- Point-person from Leeds meeting with directors of the interdisciplinary telecom program from the school of engineering.

- Ambassador for the track; In charge of reach-out to and bonding with industry partners, including Webroot, IBM, and CrowdStrike.

Honors and Awards

Fellowships

- NSF Graduate Research Fellow (DGE-1247842) - \$132,000
- GAR Foundation Fellow - \$24,000

Grants

- David Berg Center for Ethics and Leadership at the University of Pittsburgh -\$8,420
- Brigham Young University Marriott School of Business - \$1,000
- Rollins Center for Entrepreneurship & Technology (2013) - \$4,000

Scholarships

- Brigham Young University Undergraduate Scholarship - \$8,278
- BYU Masters of Information Systems Management Scholarship - \$4,380
- Robert K. Thomas BYU Honors Department Scholarship - \$1,488
- Khona Family BYU Honors Department Scholarship - \$1,488
- Ella M. Herman Scholarship - \$1,054

Competitions

- AIS Global Competition 2012, Windows Phone Development Track, 2nd Place Worldwide

Areas of Expertise

- Statistics
- Machine learning
- Predictive Analytics, Business Intelligence
- Data visualization
- Databases
- Cloud Computing
- DevOps
- Server Administration
- Web development

Technical Skills

- R (tidyverse, dplyr, ggplot2), SAS, SPSS, python (pandas)
- MySQL / postgresql, MS Access, S3/Glue/Athena, MongoDB
- Python (scikit-learn, scipy, numpy), Tensorflow (a little), R (keras), RapidMiner, Alteryx
- vagrant, packer, terraform, git, chef, ansible, pytest
- AWS (EC2, Glue, Athena, S3, IAM, SageMaker)
- GCP (Compute, Cloud Storage, and whatever they call their AutoML offering now)
- html/css/less/sass/scss, bootstrap (tbs), bower, npm & grunt, pip, Jekyll,
- javascript/jquery
- Bash
- Vim
- Python
- Docker

- Powershell
- Java
- php (slim, CakePHP, propel)
- markdown, twig/Jinja2
- Nginx, apache, gunicorn
- Linux (Debian preferred), Windows server (active directory and group policies)
- VBA for Excel

Area-of-expertise Narratives

The below narratives illustrate how I have used the above technologies within the stated areas of expertise.

Check out my github activity for more! Not all of my activity is "open," though – current research projects are typically marked as "private"

Habituation and Generalization Studies

This example describes what I call Full "Academic Stack" Development that I have done for one of the research projects in my cybersecurity stream. It includes the creation of web-based field experiments, data collection, analysis, and hypothesis testing.

- I used `npm` and `yarn` for javascript package management, and `git` / `github` for source code control.
- Each "modal" (popup) in this study shares common code, so I used `webpack` to let me write javascript classes with inheritance. `webpack` and `grunt` scripts also build and bundle the source javascript and `scss` files that are used by the modals.
- The front-end uses `jquery` / `d3` / `underscore` for interactivity.
- The web task dynamically loads page elements in order to keep responsivity high. I used python `Flask` for serving the task and for running a json api that the client-side javascript calls.
- User data is stored in a `mysql/postgres` database (depending on the server host). The database is built automatically and interfaced with by python code using `sqlalchemy`.
- The task integrates a Qualtrics survey. Data is passed to the survey via web url parameters, so each participant's identifier gets recorded into the Qualtrics data for matching later.
- The task is deployed to Heroku, Salesforce's platform-as-a-service solution. This runs containerized applications on AWS hardware.
- I wrote "campaign" functionality to automate staggered posting of tasks to AWS Mechanical Turk, using the python `boto3` library integrated with the `psiturk` library.
- At analysis time, I queried data using `sqlalchemy`. After parsing json datastrings, I use `pandas` DataFrames to merge together task behavior, mouse-tracking data, and survey data tables. I save these to csv files.
- I did statistical analysis primarily in R, using the `tidyverse` collection of packages (`dplyr`, `ggplot2`, etc.). I created models using `glm` and `lm`, and I specified follow-up contrasts using `emmeans`. I used `knitr` to render a report from an r-markdown file.

Studies on
confirmation bias for
readers of online news

This example demonstrates consuming cloud-computing services – specifically, stringing together several AWS cloud computing services in order to capture mouse-tracking data for a web-based field experiment.

- I manually downloaded snapshots of dozens of news articles from various online publication sources. Then I wrote python classes for each publication source to scrape the articles' content, headlines, and header image. This data was stored in a `mongodb`.
- I created an api that could display article content as if from any source, using `Flask` templates.
- I collected mouse-tracking data while participants read news articles, and posted it to `AWS firehose` via an `AWS api gateway`. Firehose stored data in `s3`. This was crawled with `AWS glue`, to create query-able `AWS Athena` tables.
- I used Python scripts to query the Athena tables, and to group the mouse-tracking data by article-interaction, based on timestamps recorded in task-tracking data. I used `R` scripts to automate statistical analysis, using `lme4` for linear mixed models, since the data was of repeated-measures nature.

Topological Data
Analysis for a
Nomological Network
of IS Survey Items

This example demonstrates some of my experience with using machine learning packages for research.

- I computed semantic space embeddings for IS survey items, using embedding libraries such as `word2vec` and `GloVe`.
- I used `sklearn` to feed the data through various modeling algorithms. I also fit models using DataRobot's AutoML platform.
- I wrote a script to use python to interact with a Java trained ML model downloaded from DataRobot
- Then, I used `numpy` and `scipy` to pull together model predictions from DataRobot
- I applied various dimensionality reduction techniques (projections) to get from 11-thousand down to 3- or 2- dimensions, using various `sklearn` manifolds, including `IsolationForest`, `t-SNE`, `l2-norm`, and `PCA`.
- I used `scipy.sparse.csgraph.shortest_path` to calculate shortest walking distances between all item-pairs from the graph, which I prepared using `scipy.spatial.distance.pdist`.
- I used the `Mapper` algorithm (via python `KeplerMapper` library) to divide the projection into a grid of hyperspheres. Then I used agglomerative clustering (via `sklearn.cluster.AgglomerativeClustering`) on each cluster to obtain nodes. I linked overlapping nodes, creating a "graph."
- I became a core developer of the scikit-tda python `KeplerMapper` library.

- I used KeplerMapper to visualize the graph using javascript d3-force graph.

InfoSec DevOps

This example demonstrates some of my self-taught efforts with cloud-based DevOps. It involved moving virtual machines from usb-based "golden image" virtualbox ISOs to full code-as-infrastructure DevOps.

- I used `packer` to automate the preparation of a raw image of Debian-based Kali OS to be able to run on Google Cloud (GCP – it's cheaper for students than AWS).
- I used `virt-manager` on a gcp-launched kali image (that's nested virtualization!) so students can launch several "penetration testing lab" virtual machines for class assignments.
- I used `vagrant` and `chef` to provision the virtual machine images. The use of Vagrant means that I can update the vagrant build script and have students download and rerun the script to get fixed VM images mid-semester, if needed. I used chef because that is what metasploitable3 uses, and I wanted to be able to contribute back to metasploitable3.
- I used `terraform` to launch a separate subnet, vpn server, and vulnerable midterm assessment server for each student team. The vulnerable servers are only accessible via a connection to the given vpn server, *except* that ssh is open to the world so that I can ssh in and fix images if needed, via `ansible`.

Professional Affiliations

- IFIP Working Group 8.11/11.13, "Information Systems Security Research" Active Member
- Association for Information Systems Member

Foreign Language

- Spanish

Links

- 🌐 <https://daveeargle.com>
- ✉ dave@daveeargle.com
- 👤 [deargle \(https://github.com/deargle\)](https://github.com/deargle)
- 📖 StackOverflow (<https://stackoverflow.com/users/1396649/deargle>)
- 📄 Google scholar (<https://scholar.google.com/citations?user=Nw7ibigAAAAJ&hl=en>)
- 🆔 ORCID (<https://orcid.org/0000-0002-4056-8114>)