

# Eva Sarafianou

<https://github.com/esarafianou> | Seattle, WA | [eva.sarafianou@gmail.com](mailto:eva.sarafianou@gmail.com)

Security and Software Engineer interested in Application Security

---

## Experience

### Auth0 / Application Security Engineer

AUGUST 2018 - PRESENT, SEATTLE

- Secure Development Lifecycle - Risk Assessments, Threat Modelling
- Security guidance to Engineering teams
- Security Reviews and Testing
- Security in CI/CD
- Development of security tools and libraries
- Vulnerability Management
- Responsible Disclosure Program

### CENSUS S.A. ([website](#)) / Security Consultant

NOVEMBER 2016 - APRIL 2018, ATHENS/SEATTLE

*Worked with: Chinese Mobile Vendor, Greek Private Banks, e-Healthcare Software Providers, Banking Software Providers, Insurance Providers, Software Providers*

- Web Application Security Testing
- iOS Application Security Testing
- Android Application Security Testing
- Source Code Auditing
- Internal Infrastructure Penetration Testing
- Staff Security Awareness Training
- Secure SDLC Consulting and Documentation: Design Level Reviews, Security Architecture, Threat Modeling, Data Classification, Disposal Plan
- Secure Mobile Payment Applications
- Implementation of security patches (in NodeJS)

### Freelance / Linux system administrator

NOVEMBER 2016 - PRESENT, ATHENS

- Maintaining 10 hosted sites
- Working with nginx, Ghost, MySQL, Let's Encrypt
- Performed server migration with zero downtime using DNS load balancing
- Secured SSH access and distributed GPG signed key fingerprints to users

### Crypto.Sec Lab, University of Athens / Security Researcher

MARCH 2016 - JANUARY 2017, ATHENS

**Rupture**, a compression side-channel attack framework ([website](#))

- Developed RESTful API using **Django** ([design documents](#))
- Developed WebSocket command & control server using **NodeJS**
- Developed Web UI using **React.js** and **Bootstrap** in **ES6**
- Integrated **BetterCap** to facilitate MitM
- Followed **TDD** using **Jasmine**

**CTX**, a cryptographic library that defends against side-channel attacks ([website](#))

- Developed integrations for Django, Flask, Express.js, Koa
- Developed client library, published in Bower ([link](#))

### National Technical University of Athens / Teaching Assistant

FALL 2016, ATHENS

Reviewed crypto assignments and helped undergraduate students with course material.

---

## Conference Talks

### Productizing TLS Attacks: The Rupture API / Real World Cryptography Conference

JANUARY 2017, NEW YORK

Presented the latest improvements on our tool for conducting cryptographic compression side channel attacks. ([video](#)) ([paper](#))

### CTX: Eliminating BREACH with Context Hiding / Black Hat Europe

NOVEMBER 2016, LONDON

Talked about novel mitigations for compression side-channel attacks. ([link](#))

### Rupture: Automating cryptanalysis of HTTPS for AES ciphers / BSides Athens

JUNE 2016, ATHENS

Talked about automating cryptanalysis and in particular how AES, being a block cipher, can complicate measurements of ciphertext lengths. ([video](#))

### The MitM framework BetterCap / FOSSCOMM

APRIL 2016, ATHENS

Presented BetterCap, a MitM framework aiming to be a better alternative to Ettercap.

---

## Education

### National Technical University of Athens / Master of Engineering

SEPTEMBER 2011 - FEBRUARY 2017, ATHENS

Electrical and Computer Engineering

---

---

Scored **top 0.1%** in entrance exams.

**Thesis:** Tool implementation for conducting cryptographic compression side channel attacks against the TLS protocol ([link](#), intro in Greek)

---

**Side Projects**    **harmonise.it** ([github](#), [live version](#))  
A platform which helps music theory and harmony students practice harmony rules  
*Node.js, GraphQL, React.JS, Relay, PostgreSQL*

---

**Workshops**    **Mobile Application Security (Android) / Conference on Informatics in Education**  
OCTOBER 2017, ATHENS  
Taught basic Android internals, Android Application Security and common Android related Vulnerabilities. Workshop on a vulnerable Android App ([DIVA](#))

---

**Skills**    **Languages:** Python/Django, JS, NodeJS, GraphQL, Relay, React.JS, Express.JS, bash, HTML5, CSS Bootstrap, C, Java  
**Security/Cryptography:** OWASP, TLS, Cryptography, Web Application Security, Secure SDLC, compression side-channel attacks, BREACH, Linux security, iOS Security, Android Security  
**Tools:** Git/GitHub, Burp, Nmap, sqlmap, GPG, Bettercap, MySQL, Metasploit, qark, needle, frida

---

**Languages**    Fluent English Speaker, Native Greek Speaker

---

**Awards**    [Google Travel Grant](#) to Hack In The Box [Security Conference](#) in Amsterdam 2017