Privacy, Networking & Security Research Intern

Mozilla is hiring Privacy, Networking, & Research Engineering Interns onto our technical teams throughout the world. Our headquarters are based in the Bay Area, but we have positions in our offices in Toronto and Berlin!

We are engineers, designers, makers, and problem solvers. We work in the fishbowl known as the open source community, with a clear focus on making the Web better. Working with us, you'll help build interesting new features, improve Mozilla products, and explore new product directions. To be part of the team, we ask that you be user centered, technically-curious, and excited to be moving the Mozilla mission forward.

As a part of our Mozilla Internship Program, you will:

- Impact challenging projects influenced by our family of Mozilla products in and outside of the Firefox web browser (accessibility, voice design, developer tools, mobile, and mixed reality), Rust, Pocket, and more
- Be mentored by a fellow teammate and someone who shares the same values
- Do real work on real projects and make contributions that will impact hundreds of millions of users
- Participate in social events with your fellow interns (amusement parks, ice cream and boba socials, board game nights, escape rooms, and painting parties)
- Meet with Mozilla leaders including our CEO, Executive Chairwoman, CPO, Chief R&D Officer, CMO, and Executive Foundation Director
- Present your work to Mozilla leaders and fellow team members

Perks include:

- Market competitive pay
- Catered lunches, snacks, and drinks
- Housing service or housing stipend provided
- Flights and ground transportation to and from internship
- Work visas sponsored
- Attendance at our bi-annual All Hands Meeting

Application and Interview Process

- Recruiting begins in September, and we hire on a rolling basis through March. While there is no set application deadline, we do have a limited number of positions open each year, so please apply early!
- Locations include Mountain View, San Francisco, Toronto, Berlin, and Paris.

Please refer to our internship listings for specific locations offered by position.
- Process starts with a resume review followed by a HackerRank challenge (technical) or document submission (non-technical).
- Upon passing, you will partake in two technical and behavioral interviews with team members (coding and situational questions are fair game) followed by a hiring manager interview and ultimately, an offer decision.

We have 8 positions open on the following teams:

Privacy, Networking & Security Intern - Project: Anti-Phishing UI (Toronto, Canada)
Firefox Privacy & Security Engineering team builds and maintains Firefox features and services to protect the security and privacy of Firefox users. We are looking for an intern to help us with our anti-phishing efforts as there is ongoing research within Mozilla. We intend to find better ways to detect phishing sites - this may include something such as detecting and surfacing confusing urls disguised as trusted websites.

Privacy, Networking & Security Intern - Project: Enhance Download Protection (Berlin, Germany)
The Security Engineering team at Mozilla is responsible for Download Protection, which protects users against malicious files that they attempt to download on Firefox. We use C++, JavaScript, Git and numerous advanced programming tools to develop software to achieve our goals. We're looking for an intern to help us with increasing the detection rate of Download Protection and minimizing the risk for Web users.

Privacy, Networking & Security Intern - Project: Improve Necko Test Infrastructure (Berlin, Germany)
The Networking (Necko) team at Mozilla is responsible for ensuring Firefox is able to communicate with web servers across the world using standardized networking protocols (such as HTTP, FTP, etc). For testing our code we use tools such as Javascript, Python, Node.js. We are looking for an intern to help us improve our test infrastructure, working on emulating different network settings (proxy servers, NTLM servers etc.) across our large user base. This will allow us to add more automated tests easily and detect bugs before they are deployed. It will also enable us to move faster without fear of breaking existing deployment.

Privacy, Networking & Security Intern - Project: Improving Performance of Client-Side Personal Data Breach Database Use (San Francisco, CA and Mountain

View, CA)
As we look to increase the ways we can protect a user's personal data, the potential for negatively impacting performance in Firefox increases. Potential solutions for this could be as simple as using cascading bloom filtering on local data stores, or as complex as anonymized, server-based secure verification of data in a set.

The goal is to develop a methodology by which we can scale (or at least assure) performant data checking as we expand our ability to protect the various personal data of end users.

Privacy, Networking & Security Intern - Project: Integrate HTML Sanitizer (XSS-Filter) into Firefox (Mountain View, CA)
According to OWASP, two thirds of all web applications are vulnerable to Code Injection Attacks. Since XSS still accounts for the vast majority of security bugs within web applications, Firefox should provide an API that allows sanitizing HTML strings. Not only could this sanitizer be exposed to web applications but it could also be consumed for sanitizing our own applications. To start, we could use the ruleset of 'DOMPurify', an HTML and JS sanitizer which has been proven to provide strong mitigations against XSS.

Privacy, Networking & Security Intern - Project: Restricting DOM Access to Certain Attributes to Avoid Data Exfiltration (Mountain View, CA)
The current practice of loading third party JavaScript into the same execution context as the top-level document opens the door to data exfiltration, and the current security model (Same-origin-Policy, Content Security Policy, sandboxed iframes, etc.) was not built to prevent such data exfiltration attempts.

In more detail, imagine a top-level document foo.com which loads a script using <script src="bar.com> into the same execution context of foo.com. As a consequence, bar.com gets full access to the DOM and is able to exfiltrate confidential user data. In a simplified attack scenario the attacker would traverse the entire DOM and pick values of interest (credit card numbers, social security numbers, etc). By performing a GET request to an attacker controlled server, the attacker could send the exfiltrated user data as a payload. On the server, the attacker could then re-assembles the harvested information.

Simply blocking such scripts maps to the security/privacy guarantees that tracking protection offers. Within this project we would allow potentially malicious scripts to load,

but observe and evaluate all DOM access. A monitoring system in the DOM-Bindings would allow us to better quantify how often such exfiltration attempts happen in the wild, and hence provide a better understanding as to how to stop such exfiltration attempts.

Security Engineering Intern (San Francisco, CA)
Firefox Operations Security protects the core services and release engineering infrastructures Mozilla relies on to build, ship and run Firefox. The intern would be working on the Fraud Detection pipeline, implementing security controls to catch malicious behavior in our core services.

Basic Qualifications:

- Must be currently enrolled in a Bachelor's, Master's or PhD degree program in Security Engineering, Computer Science, Computer Engineering, or a related technical discipline with a focus on security and privacy
- Must be graduating December 2020 and onward
- Familiarity with networking, web security, and web privacy concepts

Preferred Qualifications:

- C / C++
- Javascript, HTML, and CSS,
- Familiarity with NodeJS ecosystem
- Experience with algorithmic efficiency or cryptanalysis
- Understanding of Secure System Development

About Mozilla
Mozilla exists to build the Internet as a public resource accessible to all because we believe that open and free is better than closed and controlled. Join us and become part of our mission to promote openness, innovation and opportunity online.

Mozilla is committed to Equal Employment Opportunity throughout our recruiting and hiring process and is dedicated to increasing diversity in our workplace.