Henry Birge-Lee

74 Beavers St.
High Bridge, NJ 08829
(213) 453-2724
birgelee@princeton.edu

EDUCATION

Princeton University, Princeton, NJ
AB in Computer Science, May 2021
Summa Cum Laude (highest honors), **Advanced Standing** (three years of study)

North Hollywood High School Highly Gifted Magnet, Los Angeles, CA
High School Diploma, with Honors, June 2015

HONORS, AWARDS, ACHIEVEMENTS

Runner up for the 2021 Computing Research Association Outstanding Undergraduate Researcher Award. Given to four awardees and five runner ups from all colleges and universities in North America for outstanding research.

Awarded the Calvin Dodd MacCracken Senior Thesis Award. Given to three graduates of the Princeton engineering school class of 2021 to recognize the senior thesis or project work that is most distinctive for its inventiveness and technical accomplishment.

Lead Author on "Bamboozling Certificate Authorities with BGP." Runner up for the 2020 Caspar Bowden PET Award for an outstanding contribution to privacy enhancing technologies.

Lead Author on "Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt." Finalist for the CSAW'21 Applied Research Competition for the best security paper with a practical impact.

Presenter of "Using BGP to acquire bogus TLS certificates." Awarded Best Talk at HotPETS '17.

Awarded the Outstanding Computer Science Senior Thesis Prize. Given to twelve graduates of the Princeton Computer Science class of 2021 to recognize outstanding work on a Computer Science senior thesis.

National Champion CyberPatriot National High School Cyber Defense Competition Spring 2014, 2nd Place Spring 2015. Competed as a team of five to secure networks, servers, and workstations against live attackers. Won first place in National Open Division.

WORK EXPERIENCE

Research Software Engineer at Princeton University
(June 2021 - Present)

I play a lead role on a large, collaborative, data-based study with Let's Encrypt (the world's largest public certificate authority) to monitor and instrument Let's Encrypt's deployment of multiple vantage point domain control validation (that is based on a previous USENIX Security paper that I was lead author on) and generate recommendations for expanding the deployment. I also collaborate with researcher's at the University of Virginia and ETH Zurich to create a production-grade deployment of a secure routing backbone that that we recently developed. In addition, I perform work on software-defined networks with a focus on advanced inter-domain routing.

Student Employment as a Research Programmer at Princeton University
(September 2020 - May 2021).

I worked on Princeton's project to secure domain-validated certificates from BGP attacks and collaborated closely with members of the Let's Encrypt engineering and SRE teams to analyze their deployment of multiple vantage point domain control validation. I also worked in collaboration with researchers at Princeton University, ETH Zurich, and University of Virginia to develop and deploy an Inter-domain routing security system that leverages the partial deployment of emerging secure backbone technologies to enhance global Internet security (including the security of non-participating networks).

Full-Time Research Programmer at Princeton University
(June 2017 - September 2020).

I was the lead researcher servicing Princeton's project on securing domain-validated certificates against BGP attacks and conduct network security research. I developed and analyzed state-of-the-art network security defenses and attacks. Some of my responsibilities included launching ethical real-world BGP attacks, developing novel simulations of BGP attacks on TLS domains, analyzing certificate issuance data shared by Let's Encrypt (the world's largest web CA), and working on a secure backbone for the public Internet by leveraging SCION (a next-generation Internet architecture).

Freelance Security Consultant (Aug. 2016 - May 2017). Performed security reviews and developed secure systems for small companies (often e-commerce websites). I specialized in SSL/TLS configuration and deployment.

Open Nuclear Counterforce Simulation (June 2016 – Aug. 2016). Was contracted with an international relations professor to develop a user interface and simulation of a nuclear exchange between the three major nuclear powers. The simulation calculates the probability and extent of a retaliation from a nuclear power after a first strike by another power. The application is programmed in PHP with a MySQL database.

Freelance Website Developer (June 2016 – Aug. 2016). Worked as a full stack developer on an ASP.NET dating website. Worked with Visual Studios 2015 and MS SQL to solve a variety of problems from layout to email notifications.

CONFERENCE COMMITTEE MEMBERSHIP

Member of the Artifact Evaluation Committee for USENIX Security '21. https://www.usenix.org/conference/usenixsecurity21/call-for-artifacts

Member of the Artifact Committee for the Annual Computer Security Applications Conference (ACSAC '19). https://www.acsac.org/2019/committees/artifact/

SKILLS

Networking: BGP Configuration, Internet Topology Analysis, Network Data Collection (i.e., Network Scanning, Traceroute), Linux Packet Manipulation/Processing (i.e., iptables, Scapy), DNS Measurement and Instrumentation, Cisco Router and Switch Configuration (including routing table configuration, NAT including overloading, trunking using 802.1q, Ethernet link aggregation, IP Helper)

Data Processing: Large-Scale Data Analysis, Multi-threaded/Multi-core HPC Application Development/Deployment (i.e., Slurm), Lightweight Data Analysis (SQL data processing, NumPy/Pandas, In-memory data representations)

Programming/Markup Languages: Python, Java, C/C++, C#, SQL, Javascript, HTML/CSS, Ruby, Haskell, PHP, IDL, Racket

Server Administration Experience: SQL, HTTP (Apache, IIS, node.js express), VPN (Open VPN, PPTP, Wireguard), Windows Active Directory, DNS (Microsoft DNS, Bind)

Application Development: Git version control, Test Driven Development, Unit Testing (JUnit)

PUBLICATIONS

Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal. 2018. Bamboozling Certificate Authorities with BGP. In *Proceedings of the 27th USENIX Security Symposium (USENIX Security '18)*. USENIX Association, Baltimore, MD, 833–849. https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee **Runner up for the 2020 Caspar Bowden PET Award.**

Henry Birge-Lee, Liang Wang, Daniel McCarney, Roland Shoemaker, Jennifer Rexford, and Prateek Mittal. 2021. Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt. In *Proceedings of the 30th USENIX Security Symposium (USENIX Security '21)*. USENIX Association, Vancouver, CA. **Finalist in the CSAW'21 Applied Research Competition**

Henry Birge-Lee, Liang Wang, Jennifer Rexford, and Prateek Mittal. 2019. SICO: Surgical Interception Attacks by Manipulating BGP Communities. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. Association for Computing Machinery, New York, NY, USA, 431–448. DOI:https://doi.org/10.1145/3319535.3363197

Yixin Sun, Maria Apostolaki, **Henry Birge-Lee**, Laurent Vanbever, Jennifer Rexford, Mung Chiang, and Prateek Mittal. 2020. Securing Internet Applications from Routing Attacks. Accepted to appear in *Communications of the ACM (CACM)* in 2021.

Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal. 2017. Using BGP to acquire bogus TLS certificates. Talk Abstract in *Hot Topics in Privacy Enhancing Technologies (HotPETS '17)*. Minneapolis, MN. https://www.petsymposium.org/2017/papers/hotpets/bgp-bogus-tls.pdf **Winner of the 2017 HotPETS Best Talk Award**

Walter Gekelman, Patrick Pribyl, **Henry Birge-Lee**, Joe Wise, Cami Katz, Ben Wolman, Bob Baker, Ken Marmie, Vedang Patankar, Gabriel Bridges, Samuel Buckley-Bonanno, Susan Buckley, Andrew Ge, and Sam Thomas. 2016. Drift waves and chaos in a LAPTAG plasma physics experiment. In *American Journal of Physics Volume 84,* 118-126. https://doi.org/10.1119/1.4936460

INVITED TALKS

- Presentation for "Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt" at the 30th USENIX Security Symposium, Virtual, Aug 2021.
- Presentation for "Bamboozling Certificate Authorities with BGP" at the 27th USENIX Security Symposium in Baltimore, MD, Aug 2018.
- Presentation for "SICO: Surgical Interception Attacks by Manipulating BGP Communities" at the 2019 ACM SIGSAC Conference on Computer and Communications Security in London, UK, Nov 2019.
- Presentation for "Using BGP to acquire bogus TLS certificates" at the 2017 Hot Topics in Privacy Enhancing Technologies Symposium (HotPETS '17) in Minneapolis, MN, July 2017. **My presentation was awarded best talk.**
- Presentation on BGP attacks against the PKI at the September meeting of the CA/Browser Form's Validation Working Group (virtual). Sep 2018.

RESEARCH PROJECTS

- **Securing the PKI from BGP Attacks (Princeton University and Let's Encrypt).** The Public Key Infrastructure (PKI) protects users from malicious man-in-the-middle attacks by having trusted Certificate Authorities (CAs) vouch for the domain names of servers on the Internet through digitally signed certificates. Ironically, the mechanism CAs use to issue certificates is itself vulnerable to man-in-the-middle attacks by network-level adversaries. Malicious Autonomous Systems (ASes) can use Border Gateway Protocol (BGP) attacks to hijack a victim's traffic and obtain a certificate for a domain they do not control. In this project I work to secure the PKI from BGP attacks. Our methods are diverse, ranging from running state-of-the-art simulations of BGP attacks to working with engineers at Let's Encrypt, the world's largest CA, on the engineering/evaluation effort involved with deploying countermeasures. **This project has already lead to the improved security of millions of Internet users through the deployment of multiple vantage point domain control validation by Let's Encrypt, which protects domains against BGP attacks:** https://www.princeton.edu/news/2020/02/21/internet-security-borne-out-collaboration-between-princeton-and-lets-encrypt**.** Research Mentors: Prateek Mittal and Jennifer Rexford. Associated Researchers: Yixin Sun, Liang Wang, Daniel McCarney, Roland Shoemaker, and Anne Edmundson. Publications (citations above): "Bamboozling Certificate Authorities with BGP," and "Using BGP to acquire bogus TLS certificates." Also preparing a manuscript for submission to USENIX Security '21.

- **Surgical Interception Attacks Using BGP Communities (SICO) (Princeton University).** The Border Gateway Protocol (BGP) is the primary routing protocol for the Internet backbone, yet it lacks adequate security mechanisms. While simple BGP hijack attacks only involve an adversary hijacking Internet traffic destined to a victim, more complex and challenging interception attacks require that adversaries intercept a victim's traffic and forward it on to the victim. In this project I exposed a powerful new methodology for launching BGP interception attacks that significantly increased the viability and effectiveness of these attacks. Furthermore, my work introduced highly-targeted BGP interception attacks that allowed an adversary to target an interception attacks to both source and destination IP addresses. Research Mentors: Prateek Mittal and

Jennifer Rexford. Associated Researcher: Liang Wang. Publications (citations above): "SICO: Surgical Interception Attacks by Manipulating BGP Communities."

- **Secure Backbone Autonomous System (SBAS) (Princeton University, ETH Zurich, and University of Virginia).** The Border Gateway Protocol (BGP) is highly vulnerable to routing attacks where an adversary announces malicious routes to a victim's destination. The SBAS project aims to secure Internet routing from these attacks by leveraging SCION, a next-generation Internet architecture that is resistant to routing attacks, as a secure backbone that would allow participating networks to be immune to BGP attacks while still using the IP architecture and not having to fully adopt SCION. Research Mentors: Prateek Mittal, Adrian Perrig. Associated Researchers: Yixin Sun, Joel Wanner, Liang Wang, Jonghoon Kwon, Markus Legner