Rahul Chatterjee

Contact Information

Cornell Tech, 2 W Loop Rd, New York,
NY 10044

E-mail: rahul@cs.cornell.edu
Web: `https://www.cs.cornell.edu/~rahul/`

Research Interests

Building human aware secure systems that are usable, human friendly, and provably secure.

Education

Cornell University — Ithaca, NY
PhD, Computer Science — August 2015 - present
Advisor: Thomas Ristenpart

University of Wisconsin, Madison — Madison, WI
Masters, Computer Sciences — August 2013 - May 2015

Indian Institute of Technology, Kharagpur — Kharagpur, West Bengal
Bachelor of Technology, Computer Science and Engineering — July 2008 - June 2012

Work Experience

Two Roads Technological Solutions Pvt. Ltd. — Bangalore, India
Software Developer and Quantitative Analyst — June 2012 - June 2013

Internship Experience

Dropbox, Abuse prevention team — San Francisco, USA
Project: Cluster IPs based on their authentication behavior in order to improve abuse prevention techniques. — Summer 2016

Microsoft Research Technologies — Redmond, USA
Project: Analyzing *Crypto Board* data to infer common problems in security engineering. — Summer 2015

Adobe Systems India Pvt. Ltd. — Noida, India
Project: Generating smart catchy tags for images from the image meta-data. — Summer 2011

Selected Publications

[1] **Rahul Chatterjee**, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, Thomas Ristenpart, "The Spyware Used in Intimate Partner Violence." *39th IEEE Symposium on Security and Privacy 2018 (Oakland)*

[2] **Rahul Chatterjee**, Joanne Woodage, Yual Pnueli, Anusha Chowdhury, Thomas Ristenpart, "The TypTop System: Personalized Typo-tolerant Password Checking." *ACM CCS 2017 (Dallas, Texas)*

[3] Joanne Woodage, **Rahul Chatterjee**, Yevgeniy Dodis, Ari Juels, and Thomas Ristenpart, "A New Distribution-Sensitive Secure Sketch and Popularity-Proportional Hashing." *Crypto 2017 (UCSB, California)*

[4] **Rahul Chatterjee**, Anish Athayle, Devdatta Akhawe, Ari Juels, Thomas Ristenpart, "pASSWORD tYPOS and How to Correct Them Securely." *37th IEEE Symposium on Security and Privacy 2016 (Oakland)* (Awarded **distinguished student paper award**)

[5] Adam Everspaugh, **Rahul Chatterjee**, Samuel Scott, Air Juels, Thomas Ristenpart, "The Pythia PRF Service." *USENIX Security 2015.*

[6] **Rahul Chatterjee**, Joseph Bonneau, Ari Juels, Thomas Ristenpart, "Cracking-Resistant Password Vaults using Natural Language Encoders." *36th IEEE Symposium on Security and Privacy 2015 (Oakland).*

Teaching Experience

- TA for Building Startup Systems — Fall, 2017
- TA for Cryptography, Instructed by Prof. Thomas Ristenpart — Spring, 2016
- TA for Introduction to AI, Instructed by Prof. Bart Selman — Fall, 2015
- TA for Introduction to Cryptography, Instructed by Prof. Somesh Jha — Fall, 2014
- TA for C++ for Java Programmars, Instructed by Jim Skrentny. — Fall, 2013

Research Projects

Technology abuse in domestic violence ([1])
Via a measurement study of Google, and mobile app stores we show that thousands of *dual-use* mobile apps — applications that have legitimate use case (e.g., Find my Phone), but can be easily repurposed to spy on an intimate partner — are available inside and outside official mobile application stores. In intimate partner violence situation, dual-use apps can be and are being used for spying on victims, and this can lead to other forms of harassment and violence. Existing anti-spyware apps don't flag dual-use apps as a threat. Some developer of dual-use apps are promoting IPV use case of their apps. We are now building a dual-use app detection and removal tool based on our measurement pipeline.

Typo-tolerant password checking ([2],[3],[4])
Small typographical errors during entering password, such as typing 'pASSWORD' instead of 'Password', results in login failure. I analyze to what extent typos in passwords affect the usability, and how security will be impacted should we allow some small typos during login. We conducted studies with Dropbox, Inc. and on Amazon Mechanical Turk to conclude that, (a) typos are serious burden on users, (b) allowing small set of carefully chosen typos can improve usability while negligibly impacting security. Later, I build a secure password checking system, called TypTop that will monitor login mistakes of a user, and adapt to allow login with typos that the user makes often and safe to do so.

The Pythia PRF services ([5])
Create a remote PRF service that can be used for password hardening with some added features, such as, the PRF only has access to the blinded version of the password—therefore compromise of the server does not leak the passwords. One can rotate the secret key of the PRF and update the stored hash values of the passwords without access to the plaintext password.

Cracking resistant password vault ([6]) Built a new kind of password vaults (password managers) that prevent offline cracking attack. Traditional password managers are susceptible to offline brute-force guessing attack against the master password used to encrypt the passwords. In NoCrack, we designed a new encryption scheme, such that decryption with a wrong guess will result in a plausible vault, making it hard for the attacker to distinguish between a wrong guess and a correct guess, unless they try the vault passwords online. It uses existing password cracking methodologies in defense of password vaults to create effective decoy password vaults.

Bachelor Thesis

Sentence Fluency Improvement using Monolingual Corpus
Advisor : Prof. Sudeshna Sarkar, CSE, IIT Kharagpur
Built system to improve *fluency* of machine generated texts or second language writer's texts using only monolingual corpus with minimum language dependent information. Using Markov model based sentence prediction technique, I build a system to produce sentences that are semantically close to the given input sentence but has higher fluency. This project was selected one of four best BTech projects in the department.

Academic Achievements Awards and Scholarships

- Distinguished student paper award for [2] at IEEE S&P, 2016.
- Awarded **special CS fellowship** from the department of Computer Sciences, UW - Madison.
- Secured rank **4th** in the North Central region in ACM-ICPC regional contest 2013.
- Received IMPRS-CS fellowship for Master Studies at MPI-Informatics, Saarbrucken, 2012.
- Jagadish Bose National Science Talent Search(JBNSTS) scholarship, 2008.
- Selected for admission to *B.Math* in Chennai Mathematical Institute(CMI), Chennai, 2008.
- Ranked **254** in IIT Joint Entrance Exam (IIT-JEE), 2008 (out of 200 thousands participants)
- Ranked **12** in state engineering entrance exam, WBJEE 2008 (out of 50 thousand participants)
- Selected for in Indian National Mathematics Olympiad(**INMO**) exam in 2007.

Extra Curricular Activities

- Board member of PhD student association at Cornell Tech.
- Member of executive committee of Bengali Association of Madison (BAM), WI in 2014-15. BAM organizes lots of Indian cultural events in Madison, WI.
- Captain of Maths Olympiad team of residence hall and won Silver and Gold in 2011 and 2012 in inter hall Mathematics Olympiad in 2011 and 2012 respectively.
- Secured Second position in **Yahoo HackU** 2012 at IIT Kharagpur.