Clement Fung

Email: clementf@andrew.cmu.edu
Website: *https://clementfung.me*

SUMMARY

Machine learning models present a unique threat model. As a result, when machine learning is integrated into real-world systems, the underlying assumptions and threats change. My research explores how these changes affect the privacy and security of such systems when they are deployed for real-world use. Most notably, I am interested in attacks and defenses for distributed multi-party machine learning systems (such as federated learning) and the security and explainability of machine-learning-based cyber-physical systems.

PUBLICATIONS

Refereed publications

- **Biscotti: A Blockchain System for Private and Secure Federated Learning**
  Muhammad Shayan, Clement Fung, Chris J.M. Yoon, Ivan Beschastnikh.
  IEEE Transactions on Parallel and Distributed Systems (TPDS)
  Volume 32, Issue 7. July 2021.
- **Towards a Lightweight, Hybrid Approach for Detecting DOM XSS Vulnerabilities with Machine Learning**
  William Melicher, Clement Fung, Lujo Bauer, Limin Jia.
  The Web Conference 2021
  Ljubjana, Slovenia (Virtual). April 2021.
- **The Limitations of Federated Learning in Sybil Settings**
  Clement Fung, Chris J.M Yoon, Ivan Beschastnikh.
  23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)
  Donostia/San Sebastian, Spain (Virtual). October 2020.
- **Brokered Agreements in Multi-Party Machine Learning**
  Clement Fung, Ivan Beschastnikh.
  10th ACM SIGOPS Asia-Pacific Workshop on Systems (APSys 2019)
  Hangzhou, China, August 2019.
- **GainForest: Scaling Climate Finance for Forest Conservation using Interpretable Machine Learning on Satellite Imagery**
  David Dao, Catherine Cang, Clement Fung, Ming Zhang, Nick Pawlowski, Reuven Gonzales, Nick Beglinger, Ce Zhang.
  Climate Change: How Can AI Help?: ICML 2019 Workshop
  Long Beach, CA, June 2019.

Pre-prints

- **Dancing in the Dark: Private Multi-Party Machine Learning in an Untrusted Setting**
  Clement Fung, Jamie Koerner, Stewart Grant, Ivan Beschastnikh.
  ArXiv Preprint: *1811.09712*
  November 2018.
- **Mitigating Sybils in Federated Learning Poisoning**
  Clement Fung, Chris J.M. Yoon, Ivan Beschastnikh.
  ArXiv Preprint: *1808.04866*
  August 2018.

EDUCATION

PhD, Societal Computing, School of Computer Science 2019 - present
Carnegie Mellon University, Pittsburgh, PA
Cumulative GPA: 3.87 / 4

Research Projects:
- DOM-XSS-ML: A hybrid, machine learning system to detect DOM-XSS with reduced overhead
- ICS-ML: Securing industrial control systems with machine-learning-based anomaly detection

Graduate Courses:
- 18731 - Network Security (*Prof. Vyas Sekar*)
- 17762 - Law of Computer Technology (*Prof. Michael Shamos*)
- 36700 - Probability and Mathematical Statistics (*Prof. Valerie Ventura*)
- 18739 - Security and Fairness of Deep Learning (*Prof. Piotr Mardziel*)
- 18730 - Introduction to Computer Security (*Prof. Virgil Gligor*)

MSc, Computer Science 2016 - 2018
University of British Columbia, Vancouver, BC
Cumulative GPA: 88 / 100

Thesis:
- Dancing in the Dark: Private Multi-Party Machine Learning in an Untrusted Setting.
  Supervisor: Ivan Beschastnikh

Achievements:
- UBC CS Department Graduate Teaching Assistant Award, 2017
- UBC CS Department Student Service Award, 2017

Research Projects:
- Biscotti: A secure, private blockchain-based system for multi-party machine learning
- FoolsGold: A sybil-resilient federated learning protocol against model poisoning
- TorMentor: A system for distributed, collaborative, anonymous machine learning
- InsuLearn: A system for distributed learning on private medical data
- DistributedClocks: A library for vector clock instrumentation of distributed systems

Graduate Courses:
- CPSC 532R - Graphical Models (*Prof. Siamak Ravanbakhsh*)
- CPSC 540 - Advanced Machine Learning (*Prof. Mark Schmidt*)
- CPSC 538W - Data At Scale (*Prof. Andrew Warfield*)
- CPSC 538B - Distributed Systems (*Prof. Ivan Beschastnikh*)
- CPSC 536F - Algorithmic Game Theory (*Prof. Hu Fu*)
- CPSC 340 - Machine Learning (*Prof. Mark Schmidt*)

BASc, Systems Design Engineering (Dean's Honour's List Distinction) 2011 - 2016
University of Waterloo, Waterloo, ON
Cumulative GPA: 88 / 100

Capstone Project:

- Driven: A Automated System for Intelligent Annotation and Analysis of Lane Change Sentiment
  Supervisor: Alexander Wong

Awards:
- Sanford Fleming Award for Co-operative Proficiency, 2016
- GM Canada Innovation Award, 2016 - *$500*
- W.W. King Exchange Fellowship, 2015 - *$500*
- President's International Experience Award, 2014 - *$1500*
- Sanford Fleming Award for Outstanding Communication in Work Term Report, 2013 - *$300*
- Colonel Hugh Heasley Engineering Scholarship, 2011 - *$10000*
- University of Waterloo President's Scholarship of Distinction, 2011 - *$2000*

Achievements:
- Dean's Honour's List, Winter 2016 - *Rank unknown*
- Dean's Honour's List, Winter 2013 - *Ranked 2nd / 81 students*
- Dean's Honour's List, Spring 2012 - *Ranked 2nd / 85 students*
- Dean's Honour's List, Fall 2011 - *Ranked 3rd / 94 students*

TEACHING EXPERIENCE

Teaching Assistant Sept 2016 - Dec 2018
University of British Columbia

- DSCI 571: Supervised Learning Fall 2018
  Instructors: Michael Gelbart, Varada Kolhatkar
- DSCI 523: Data Wrangling Fall 2018
  Instructors: Jenny Bryan, Rodolfo Lourenzutti
- CPSC 340: Machine Learning Winter 2018
  Instructor: Michael Gelbart
- CPSC 340: Machine Learning Fall 2017
  Instructor: Mark Schmidt
- CPSC 210: Software Construction Winter 2017
  Instructors: Norman Hutchinson, Paul Carter, Mehrdad Oveisi
- CPSC 210: Software Construction Fall 2016
  Instructors: Norman Hutchinson, Ryan Vogt, Jonatan Schroeder

PROFESSIONAL EXPERIENCE

Research Assistant August 2019 - present
Carnegie Mellon University, Pittsburgh, PA, USA
- Research on machine learning, security and the industrial internet-of-things in CyLab.

Software Engineer January 2019 - July 2019
Oasis Labs, Berkeley, CA, USA
- Developed applications for secure data sharing and other confidential use cases in an early stage blockchain startup.

Research Assistant January 2017 - December 2018
University of British Columbia, Vancouver, BC, Canada
- Research on the security of machine learning systems in the Networks, Systems and Security (NSS) Lab.

Software Engineering Intern June - August 2015
LinkedIn Corporation, Sunnyvale, CA, USA
- Analytics: Building infrastructure for online relevance scoring at scale

Software Engineering Intern September 2014 - December 2014
LinkedIn Corporation, Mountain View, CA, USA
- Distributed Data Systems: Prototyped and designed new derived data serving system, Venice

Software Engineering Intern January 2014 - April 2014
Voicebox Technologies, Bellevue, WA, USA
- Server and Tools: Implemented layer for concurrent database access on a mobile service

Software Developer May 2013 - August 2013
Ontario Institute for Cancer Research, Toronto, ON
- Software developer in Paul Boutros' bioinformatics research group

Software Developer September 2012 - December 2012
pVelocity, Toronto, ON

QA Analyst January 2012 - April 2012
pVelocity, Toronto, ON