CDMS Research Seminar

Analog vs. Digital Epsilons: Implementation Considerations for Differential Privacy

Wednesday, 27th July 2022, 10:00 am

https://uws.zoom.us/j/85147401905?pwd=ERdms_qKSiqvNByWx6pDb9q3hXOLN-.1

Speaker: A/Prof Olya Ohrimenko, University Melbourne

Abstract: Differential privacy (DP) provides a rigorous framework for releasing data statistics while bounding information leakage. It is currently a de facto privacy framework that has received significant interest from the research community and has been deployed by the U.S. Census Bureau, Apple, Google, Microsoft, and others. However, DP analysis often assumes a perfect computing environment and building blocks such as random noise distribution samplers. Unfortunately, a naive implementation of DP mechanisms can invalidate their theoretical guarantees. In this talk, I will highlight two attacks based on implementation flaws in the noise generation commonly used in DP systems: floating-point representation attack against continuous distributions and timing attacks against discrete distributions. I will then show that several state-of-the-art implementations of DP are susceptible to these attacks as they allow one to learn the values being protected by DP. Our evaluation demonstrates success rates of 92.56% for floating-point attacks in a machine learning setting and 99.65% for end-to-end timing attacks on private sum. I will conclude with suggested mitigations, emphasizing that a careful implementation of DP systems may be as important as it is for cryptographic libraries. The talk is based on joint work with Jiankai Jin (The University of Melbourne), Eleanor McMurtry (ETH Zurich) and Benjamin Rubinstein (The University of Melbourne), that appeared in IEEE Symposium on Security and Privacy 2022.

Bio: Olya Ohrimenko is an Associate Professor at The University of Melbourne which she joined in 2020. Prior to that she was a Principal Researcher at Microsoft Research in Cambridge, UK, where she started as a Postdoctoral Researcher in 2014. Her research interests include privacy and integrity of machine learning algorithms, data analysis tools and cloud computing, including topics such as differential privacy, verifiable and data-oblivious computation, trusted execution environments, side-channel attacks and mitigations. Recently Olya has worked with the Australian Bureau of Statistics and National Bank Australia. She has received solo and joint research grants from Facebook and Oracle and is currently a PI on an AUSMURI grant. Olya holds a Ph.D. degree from Brown University and a B.CS. (Hons) degree from the University of Melbourne. See https://people.eng.unimelb.edu.au/oohrimenko/ for more information.

Rodrigo Calheiros is inviting you to a scheduled Zoom meeting.

Topic: CDMS Seminar: Analog vs. Digital Epsilons: Implementation Considerations for Differential Privacy
Time: Jul 27, 2022 10:00 AM Canberra, Melbourne, Sydney

Join Zoom Meeting
https://uws.zoom.us/j/85147401905?pwd=ERdms_qKSiqvNByWx6pDb9q3hXOLN-.1

Meeting ID: 851 4740 1905
Password: 809180
One tap mobile
+61280156011,,85147401905#,,1#,809180# Australia
+61370182005,,85147401905#,,1#,809180# Australia

Dial by your location
+61 2 8015 6011 Australia
+61 3 7018 2005 Australia
+61 7 3185 3730 Australia
+61 8 6119 3900 Australia
+61 8 7150 1149 Australia
Meeting ID: 851 4740 1905
Password: 809180
Find your local number: https://uws.zoom.us/u/kbhlystTdm

Join by SIP/H.323:
85147401905@zoom.aarnet.edu.au
or 85147401905@zmau.us
or 103.122.166.55 (Australia)
Meeting ID: 851 4740 1905
Password: 809180

Join by Skype for Business