

CWSF 2016 - Montreal, Quebec



Dylan Beswick

Really Random?

Challenge: Discovery

Category: Junior

Region: Northern British Columbia

City: Hudson's Hope, BC

School: Hudson's Hope School

Abstract: Most of us don't know this, but a secure internet connection relies on "random" numbers. Since computers cannot generate truly random numbers, we had to come up with an alternative: pseudorandom numbers. However, they rely on a good seed source. A bad seed source creates bad pseudorandom numbers. In my experiment, I tested different seed sources to see which are good and which are not.

Biography

I am a 12 year old math enthusiast who became hooked on computer programming in grade 4 with the discovery of the MIT Scratch website. This led to my learning of many other programming languages like Python, Ruby, JavaScript, SQL, HTML and CSS. I am proud to say that I have built TCP socket home control systems via the internet, and have found and suggested patches for security vulnerabilities on the Scratch website. In addition to programming, my interests include soccer, volleyball, badminton, snowmobiling, fly-fishing and playing the piano. My science fair project on password strength earned the regional top grade 6 project last year. I have also attended the provincial heritage fair and received the 2015 B.C. Lieutenant Governor Historical Literacy Award for my project on Canada's postal history. Currently, my dream for post-secondary education is to go to MIT and take computer science. The inspiration for my project came as a result of watching a video on advanced TLS. TLS needs access to random numbers, starting my interest in random number sources. My future project improvements include exploring more seed sources, testing different algorithms and expanding my statistical analysis to make my results more accurate.

Awards

Value

The Actuarial Foundation of Canada Award - Junior Sponsor: The Actuarial Foundation of Canada	\$500
Total	\$500