# The 24 hour cycle of truth for Whitenoise

Notes from the editor:

Stephen Hawking wrote a brilliant and beautifully illustrated book called The Universe in a Nutshell. This is the History of Whitenoise in a nutshell and these tiny stories are likely to get a lot of mileage.

We had the unfortunate experience of having to address a fraudulent, published paper claiming that Whitenoise could be broken. Even though in private correspondence Hongjun Wu told WNL that Whitenoise with a 3-byte delinearization foiled his “break”, he refused to retract his paper. To this day he claims his break still works even though he can’t be bothered to test it. Can you imagine the Federal Drug Administration (FDA) or pharmaceutical companies conducting their research in the same way?

This created a real barrier in our marketing efforts. Still not knowing the entire story ourselves, it was clear that this was about business and competition reasons.

In the fall of 2007, the following strategy was taken to force Hongjun Wu to publicly state the truth that his break doesn’t work.

By necessity I was forced to use the CC function for a group email (which was admittedly risky and generally poor taste). I was forced by necessity to use certain person’s real identities. Research and truth cannot exist in the dark. I am now respecting the need for privacy [secrecy] of these observers because of the positions they hold. To do so, their names have been redacted in the real transcripts.

The people who have been woven into this story cannot accurately tell their own stories without at least passing mention of Whitenoise. This in turn will always keep the Whitenoise story alive.

Welcome to truth and marketing in the age of the Internet and Google research.

It pays to read more than just the abstract that Google provides. Truly you cannot read a book by its cover.

Imagination IS the strongest weapon known to man.

In order to get the truth publicly admitted it was necessary to issue to following challenge to a very large and important audience.

On Nov 19, 2007 8:21 AM, Andre Brisson <brisson@lightspeed.ca> wrote:

November 19, 2007

Everyone addressed, including the Emmy award winning TV director/producer, have in some way touched Whitenoise.

I have attached a history of Whitenoise. Before publishing this document, I would like to offer each of you an opportunity not provided before to Whitenoise. Before publication, and in the interest of sound journalism and accurate academic research, I would like each of you to read the attached history of Whitenoise and offer any clarifications of dates, timing or substance. I thank you in advance for the efforts you make in helping us edit this document for complete accuracy prior to publication.

Mr. Hongjun Wu

"This is a personal invitation for you to join the insured $100,000 Whitenoise Security Challenge at http://www.wnlabs.com/WhitenoiseSecurityChallenge. You are free to use the purported Whitenoise break by Hongjun Wu posted at http://eprint.iacr.org/2003/250 for a specification of patented Whitenoise at http://eprint.iacr.org/2003/249.

You may collaborate with an American or Canadian colleague or institution as a team so that you meet contest rules requirements, and you are free to solicit help from any one of the experts cc'd on this email. By necessity it would mean that you would have to share the money with any expert you solicit to help you but I believe that it would still be worth your time.

You have published to the world that it is easy to break Whitenoise

and you have left it there even though you have indicated in direct communications with Whitenoise Laboratories Inc. that you cannot be bothered to prove this by actually attempting a break. I am hoping that the insured prize money will change this attitude.

The Whitenoise Security Challenge provides 1,000,000 bytes of the key stream or 13.33 times the 80,000 bytes you claim are needed to easily break the algorithm. The reply to Hongjun Wu's purported claim is found at: http://www.wnlabs.com/Papers/Response.pdf.

Scientific method and actual public demonstration are more highly valued and respected than public commentary. The purpose of the contest is to shed light on the credibility of claims you have made which is why we ask any independent third party or institution to use your theory to win the contest. Let your professional colleagues know about this challenge.

If you have comments or questions concerning this matter please use Reply All. The persons CC'd represent academia, the Canadian government, associations, vital public functions like the press, business channels and known experts. All have been exceedingly helpful to Whitenoise work and would be interested in your response. Visit the official http://www.wnlabs.com/WhitenoiseSecurityChallenge site often to track submissions if any.

I am considering using this documentation at the end of the contest period, if you or the public fail to break Whitenoise, as proof that you are fully aware of this request to validate your published work. Government agencies could not do so. I will consider over the contest period whether this letter is to be published and made available to the public.

I am also considering sharing your previous emails to Whitenoise Laboratories Inc. where you acknowledge that Whitenoise with a multi-byte delinearization resists your attack. The fact that you would fail to publicly acknowledge this after your previous published claims is an affront to quality research and does the entire community a disservice.

Andre Brisson CEO/President

Partner@thirdbrigade.com is intended for Brian O'Higgins
info@byressecurity is intended for Eric Byres
listmanager@sinmonsingh.net is intended for Simon Singh

-----Original Message-----
From: Hongjun Wu [mailto:wuhongjun@gmail.com]
Sent: Tuesday, November 20, 2007 9:49 AM
To: Andre Brisson
Cc: cadams@site.uottawa.ca; partner@thirdbrigade.com; info@byressecurity.com; itraore@ece.uvic.ca; paul_thiel@telus.net; Clay_Howey@bcit.ca; Hassan_Farhangi@bcit.ca; listmanager@simonsingh.net; asw@ieee.org; [redacted]cs.columbia.edu; daw@cs.berkeley.edu; [redacted]; fabro@loftyperch.com; schneier@schneier.com; Amardeep Gill; Brent Sternig; Chris Cambon; Elsie Au; Kevin Cudihee; Lee, Clarence; Shebia Leung; Vaani Nadhan; [redacted]; alnoor@shikatronics.com; dave.church@internatonal.gc.ca; [redacted]; osnir@mastertronics.com.br; prodrigue@shikatronics.com; rharrison274@rogers.com; richard@techincentives.ca; Al MacKinnon; amadar@deloitte.ca; Anand Deshpande; Andrej Dobos; Armen Vardanian; Arnold Leung; Beach, Michael C; bernard brisson; bhaidri@absolute.com; Bill Thorpe; BIV HighTech Directory; brad_wait@canaccord.com; brandon_boddy@canaccord.com; [redacted]; Chris Blask; Chris Pinter; chris.langdon@telus.com; Christopher Kuljis; Colin Campbell; Colleen Pennington; Curtis Blais; [redacted]; Dave Matthews HP; David Harrison; Debra Kirby; Debra Williams; Element & Associates; Eric Tardieu; eric.j.shum@ca.pwc.com; Eugen Simion work; Fabien Dormoy; Gary Godshalk; Gary Tremblay; Graeme Durant; Greg Aasen; Greg Desaulniers; greg.julian@bell.ca; guy.huntington@hvl.net; Hironmoy Bhomik; Ian Banks; Ian Cooper; ian@viff.org; jdow@rainmaker.com; Jennifer Lucas; Jennifer Rocha; Joann Smith; John Bean; jordon@mainsailpartners.com; Jozef Starosta; Kaare Myrland; Ken Hill; Kevin Tribe; Lawrence Loewen; Madeleine Guibert; Mandy K. Cheema; Marc E. Levy; [redacted]; Mark Winter; [redacted]; Mark Zanotti; marketing@missionuav.com; martyn@idmail.com; Michael B. Jones; Michael Cannata; Michael Zino; Mike Nelson; Nahar Ros; Neal Nicholson; Price. Kagey; rahamat bidin; rahamat@Encrya.com; Ram Pai;

Raymond.Lawson@telus.com; [redacted]; Riccardo Pivetta; roger@privatesoftware.net; Sameer Karmarkar; Scott Shaw work; Steve Anderson; Steven Clark; Stuart Phillips; Tanasut Rasmidatta; Tim Garon; Tim MacFarlane; tmccon; Tom West; Tom West; Toshiro Ikeda; Val Swannell; Vtulai; [redacted]; susana@winbc.org; Carmen; Caroline Lewko; Caroline Lewko (WIP); CATAAlliance; Cindy Pearson; JETRO Vancouver; Michael Bidu; Shana Korotash; SOIC 2007 System; WMSCI 2007 System; Cliff.Smith@international.gc.ca; Anton. Kuipers; Barabana, Mary Gail; Claude Belisle; Craig Fulton; George Green; Harold Deck; Jacques Siegrist; Jenelle. Hawkins; June.Shinagawa@international.gc.ca; Kojiro Ichikawa; Lucia Marc CSE; Neil: VAN Callow; Nick Fong; [redacted]; Sean. Barr; Shabnam.Parang@international.gc.ca; [redacted]; Sunil. Sharma; Wendy. Trusler; [redacted]

Subject: Re: Whitenoise invitation and request for assistance in editing History of Whitenoise document

*To all: Sorry for the spam. I have to reply this e-mail to all (as requested by Andre Brisson).*

*I notice that most of the people on the cc list are not cryptographers. It is a bit funny for me to send a cipher related e-mail to so many noncryptographers.*

*Mr. Andre Brisson,*

*1) You claim in the "response" that my attack does not break the original Whitenoise. But you revised the Whitenoise design following my attack. Is it too funny?*

*You don't understand my attack on the original Whitenoise. It is because that you even do not understand the concept of "equivalent keys" in cryptography. I added more details on Feb. 19 2004 to explain it. But even four years later, you still could not understand the attack.*

*2) Are you honest? .*
*My attack breaks the original Whitenoise. But in the challenge, you*

*provided the revised Whitenoise. In your e-mail, you are trying to use the revised Whitenoise to show that my claim on the original Whitenoise is incorrect. It is ridiculous.*

*You are cheating the community and trying to damage my reputation just for the purpose of advertising your poor cipher (the cipher is with the funny 240,0000-bit minimal strength as given at your challenge site, and the cipher is extremely slow comparing to many modern stream ciphers). It does no matter that you do not know cryptography well, but it does matter that you cheat people.*

*You should award $100,000 for breaking the original Whitenoise if you think that my attack does not break it.*

*3) My attack shows that the original Whitenoise is insecure.* ***The revised Whitenoise can resist my attack on the originnal Whitenoise. OK?***

*In fact, it is improper for you to call the revised version as Whitenoise. Just remind you that Whitenoise has been broken. You need to call the revised Whitenoise as Whitenoise 2.0 or any other name since different specifications should be named differently, and you have already named the original Whitenoise cipher as Whitenoise.*

*4) Sometimes it is not difficult to break a cipher designed by some amateurs; but it is difficult to explain to the amateurs that their cipher is insecure. So it is a joy to analyze a cipher designed by excellent cryptographers; but it is a headache to analyze a cipher designed by amateurs.*

*5) I like this humor in the history document: "Brisson and Boren wonder whether there may be a use for the Whitenoise structure in physics in order to overcome some of the restraints posited by the Uncertainty Principle. The Whitenoise structure might lend itself to research in other scientific endeavors like clean energy sources."*

*6)* ***Also this one: "Whitenoise Laboratories Inc. current advisors include talented experts."***

*Regards,*
*Hongjun Wu*

On Nov 19, 2007 8:21 AM, Andre Brisson <brisson@lightspeed.ca> wrote:

To all cc'd – this will be our last group email.

Unfortunately, this entire exercise was necessary for the truth to come out. Anyone that has input for the History of Whitenoise, we await your reply.

Dr. Traore, you can see the clarification you requested in History of Whitenoise ver 13.

Sincerely Andre Brisson

Dear Mr. Wu

***Thank you for publicly acknowledging that you cannot break Whitenoise with a 3-byte draw delinearization.***

I really wish you would have carefully read who the email was addressed to before writing this questionable response with disparaging comments. I really wish you would have read the rebuttal that ePrint did not allow published at that time.

http://www.wnlabs.com/Papers/Response.pdf

I would like to personally apologize to the following persons:

- Simon Singh - author of The Code Book
- Carlisle Adams – creator of CAST Encryption algorithm, professor at the University of Ottawa

- [redacted] – Fellow at AT&T and Professor at Cornell University
- Brian O'Higgins – Founder of Entrust Technologies and currently CTO of Third Brigade
- Dr. Issa Traore – professor at the University of Victoria
- Dr. Hassan Farhangi – current director of the British Columbia Institute of Technology Group for Advanced Information Technology (GAIT)
- Paul Thiel – former director of the British Columbia Institute of Technology Group for Advanced Information Technology (GAIT)
- [redacted] - Senior Fellow Lockheed Martin, IS&GS
- Dr. Andrew Wright formerly board member PMC Sierra
- [redacted] – CTO Lockheed Martin
- Eric Byres – CTO of Byres Security
- Clay Howey – Fellow the British Columbia Institute of Technology Group for Advanced Information Technology (GAIT)
- [redacted] – Entrepreneur in Residence University of British Columbia – Founder of Excert sold to RSA
- Mark Fabro CISSP, CISM currently CTO/President of Lofty Perch; former Chief Scientist for Bearing Point
- [redacted] – VP Cubic Defense contractors
- [redacted] – Anteon
- Nicholas Fong – security expert for the National Research Council of Canada
- [redacted] – Chairman of the Board for Sasktel
- The experts at TELUS
- Shebia Leung -marketing British Columbia Institute of Technology
- Bruce Schneier – Cryptogram – creator of Twofish with Wagner et al
- David Wagner – professor at the University of California, Berkeley
- [redacted] – Emmy Award Winning TV director/producer
- Alnoor Sheriff – President CEO of Shikatronics Inc. global distributors
- And of course everyone else
-

Regarding point 2 – please study
http://www.wnlabs.com/algorithm/WhitenoiseAlgorithmVisualLook.pdf
slide number 12

***Mr. Wu, thank you for your frank and public disclosure that you cannot break Whitenoise with a multi-byte delinearization.***

Andre Brisson