**The History of Whitenoise**

"Spin a Rubik's Cube fast enough and you see a sphere. That would be a good foundation for a cipher," thought **Andre Brisson**. "Why stop at three dimensions?" thought **Stephen Boren.**

Brisson and Boren were inspired after reading **The Code Book by Simon Singh.** At the same time**,** electronic theft was reaching new heights (and continues to this day). Ideas and timing collided to create **Whitenoise** and a **deterministic random number generator** and **symmetric stream cipher** was born.

Once the initial version of Whitenoise was complete, in 2002, Brisson and Boren approached the British Columbia Institute of Technology Group for Advanced Information Technology (**GAIT**), which develops advanced computer technologies and concepts to solve complex problems for industry clients. They also solicited the expertise and advice of **Paul Thiel (Director of the GAIT Lab at that time), Eric Byres and Clay Howey. Dr. Issa Traore of the University of Victoria** was recommended as having the expertise, equipment and resources to properly conduct the kind of performance testing of Whitenoise that was required at this stage. His lab was involved in various software and network security projects at that time.

**The Performance Analysis** was conducted by the Department of Electrical and Computer Engineering, University of Victoria, B.C., Canada. Once completed in February of 2003, this Performance Analysis revealed that an un-optimized version of Whitenoise did not have a single statistical failure in randomness testing against the NIST test suite, which is used to evaluate different characteristics of key based technologies. The sensitivity of these tests was set to an order of magnitude higher than normally used to **evaluate AES algorithms** – Whitenoise performance was tested to allow only one statistical failure in every thousand tests. There were no failures. Neither was a very powerful computer array able to guess a key. Whitenoise generated data random enough on the first round to properly use this test suite.

**Key based technologies** that can be used for encryption are regulated technologies because of national security implications. All appropriate Canadian government defense and policing agencies mandated to oversee and evaluate these kinds of technologies were contacted immediately after receiving the performance analysis.

Soon after, in March of 2003 a director at **Scotia McLeod** investment recommended the initial Board of Advisors for the company that would come to be named Whitenoise Laboratories Inc. **David Archibald**, **Arthur MacDonald** and **Alan Lytle** became the first advisory board members. These men played key roles in building Nortel into the most valuable company in Canadian history (to that date).

In April of 2002, **Brian O'Higgins, Co Founder of Entrust Technologies** met with the advisors and creators of Whitenoise. Entrust Technologies Inc. was initially spun out of

Nortel in one of the most valuable financial transactions for Nortel to that date. Advice was then sought from **Carlisle Adams**, creator of the **CAST encryption algorithm** and an internationally known and respected cryptographer. Mr. Adams previously worked for Entrust Technologies and is currently a professor at the University of Ottawa, Canada.

The weight of Mr. O'Higgins reference led to a security analysis performed by **David Wagner** who is a published cryptanalyst from the University of California, Berkeley. Wagner was contacted in the spring of 2003. In the fall of 2003, David Wagner's final security analysis [not drafts] was received and soon posted on ePrint, the archive run by the International Association of Cryptographic Research. David Wagner wrote "*"Exhaustive key search is not a threat. Whitenoise uses keys with at least 1600 bits of randomness. ... Even if we hypothesized the existence of some magic computer that could test a trillion-trillion key trials per second (very unlikely!), and even if we could place a trillion-trillion such computers somewhere throughout the universe (even more unlikely!), and even if we were willing to wait a trillion-trillion years (not a chance!), then the probability that we would discover the correct key would be negligible (about $1/2^{1340}$, which is unimaginably small)."*

During this time a complete specification was being written up for both the patenting process and to provide full disclosure to the scientific community. Wagner's security analysis was posted at ePrint, the archive for the International Association of Cryptographic Research in **October of 2003**.

A specification for Tinnitus was posted at ePrint on **28 Nov 2003**. The specification for Tinnitus was intended for academic purposes only. This specification proposed three different delinearization processes that can be used in conjunction with Whitenoise.

Two days later **30 Nov 2003 Hongjun Wu** published a paper with a purported break based on a reduced version of Whitenoise he created after reading David Wagner's security analysis. [On **November 20, 2007** Mr. Wu publicly acknowledged that his "break" does not work on Whitenoise when it is deployed using a three byte substitution.] The creators of Whitenoise worked with crypto mathematicians over a four month period to try to validate the purported Whitenoise break on the reduced and revised version of Whitenoise proposed by Wu. They were unable to do so. Opinions were sought from institutions. The reply or rebuttal that was intended to be published on ePrint is available at: http://www.wnlabs.com/Papers/Response.pdf and has now, as of November , 2007 been allowed to be included as an addendum to the original paper and the version reduced (by Wu) using a simple substitution as the delinearization layer. This break has never been demonstrated to work. Original "Tinnitus" files with Whitenoise with simple substitution are available directly from Whitenoise Laboratories Inc. for academics interested in continued research.

Hongjun Wu last revised his hypothesis on **19 Feb 2004**. The Tinnitus specification was last revised **30 Mar 2004**, over a month after Hongjun Wu posted his last hypothesis. There has been no subsequent follow up by Wu. Both Hongjun Wu and David Wagner were credited in the revision dated and published at http://eprint.iacr.org/2003/249

The $100,000 Whitenoise Security Challenge was created to provide a public forum for editors and experts to publicly substantiate their opinions or hypotheses. It has a financial incentive large enough to merit the effort serious scientific method demands in substantiating the validity, reliability, and credibility of public opinions and claims. It also serves a role in being as public a vehicle as was used to promote opinions and hypotheses. This insured contest runs from October 15, 2007 through April 15, 2008. http://www.wnlabs.com/WhitenoiseSecurityChallenge.

In 2007 Whitenoise received its international patents.
(US Patent Number 7,190,791)
(European Patent Number EP1566009)

From its inception, Whitenoise has been tested in security applications and technologies that spring from innumerable deployments. Because of the very exacting standards in the mandated security environment, research and development continues not only on the significant encryption characteristics of Whitenoise, but also on the ways this technology can be deployed outside this environment. Dynamic Identity Verification and Authentication [DIVA] is an example of how Whitenoise can be exploited for continuous authentication, inherent intrusion detection, and automatic denial of network access to criminal behavior (revocation). See Critical Insights and Differentiators of Whitenoise. Other areas of interest include DRM and authorizations. An architecture using AES algorithms and Whitenoise as an Identity Management authenticator is examined in Dynamic Distributed Key Infrastructures.

The pace of research involving Whitenoise has been greatly accelerated by sponsoring CST Practicum Projects at the British Columbia Institute of Technology, interfacing with the academic community in the Lower Mainland and by involvement with government agencies like the Canadian National Research Council. Research has also been furthered by working with cutting edge Lower Mainland companies developing a range of secure solutions. Whitenoise has benefited from the expertise of the British Columbia Technology Industry Association, WINBC, and the Wireless Industry Partnership.

Whitenoise currently sits on the Advisory Committee of the British Columbia Institute of Technology CST program.

Whitenoise was created by Andre Brisson and Stephen Boren.