Unclassified story of Whitenoise Super Key Encryption and Dynamic Identity Verification and Authentication

Contents

abrisson@wnlabs.com

Unclassified History of Whitenoise super key technologies

The Whitenoise super key process and cipher was conceived by André Brisson (British Columbia, Canada) in 1998. The first implementation was built by Stephen Lawrence Boren (British Columbia, Canada). This led to the first implementations by Stephen Boren of the inventions using Whitenoise super keys called Dynamic Distributed Key Infrastructures (DDKI) and Dynamic Identity Verification and Authentication (DIVA). http://www.wnlabs.com/pdf/Cyber_Belt_Presentation.pdf

This presentation and notification was given to NIST and members of the Fort Meade Cyber/Intel community in 2016. See slide 33.

Dynamic Distributed Key Infrastructures is a virtual symmetric key framework that can be used with Public Key Infrastructures (PKI) to address several PKI security issues. DDKI can be used in lieu of PKI.

Dynamic Identity Verification and Authentication (DIVA) is a one-time-pad implementation of Whitenoise super keys for continuous, dynamic authentication throughout a network session, data provenance and identity. One-time-pads are the only cryptographic deployment that can be mathematically proven to be unbreakable.

Whitenoise technologies are broadly patented globally including the United States of America, Canada, China, India and the European Union.

Conceptually: spinning a Rubik's Cube on its universal access in all directions etches a perfect three dimensional sphere. This became the basis for a multi-hierarchical, multi-level representation of a multi-dimensional cipher that has no limit to the number of dimensions (represented by subkeys).

Whitenoise is a stream cipher. Carlyle Adams (the creator of CAST, University of Ottawa, Canada) recognized that Whitenoise is a deterministic random number generator. Mark Fabro (Lofty Perch) recognized it as a one-time-pad.

After the invention of Whitenoise the first institutions notified and who conducted testing were the Canadian Security Intelligence Service (CSIS) and Communications Security Establishment (CSE). Government institutions rarely release internal test data on national security level technologies. It is these institutions that generally grant permission and certify external Common Criteria labs in Canada. CSE withheld permission for Whitenoise to be Common Criteria certified for several years after the publication of both the performance and security analyses.

In 2002, Paul Thiel, the Director for the Group for Advanced Information Technologies (GAIT Labs) at the British Columbia Institute of Technology succeeded after several years in getting permission and recruiting the ECE Labs at the University of Victoria, British Columbia to conduct performance analysis testing. Dr. Issa Traore conducted the performance analysis which was funded by the National Research Council of Canada.

Performance testing was conducted against the NIST test suite. The NIST test suite was made more sensitive by an order of magnitude that would allow only one statistical error for every thousand rounds (instead of one allowed statistical error for every hundred rounds). Against a super computer array Whitenoise did not even generate a single statistical error. As a random data source it tested more random then the general benchmark of radioactive decay. Whitenoise was treated as national security level cryptographic technology.

Subsequent to the Performance Analysis, a noted cryptographer at the University of California, Berkeley was contracted at the recommendation of Brian O'Higgins, founder of Entrust Technologies, to conduct a security analysis. This cryptographer was unable to identify any mathematical attacks against Whitenoise deployed in a USB implementation called Tinnitus. One reason for this is that Whitenoise key creation does not rely on difficult mathematical or arithmetic formulas to create a one-way function. Whitenoise is a mechanical representation.

The security analysis, **and recorded communications**, with the principal researcher continued during a period of about 9 months.

During the time the security analysis was being performed a prominent cryptographer and on-line crypto blogger wrote a slanderous and unfounded editorial in "The Dog House" labeling Whitenoise as "snake oil" that displayed no scientific method. **A recorded conversation** subsequently occurred where the editor of this publication refused to print a rebuttal. The author of this publication was a colleague and a frequent collaborator on joint cryptographic research with the security analysis researcher. The Whitenoise Security Analysis had yet to be delivered or published.

Political, institutional and corporate pressure from Canada eventually compelled the researcher from the University of California, Berkeley to release the security analysis. Two conclusions from this report were that there was no known mathematical attacks that were effective against Whitenoise and that Whitenoise was not susceptible to brute force (and now post quantum computing) attacks.

The security analysis also stated that brute force attacks were not a threat.

"Exhaustive keysearch is not a threat. With the recommended parameters, Whitenoise uses keys with at least 1600 bits of randomness. Exhaustive search of 1600-bit keys is completely and absolutely infeasible. 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 ½ to the 1340^{th} power), which is unimaginably small. Hence, if keys are chosen appropriately and Whitenoise is implemented correctly, exhaustive keysearch is not a threat."

A copy of this report has now been located in ePrint of the International Archives for Cryptographic Research. Previously Whitenoise Labs published this report from its website.

It is interesting to note while pride has been expressed about the research derived working with the Dog House blogger that the extraordinary results described above never merited any note or mention in their subsequent years of research when it was clearly superior.

After the publication of the security analysis, a noted Fellow at the AT&T Labs Research in Florham Park, New Jersey and former Chief Technologist for the United States Federal Trade Commission was contacted through British Columbia Institute of Technology and the University of Victoria because he is a recognized expert in Man-in-the-Middle attacks which dynamic distributed key systems prevent.

En route to the University of Victoria, British Columbia where the performance analysis was previously conducted and data housed at the ECE Labs this cryptographer gave a presentation at the IBM Theater at the British Columbia Institute of Technology. During this presentation he announced, “I have recently seen the future of the Internet.”

Whitenoise was subsequently certified by AT&T when presented through WavefrontAC, the Canadian Federal Wireless Accelerator.

The founders of Whitenoise Laboratories published the Tinnitus specifications on ePrint of the International Archive for Cryptographic Research (IACR) in 2003 in order to generate scrutiny from the cryptographic community and widespread testing of the Whitenoise algorithm for independent validation of the results of both the performance and security analyses from non-governmental institutions.

Within days of this ePrint publication a cryptographic researcher who may previously have collaborated with other cryptographers noted published a false, unsubstantiated break claim on ePrint.

Oddly the author of this false claim is acknowledged at the end of the same ePrint Tinnitus specification for assistance given to Stephen Boren on a three-byte delinearization technique to create an additional one-way function within the algorithm. The false break claim was never demonstrated but had negative effect.

Stephen Boren worked for about six months with guidance from a crypto-mathematician named Daniel Wevwrick of Communication Security Establishment to write a mathematical proof showing why the purported claim can not work.

In a highly irregular response from the IACR, the publication of this mathematical rebuttal was refused to be allowed to be published as a chronologically subsequent filing of ePrint. At most the IACR would allow addition of this material as an addendum to the original ePrint Tinnitus specification filing. This appeared to assure that this mathematical rebuttal was unlikely to be found by legitimate and non-politicized researchers in the cryptographic community as it would be seen only after the false claim paper.

In 2007 Whitenoise Laboratories Canada Inc. ran a $100,000 Security Challenge for anyone to successfully use the posted claim in a contest that provided a million bytes of key stream which was 13.3 times more key stream than the claim said was needed. This challenge was conducted in a highly

unusual way in order to force the author to demonstrate his break claim. It was also conducted in front of an audience including feted cryptographers (some noted), high ranking US government officials, and interested academic institutions.

In 2013 a former Director of Global Cyber Security Management for the US Department of Homeland Security was contracted as CEO for Whitenoise Laboratories Canada Inc. This gentleman is purported to have been seconded by the White House from the NSA to take that DHS position. It is speculated that he was involved with the US government legal team that had once attempted prosecution of Phil Zimmerman of PGP. He currently sits on advisories of many companies including the Azizi Bank in Kabul, Afghanistan.

During his tenure Whitenoise was placed in the Innovation Center of a major military contractor in the US capital region and materials were provided to the Technical Advisory Committee and Common Criteria Labs of this military contractor from whence the Snowden incident originated. In breach of understanding, the labs refused to provide any test data or results. They also refused to sell the test data and results to Whitenoise Laboratories Canada Inc.

This CEO, a former key note speaker at Black Hat, then approached Black Hat to conduct a hacking challenge to its membership as they regularly do. Black Hat refused to allow this challenge. But their competitor DEFCON did. The CEO encouraged the contest.

This resulted in a $200,000 cryptographic challenge that ran for a year during the tenure of the former Director of Global Cyber Security Management of the US Department of Homeland Security. No persons from Black Hat, DEFCON, or any institution were successful in this challenge. The accompanying challenge clock was originally branded as the BS Challenge Clock and the noted cryptographer was clearly aware of it.

The formal contest Challenge Clock still runs to this day to reinforce the daunting task hackers face. The dynamic offset was set to change every 15 seconds. Any successful attack on a commercial implementation would have to be accomplished in that time frame or the hacker has to start all over again.

Whitenoise Laboratories Canada Inc. has a permanent open challenge. Test files and source code are readily available to accredited labs, institutions and academics by permit outside of the United States and Canada.

Anonymous, independent testing can be done with the free Whitenoise Strong Encryptor utility that can be readily located through a search engine.

Description

One of the earliest descriptions of Whitenoise super key algorithm can be found at US Patent Application Publication No: US204/0096056 A1 with a publication date of May 20, 2004. All Whitenoise technology patent applications made have been granted.

Dynamic Distributed Key Infrastructure handshakes

The two handshakes of dynamic distributed key systems are simpler than PKI handshakes.

Implementations

Whitenoise deterministic random number generators

Whitenoise is a deterministic random number generator and stream cipher that is able to be implemented as a one-time-pad (DIVA). The performance analysis testing at the University of Victoria, British Columbia did not generate even a single expected statistical error in testing against the NIST test suite.

Dynamic Distributed Key Infrastructures enable distributed keys to in turn securely distribute more distributed keys.

www.wnlabs.com/downloads/Tunnel_Distributed_Keys_distributing_more_keys.pdf

A key distribution paradigm that removes key management from carriers and service providers

There are challenges faced by carriers and service providers in complying with government surveillance mandates. The recent passage of the UK Investigatory Powers Act may presage significant changes to US policy post Patriot Act. http://www.wnlabs.com/news/UK_Investigatory_Powers_Act.php

One Whitenoise implementation uses the distribution of a generic key schedule by carriers and cloud service providers to their clients. The endpoint client perturbs this generic key schedule with their own secret pass phrases to make a unique key secret to the endpoint client. When the client sends encrypted data through communications and uploads it into the cloud for storage the carrier or service provider does not have a copy of the key. As such, there is little other than the capture and retention of encrypted data that a service provider can be compelled to do.

When the upload or transmission is further encrypted (double encrypted) over TLS or SSL the carriers have no copies of the first key and cannot compromise client data themselves. Neither are they able to provide all the necessary key material to outside agencies pushing responsibility to the endpoint originator of communications.

This utility provides an example of such a key schedule and is free to download for testing by researchers and can be found on the Whitenoise Laboratories Canada Inc. website (http://www.wnlabs.com/products/emailenc.php) or by searching the internet for distributors of the Free Whitenoise Strong Encryptor.

This technique was originally developed as a method of allowing manufacture of electronic components requiring cryptography in non-friendly trading partner countries without compromising final security. This was because the US DoD had so many components which were manufactured in China.

VDEE

This Virtual Drive Encryption Engine (VDEE) enables secure device storage and copy protection and is fast enough to allow an application to be run from an encrypted state. It automatically stores data in an encrypted state and there is no change in device use behavior. This utility is available for free testing by researchers at http://www.wnlabs.com.

Whitenoise implementation on microprocessors

Whitenoise can process two bytes per clock cycle and is scalable from there. RSA Spritz requires 27 clock cycles to process a single byte.

http://www.wnlabs.com/downloads/Whitenoise_Usage_scenarios.pdf

http://www.wnlabs.com/technology/WN_Chips.php

Whitenoise DIVA TLS openSSL extension

The following link provides an explanation, demonstration and specification of how to easily harden TLS-SSL PKI implementations. This a critical and simple way to make up on our cybersecurity deficit.

When Whitenoise/DIVA/DDKI implementations are used in conjunction with PKI a two-channel, multi-factor challenge is created where a hacker has to break two keys simultaneously for every break attempt; and, one of the keys isn't available and that key is a dynamically and continuously changing one-time-pad. Since there is only a single one-time distribution of one key this enables simple, ubiquitous distribution by a single on-line upgrade and update.

http://www.wnlabs.com/technology/WNL_TLS_extension.php

Tunnel

Secure point-to-point communications and distributed keys securely distributing more distributed keys.

www.wnlabs.com/downloads/Tunnel_Distributed_Keys_distributing_more_keys.pdf

Secure Cloud Accelerator
http://www.wnlabs.com/pdf/The_cloud_accelerator.pdf

A better bitcoin
http://www.wnlabs.com/pdf/Whitenoise_crypto_currency_mobile_payments_Tata_Innovation_2015.pdf

Turning Biometrics into one-time-pads
http://www.wnlabs.com/pdf/Gartner_Whitenoise_and_iris_biometrics.pdf

Security

Since the inception of Whitenoise there have been only two publicly (non-governmental) claimed and documented attempts at breaking Whitenoise. Neither approach was successful. Additionally, neither claim provided any test data or demonstration for other independent corroboration of their claims.

History of Whitenoise Cannot be Broken

24 hour cycle of truth

www.wnlabs.com/technology/SideChannelAttackResearch.php This attempt incorrectly deployed Whitenoise as a circular shift register and did not follow specifications. Even so, UVIC and this student ran out of money before anything could be demonstrated. Since Whitenoise is dynamic with keys changing continuously a two-year break attempt is not reflective of the real world.

It is important to note that Whitenoise is not susceptible to white noise attacks which are acoustic based side channel attacks. *https://en.**wikipedia**.org/**wiki**/Acoustic_cryptanalysis*

There have been two global hacking contests documented**.**

$100,000 Security Challenge

$200,000 cryptographic challenge

Cryptographic sciences need to achieve a point of transparency that represents fact and legitimate scientific method. Politicization and biased corporate financial interest has called this science into question.

See also

References

US National Cyber Leap Year Summit

Whitenoise Laboratories Canada Inc. and André Brisson were one of four non-US companies invited by the White House Office of Science and Technology Policy/NIST to the First US National Cyber Leap Year Summit on August 17-20, 2009. Whitenoise was the only Canadian invitee even though President Obama was using a BlackBerry from Research in Motion at the time and Elliptical Curve Cryptography was becoming popular.

External Links

United Nations International Telecommunications Union presentation – Geneva, Switzerland

European Telecommunications Standards Institute presentation – Einstein Agora, Sophia Antipolis, France

Further reading

In Denial Code Red – This book is a fictional third party look at the context. It documents the history provided above and provides a critical element in a factorial utility for Integer Factor Cryptography. It may also provide a technique of cyber war counter attack and escalation that does NOT permanently damage critical infrastructures.

This book is available through Amazon at: http://www.amazon.ca/Denial-Code-Andre-Jacques-Brisson/dp/0986728608/ref=sr_1_1?ie=UTF8&s=books&qid=1286915922&sr=1-1

Awards

http://www.wnlabs.com/news/Nokia_Challenge_Demo_Winner.php Nokia

http://www.wnlabs.com/news/GSC_Grand_Finalist.php Two Global Security Challenges

http://www.wnlabs.com/news/ifsec.php Raytheon

Whitenoise technologies are patented globally.