Name

A process for preventing the unauthorized or illegal use of Whitenoise encryption technologies

Abstract:

This is a process that will assure governments and law enforcement that they will be able to identify the misuse and unauthorized use of Whitenoise technologies and in particular Whitenoise super key encryption.

Need

There is a particular need to assure legitimate governments and law enforcement that the use of Whitenoise technologies does not threaten or impede legitimate law enforcement mandates.

TECHNICAL FIELD

The invention relates to the field of security for electronic communications and in particular secure communications using dynamic distributed key infrastructures and Whitenoise super key encryption.

Description

BACKGROUND

The most widely used method for providing security online for authentication and encryption is using asymmetrical encryption systems of the public key design where authentication relies on certificates issued by certificate servers. Public Key Infrastructure (PKI) systems have known security vulnerabilities such as being susceptible to Man-in-the-Middle [MiM] attacks, because they are often implemented improperly and because public keys are always available for factoring and because there is always key transfer to initiate a session.

The overhead of the PKI system is high, not just because of all the steps involved in the architecture, but also their choice of cryptography. The key strengths used by the PKI have been called into question recently. Public keys are compound primes and they are always available for attack. There have been significant strides in prime numbers and factoring theory. New techniques exist to factor compound primes. Fast computers factor compound primes by simplified techniques like the “sieve” method, so what used to take years now can be done in hours. Using progressively stronger keys with public key systems becomes progressively more difficult because of the additional computational overhead introduced as keys get stronger (longer). Additionally, with the advent of quantum computing all public keys will be easily factored and broken because of fixed key sizes.

SUMMARY

The security of all crypto systems, whether asymmetric or symmetric, is determined by key management, key distribution and exchange, key storage, and the nature of the keys, and how the keys are used.

In this summary, we will look at a specific case contending with the potential illegal, unauthorized use of Whitenoise in communications and on the internet. This embodiment uses **Whitenoise Super keys (patent: Boren Brisson 10/299847 granted)** or other exponential, one-time-pad keys for additional key generation (and for all security functions including encryption), the encryption function may be accomplished with any deterministic random (pseudo random) data source and any encryption algorithms.

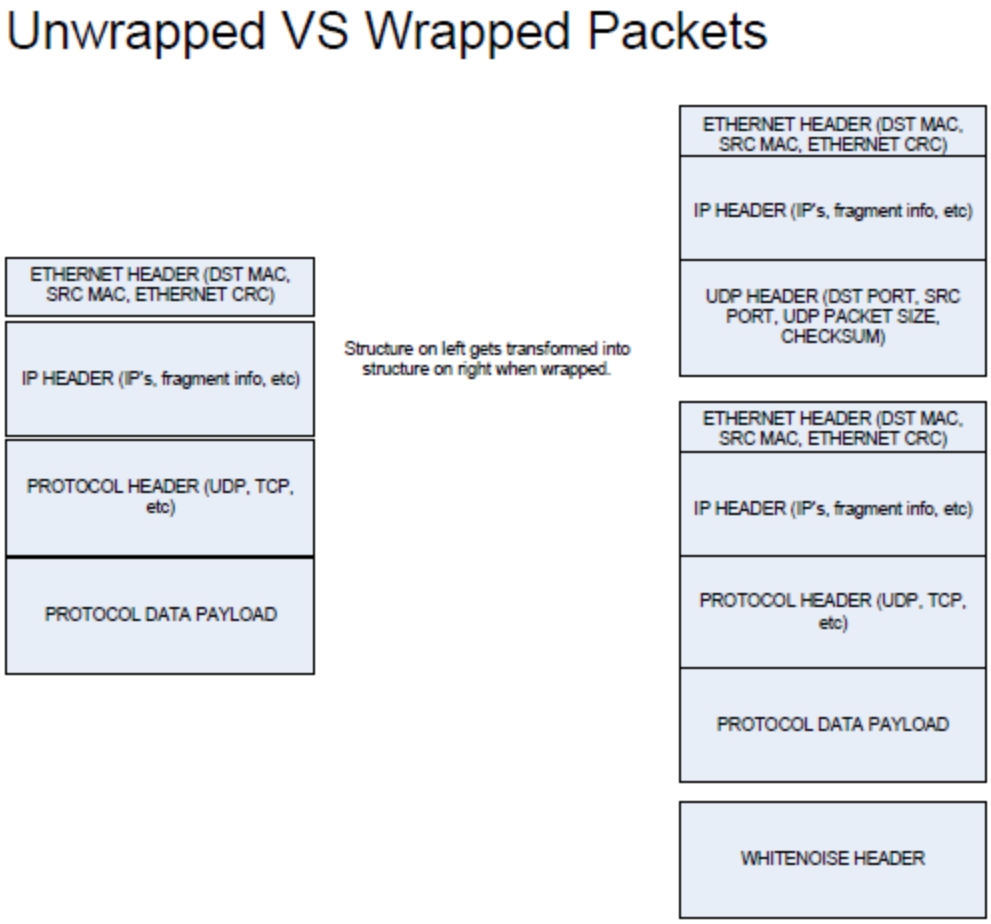
A preferred embodiment, but not restricted to this, is using a cloud or hybrid cloud operating system or platform as described in patents by **Timothy S. Vasko** **Application number:** 20130297371 and **Application number:** 20130132860 as deployed with a platform such as 1to1Real.

The following embodiments and aspects thereof are described and illustrated in conjunction with systems, tools and methods which are meant to be exemplary and illustrative, not limiting in scope. In various embodiments, one or more of the above-described problems have been reduced or eliminated, while other embodiments are directed to other improvements.

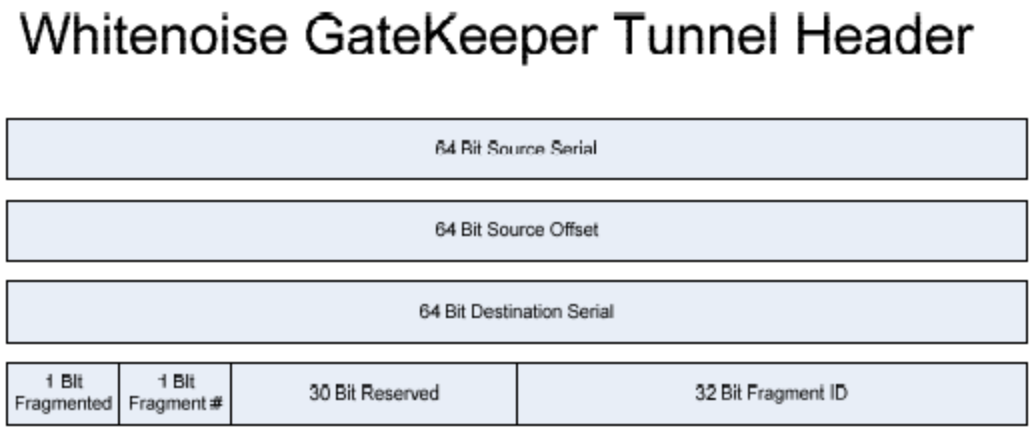
BRIEF DESCRIPTION OF DRAWINGS

Exemplary embodiments are illustrated in referenced figures of the drawings. It is intended that the embodiments and figures disclosed herein are to be considered illustrative rather than restrictive.

FIG. 1 illustrates how an identifier can be appended to authorized Whitenoise users.

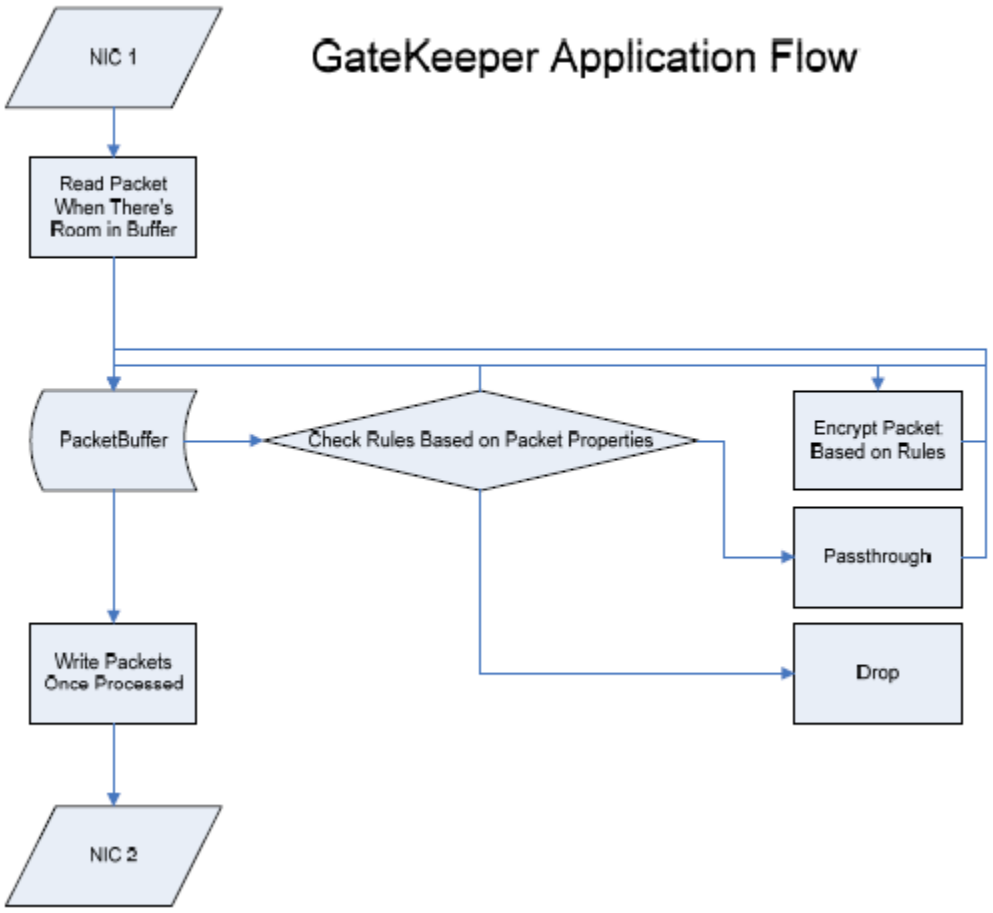


63 FIG. 2 illustrates a Whitenoise packet header



64

65 FIG. 3 illustrates an application flow



66

Throughout the following description specific details are set forth in order to provide a more thorough understanding to persons skilled in the art. However, well known elements may not have been shown or described in detail to avoid unnecessarily obscuring the disclosure. Accordingly, the description and drawings are to be regarded in an illustrative, rather than a restrictive, sense.

Whitenoise super key encryption is exponentially stronger encryption than any cryptographic key algorithms known creating keys of unlimited strength and length.

Whitenoise encrypted data has two distinct characteristics that enable this invention.

Bit independence means that any bit of encrypted data is not related to any other bit in the cipher text, particularly preceding bits in cipher text to which most encryption algorithms are dependent and which create patterns that are used to create cribs and for other hacking cyrptanalytical techniques.

A second singularly unique characteristic is that it creates the most random data known. Measuring a sample of radioactivity has been the historic benchmark of randomness. Randomness is foundational to cryptographic sciences and doing effective quantum computing.

Whitenoise cipher text is orders of magnitude more random than radioactive decay and as such is easily recognizable by simple testing in communications.

Use of this technology should have the legitimate approval of governments.

Process

i) An identifier using a Whitenoise key is appended to a packet header. This doesn't impede normal routing in communications and the Internet.
ii) An approved device, server, router is enabled with a capability which allows testing of the randomness of transmitted communications to determine whether it is more random than radioactive decay and location of legitimate use identifiers in the header.
iii) If the test for randomness determines that it is more random than radioactive decay then it is Whitenoise.
iv) If it is cipher text from a legitimate key communications continue and privacy of the communications has not been compromised.
v) If it is not identifiable as cipher text data from a legitimate, authorized Whitenoise key source then this unauthorized transmission is encrypted a second time with a law enforcement approved unique Whitenoise key and passed forward.
vi) The illegal communications is unreadable at the receiver end.

It is important to note that this technique has NOT violated the privacy of the actual communication. The communication has not been read or opened.

In use, ordinary citizens who might be using such an encryption algorithm and gets an incorrect evaluation (false positive) and experiences interrupted communications will contact system administrators and the problem would be rectified.

Criminals tend to not want to identify themselves and hence won't report that they were unable to open their communications in this legitimately authorized denial of service to criminal communications.

It is possible to collect Meta data and other legally obtained identifiers like IP addresses for forensic purposes.

Law enforcement and other duly authorized surveillance entities have the assurance that criminals will be forced to use obsolete and breakable cryptographic technologies that are currently used today.

This invention is an ability of Dynamic Distributed Key systems. Although secure and unbreakable, law enforcement is not impeded in legally mandated activities because in dynamic distributed key systems the server has identical copies of all the keys that are on a system while each endpoint or user has only their unique, distributed, exponential, private, secret key.

There are no public key infrastructure elements.

Claims

1. A method of preventing the unauthorized and illegal use of Whitenoise encryption technologies comprised of the following steps:

    i) An identifier using a Whitenoise key is appended to a packet header and which doesn't impede normal routing in communications and the Internet.
    ii) An approved device, server, router is enabled with a capability which allows testing of the randomness of transmitted communications to determine whether it is more random than radioactive decay and location of legitimate use identifiers.
    iii) If the test for randomness determines that it is more random than radioactive decay then it is Whitenoise.
    iv) If it is cipher text from a legitimate key communications continue and privacy of the communications has not been compromised.

v) If it is not identifiable as cipher text data from a legitimate, authorized Whitenoise key source then this unauthorized transmission is encrypted a second time with a law enforcement approved unique Whitenoise key and passed forward.

vi) The illegal communications is unreadable at the receiver end.