Whitenoise-DIVA-DDKI Usage Scenarios

Whitenoise, Dynamic Distributed Key Infrastructures and Dynamic Identity Verification and Authentication are very flexible and can be configured in many different ways to achieve different goals. All these usage scenarios can readily be seen on the Whitenoise technical web at:

http://www.wnlabs.com/home.php

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

Usage scenario for securing the Internet of Things 1

Usage scenario for securing the cloud, colossal data and data centers 1

Usage scenario for preventing identity theft on the web and through browsers and Authentication as a Service 2

Usage scenario for keyMail 2

In a perfect world scenario for banks, the banks would control all the keys and their clients Usage scenario for banks and financial services 3

Usage scenario for secure media and streaming services 3

Usage scenario for securing biometrics and managed, mobile, adaptive secure networks 3

Usage scenario as a failsafe for quantum cryptography and computing 3

Usage scenario in microprocessors and PICs 4

Usage scenario for securing the Internet of Things

This is a market that incumbents like RSA cannot effectively go to because of their technology. Asymmetric, public key systems require a lot of power, storage and computational overhead.

Internet of Things is estimated to be a $19 trillion vertical. Early entry here means we would have a massive niche where we would not have to compete head to head with incumbents because they do not have usable technology in this area.

http://www.wnlabs.com/pdf/Internet_of_Things_and_Whitenoise_Technologies.pdf

Usage scenario for securing the cloud, colossal data and data centers

Securing big and colossal data, and data centers, as well as securing large volumes of data before upload into the internet cloud, requires a very fast encryption and authentication crypto algorithm. There is no reason why data centers should not be retaining data in a secure encrypted manner other than speed and volume and who manages the keys.

Whitenoise-DIVA-DDKI Usage Scenarios

Dr. Rivest, one of the founders of RSA, announced an improvement on an algorithm at a talk at Charles Rive Cyber 2014:

"We estimate that Spritz can produce output with about **24 cycles/byte** of computation. (sic **1 byte per 24 clock cycles**). Furthermore, our statistical tests suggest that about 2^{81} bytes of output are needed before one can reasonably distinguish Spritz output from random output; this is a marked improvement over RC4."

Alternatively, Whitenoise can produce output with about **2 bytes per clock cycle computation**. And that is scalable. That is orders of magnitude faster than Spritz (minimum 48 times faster) with virtually no overhead or computational requirements. This illustrates exactly why RSA technologies and asymmetric processes are not a good choice for securing data centers and big data. This illustrates exactly why RSA cannot effectively deploy even 128 bit keys in the majority of devices that comprise the Internet of Things and the Cloud of Things.

http://www.wnlabs.com/papers/Nokia_SV_Open_Innovation_Challenge_WNL.pdf

Usage scenario for preventing identity theft on the web and through browsers and Authentication as a Service

The telecom DoCoMo makes a quarter of its profits from self running, third party authentication services. Companies like VeriSign are providing a level of authentication with their certificate based services. Whitenoise technologies can provide a far superior level of authentication and identity management in a far simpler manner that can be accomplished in real-time.

This is the generic capability that allows Dynamic Identity Verification and Authentication to be deployed in any environment and has browser specific plug-ins.

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

Usage scenario for keyMail

A Whitenoise key can be associated with an email account and used in an email filter to authenticate and authorize emails that will go through or which are stopped at the server.

Whitenoise-DIVA-DDKI Usage Scenarios

Usage scenario for banks and financial services

In a perfect world scenario for banks, the banks would control all the keys and their clients would never even have their own private key. In this fashion the banks would be assured that their clients could not have their private keys stolen when their credit cards are stolen, as an example. Their clients could not give their keys away.

This can be done in a single key, token system as described here:

http://www.wnlabs.com/Presentations/Stop_Credit_Card_and_Identity_Theft.pps

Usage scenario for secure media and streaming services

Speed and the ability to impose identity and provenance to high speed-high volume data allow us to effectively apply Digital Rights Management. This enables secure streaming of entertainment content, video surveillance, and high volume satellite data capture and delivery.

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

Usage scenario for securing biometrics and managed, mobile, adaptive secure networks

Currently when a person's biometric identity is stolen they are theoretically compromised for their entire lives because they can't change their biology. It is possible to turn a biometric into a one-time-pad to eliminate this problem. If a person's biometric were stolen, then all that is needed is to change the DIVA key and offset associated with it.

http://www.wnlabs.com/downloads/Gartner_Video.mp4

Usage scenario as a failsafe for quantum cryptography and computing

Quantum cryptography and quantum computing require a perfectly random data source so they can effectively solve NOT problems. They need an algorithm to create keys which are then used to encrypt quantum elements.

Because of the instability of quantum, denial of service cannot be prevented. The quantum techniques provide a great intrusion detection capability but the quantum components cannot be shielded from outside physical and quantum effects.

Because of this, a “fail safe” algorithm that can run as fast as quantum in any hardware environment is needed in order to have the capacity to switch over to more traditional crypto, albeit one that moves at extraordinary speeds, during situations where the quantum crypto is shut down because of denial of service attacks. This was presented to the European Telecommunications Standards Institute.

Usage scenario in microprocessors and PICs

Natural points of deployment for Whitenoise technologies are the same as where national security strength cryptography is monitored and regulated: the place of provision of communications and the place of manufacturing of devices utilizing cryptography, generally through chips sets and/or firmware.

RSA and current asymmetric cryptographic technologies are poor if not impossible choices for this usage. Chip manufacturers like Intel are currently struggling and trying to make obsolete algorithms and processes faster in microprocessors by altering the process as we find in AES NI (new instructions) which offloads some of the more intensive mathematical processes to the chip in an effort to gain speed. And yet, they still need crypto accelerators and more resources in high volume situations.

All the above scenarios presented are performed in software which for Whitenoise technologies operate at the same speeds as those found in hardware because of the utilization of X-Or – it moves as fast as the hardware allows.

Whitenoise technologies are the only national security cryptography that is simple enough to deploy in PICs, **Peripheral Interface Controllers**, which are the cheapest microprocessors available and which can be found in devices as simple as dolls and inexpensive children’s toys.