RSA Conference 2016

Dynamic Distributed PKI – Canadian Ontario Trade Mission

Existing security networks are easily transitioned to secure distributed PKI with the Unified Whitenoise dynamic, distributed, lockless PKI and web servers that are up to 800% faster than Apache and NGINX. Lockless programming allows multi-thread and parallel processing access to data concurrently for significant speed gains and increases in performance, efficiency and reliability. These are very simple to benchmark and do speed comparisons.

PKI on its own cannot provide complete network security. It has always been vulnerable to man-in-the-middle attacks. It is now vulnerable to many more attack classes and it is too easy for keys simply to be stolen. This is why PKI is evolving to utilize block chains with the aim of providing a distributed, unalterable ledger of information. This is a step in the right direction but block chain is inefficient. Whitenoise inherently accomplishes this with the imposition of data provenance with unique, authenticated encryption.

Dynamic Distributed Key Infrastructures, Dynamic Identity Verification and Authentication and Whitenoise **(patented globally)** are a virtual framework and virtual protocol add-on that eliminates security flaws associated with PKI. Together with PKI, they provide a two-channel (asymmetric and symmetric calls), multi-factor, continuous, dynamic authentication and authenticated encryption that imposes data and user provenance. The hacker now has a challenge where two keys have to be broken simultaneously in seconds for each breach and one key is a dynamic, one-time-pad.

About Whitenoise

whitenoise technologies

Encryption and dynamic authentication

A single distributed master key creates an unlimited number of unique and unbreakable keys that are given to all persons, mobiles and components on your network which are then continuously monitored and authenticated.

Security as a Service is a platform for SML businesses and general consumers. You can build a fast, economical, virtual, secure network server where you will be able to choose and customize secure services to protect your mobile and enterprise communications, privately stream data, secure cloud storage, secure data transfer and have 7 X 24 identity management and network monitoring. You decide whether you want a managed service or whether you have the server cloned and delivered to you.

How does it work?

Both the server and the endpoint have a copy of the key in a symmetric system. These keys are unique, deterministic random number generators that create exponential keys that can never be exhausted and continually verifies identity by the one time use of moving tokens. Dynamic Identity Verification and Authentication (DIVA) prevent all known cyber attacks and perform all security functions including inherent intrusion detection and automatic revocation.

The PKI keys used in the multichannel paradigm cannot be broken or stolen and used for illegal network access without detection by DIVA.

Attacks prevented

- Man-in-the-Middle attacks are prevented because there is no key exchange. Keys are pre-distributed and pre-authenticated and NEVER transmitted again. Offsets update independently.

- Side Channel attacks are prevented because all operations are order 1 after key load and because there is no access to the key. Side channel attacks exploit vulnerabilities and static implementation. The master key continues to refresh the random data in any registers, counters or chips in physical implementations.
- Mathematical and factoring attacks are prevented because keys are created by a binary mechanical process as opposed to arithmetic ones requiring multiplication and mods.
- Botnet attacks are prevented by configuration with server so the botnet never has access to all the key material to authenticate data being sent OUT of a network or computer.
- Brute force attacks are not feasible with the continually changing dynamic offsets.
- Denial of service attacks can be prevented by exploiting unbreakable identity and a proxy for secure network access so that hackers could never get on a network.
- Quantum computing attacks are prevented because every variable is dynamic.

Key characteristics

Both the server and the endpoint have an identical copy of the key. The server continually has the endpoint identify itself by sending tokens that are compared bit by bit. If they are identical, the session continues and both the server and endpoint update their current offset by jumping ahead in the keystream by the length of the token plus one. No keys have been transmitted and the server and the endpoint are synchronized.

- The key is a unique, exponential, deterministic random number generator (DRNG) data source.
- The Telco or service provider receives a master key (MRNG).
- The Telco can make an unlimited number of client account keys and distributes them to their customers or network endpoints one time.
- The unique, private, account keys create key streams of unlimited length and are deterministic RNG themselves. (Key structure storage requires little space.)
- The unique, endpoint, distributed, private keys create an infinite number of unique one-time-pad tokens (small key subsets) from that one-time-distributed key.
- We know where each key-based cryptographic call or control is being called from in the key stream by tracking current dynamic offsets. We track different current dynamic offsets which are pointers or indexes into the key stream for each different, key based, network security control.
- The keys and tokens can be of ANY bit strength.
- Smaller tokens for authentication can be safely used because DIVA operates as a dynamic, continuous, one-time-pad.
- Because the keys are unique they provide authenticated encryption for storage or transmission with provenance and identity.
- Because keys use the fastest function available on computers it is always as fast as the hardware.
- Because the keys are bit independent they can be parsed for secure key storage separating key structure and offsets.
- We can use the same key for any use endlessly because the keys are deterministic and of infinite length.

About Unified Software Technologies

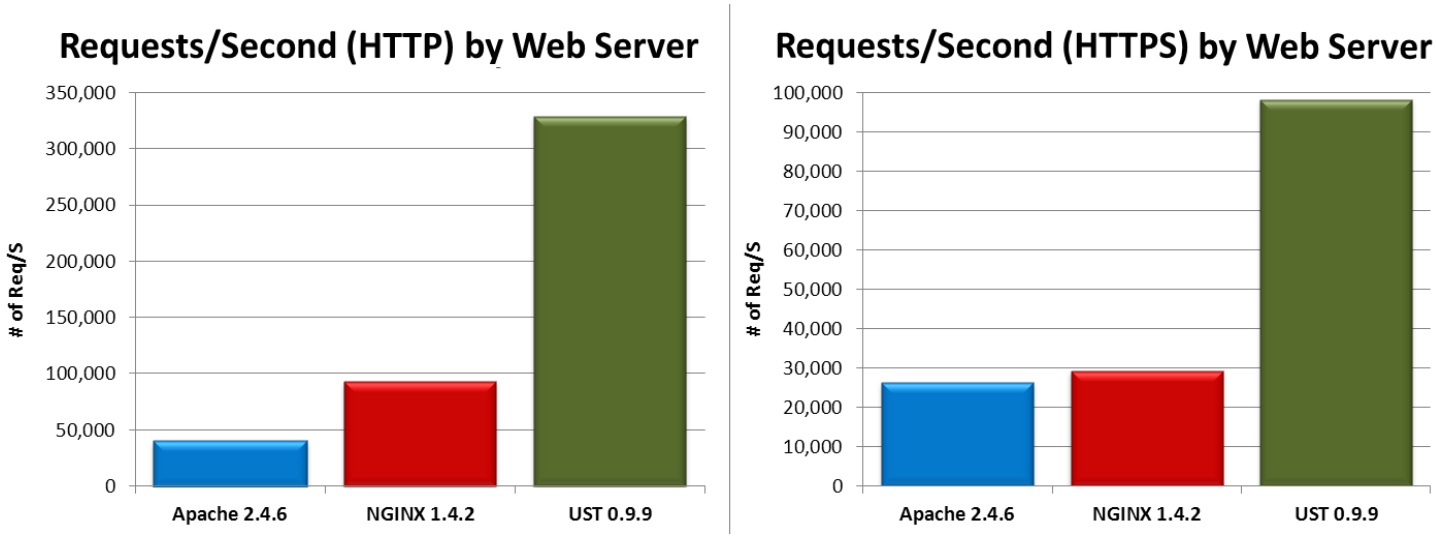
Unified Software Technologies™ (UST) is a software company specializing in parallel and high-performance computing technology. UST is now offering its breakthrough and patented solutions to boost the processing capacity of your existing Web infrastructure by a factor of approximately 4x to 8x, and efficiency by 3x to 4x.

UST's Speed™ Web and Application Server

UST™ has developed the Speed™ web and application server. Speed™ offers dramatically higher transaction rates than competing products. Achieving greater transaction volume with existing infrastructure delivers substantial cost savings while improving service capacity without costly infrastructure upgrades and expansion.

As the need to improve energy efficiency rises, your hardware and software strategies should go hand-in-hand. A simple upgrade from Apache or NGINX to the UST™ Speed™ web and application server dramatically improves the performance, stability and efficiency of your web based infrastructure and services.

As an example of UST's competitive advantages, UST's Speed™ web server delivers secure (HTTPS) content faster than NGINX is able to deliver non-secure (HTTP) traffic.



Speed™ is fast. The UST web server provides factors of 4x – 8x greater throughput than NGINX and Apache, respectively.

These advantages help businesses to grow with new market opportunities, and allow data center operators exceptional cost savings opportunities.

Speed™ is fully compliant with industry standards including IETF HTTP, SSL / TLS, and Fast CGI, ITU X509, and W3C XML. UST is offering the Speed™ web server for release on Linux x86 and x64 platforms and will be offering versions for Windows, and BSD operating systems and ARM based hardware soon.

Editions are available for platforms from enterprise, cloud, mobile, embeddable, and IoT platforms.

Data Center, Cloud, XaaS, Virtual, and Internet of Things based web application and service providers will best leverage their IT investments by incorporating the Speed™ web server into their technology stack.

Speed™ is available for end-users and for licensing within third party hardware and software products.

Unified Software Technologies is a strategic partner of Whitenoise Labs.