RSA Conference 2016

Dynamic Distributed PKI – Canadian Ontario Trade Mission

"In August, 2015, NSA announced that it planned to transition in the not distant future to a new cipher suite that is resistant to quantum attacks. Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, necessitating a re-evaluation of our cryptographic strategy." wiki Integer Factorization Cryptography(RSA), AES, and ECC are all seriously downgraded on security strength. It is a simple upgrade to address this security threat with a one-time-pad Dynamic Identity Verification and Authentication (DIVA) WN-SSL-TSL add-on.

Existing security networks are easily transitioned to secure, dynamic, distributed PKI with the Sequor Systems LLC lockless programming and the Whitenoise-SSL-TLS extension for openSSL PKI. Web servers ramp up to 800% faster speeds 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. Dynamic, distributed PKI has also been referred to as one-time-pad-PKI - OTP-PKI.

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 attack classes and it is too easy for keys simply to be stolen. Whitenoise thwarts attacks by 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 user identity and data provenance. The hacker now has a challenge where two keys have to be broken simultaneously 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?

The software generates 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 public or private 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 during a session. Keys are pre-authorized and predistributed.
- Side Channel attacks are prevented because all operations are order 1 after key load and because there is no access to the key. The master key also keeps refreshing the data in the counter, chip, register etc. so it is never reusing any key portion.

- 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
- Quantum computing attacks are prevented because every variable is dynamic and because it operates as a one-time-pad.

Key characteristics

Both the server and the endpoint have an identical copy of the key. The key has already been pre-authenticated and predistributed. 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 key length.

- The key is an exponential deterministic random number generator (RNG) data source.
- The Telco or service provider receives a master key (RNG).
- The Telco can make an unlimited number of unique 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 Sequor Systems, LLC

Sequor Systems, LLC has patented technology that provides important advantages in software development, performance, efficiency, reliability, capability, and cost.

Sequor's patented innovations in lock-free programs are available through Sequor's Edge™ Lock-free SDK and Sequor's Speed™ web and application server. Lock-free programming allows multi-thread and parallel processing access to data concurrently.

- Performance – Sequor delivers a performance improvement of up to 800% with your web applications and up to 500% with the rest of your technology stack.

- Efficiency - Sequor's technology delivers dramatic improvements in efficiency and provides important energy saving opportunities through server and equipment consolidation. Sequor's technology can also be used to increase battery life in embedded and mobile device applications.

- Reliability - Coding on multi-core architectures can be tedious, error-prone, and expensive. Sequor's lock-free technology eliminates hard to fix bugs due to software synchronization problems and makes coding optimized, multi-threaded software as easy and inexpensive as coding single-threaded systems. Systems leveraging Sequor's technology are more reliable and this is especially important in mobile and embedded and Internet of Things applications.