Securing Network Communications

SEQUOR SYSTEMS

Demonstration:

Securing network access with Whitenoise Labs identity management, one-time-pad dynamic authentication, and one-time-pad authenticated encryption.

Use of Whitenoise Labs technology with existing PKI software via standard TLS extension mechanisms.

Introduction

Subject Matter Covered in this Presentation

The purpose of this presentation is to introduce Whitenoise Lab's security technologies and demonstrate a proposed extension to the IETF Transport Layer Security (TLS) protocol that utilizes the enhanced peer authentication and data protection provided by Whitenoise. This extension is in compliance with the generic extension mechanisms of the IETF RFC 6066 for a TLS handshake.

Whitenoise Labs' Dynamic Identity Verification and Authentication (DIVA) and Dynamic Distributed Key Infrastructures (DDKI) are globally patented security technologies that provide unbreakable encryption while imposing identity of all endpoints and provenance of all data.

The server portion of this demo is running web server software developed by Sequor Systems. Sequor has developed the world's fastest PKI/TLS web server software based upon its' patented lock-free algorithms.

The demo web server is hosted on a server provisioned by Green House Data at their Tier III data center in Orangeburg, New York.

Definitions and References

Terms, Definitions, and Normative References

Definition of Terms:

- PKI – Public Key Infrastructure as defined in ITU-T X.509
- IETF – Internet Engineering Task Force
- W3C – World Wide Web Consortium
- TLS – Transport Layer Security
- SSL – Secure Socket Layer
- DDKI – Dynamic Distributed Key Infrastructure
- DIVA – Dynamic Identity Verification and Authentication
- ITU-T – International Telecommunication Union-Telecommunication Standardization

Normative References:

- X.509 – Defined in ITU-T Public-key and attribute certificate frameworks
- TLS – Defined in IETF RFC 6066

About the Authors

About Whitenoise Labs and Sequor Systems

Whitenoise Labs (WNLabs) is a technology company specializing in network security. WNLabs has developed a novel and breakthrough approach to creation, deployment, and management of one-time-pads (OTP).

WNLabs technologies are globally patented and are based upon over 10 years of development and have been validated by leading experts in the field.

Sequor Systems (Sequor) is a technology company specializing in the application of lock-free algorithms. Using its novel and patented technology, Sequor has developed the world's highest performing, most efficient, and most resilient web and application server software available.

Sequor has developed a TLS extension for its web and application server product that incorporates WNLabs unbreakable dynamic, continuous verification and authentication technology.

Network Security Challenges

Challenges Facing Network Security

With advances in computing technology, and in particular quantum computing, attacks are rapidly becoming an existential threat to mathematical or arithmetic-based cryptography. Successful attacks already exist for all cipher algorithms within Suite B (including RSA, ECC & AES). The TLS-DIVA integration described in this paper prevents these attacks by enciphering critical aspects of TLS protocol messages with Whitenoise Lab's one-time-pad technology.

Loud warning from NSA and NIST

NSA is moving away from ciphersuite B because it is not secure against quantum computing attacks.

“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.”

Whitenoise Labs

Making One Time Pad Technology Practical, Reliable, and Manageable

WNLabs innovations in one-time-pad technology make the use of OTPs practical, reliable, and manageable. Dynamic Identity Verification and Authentication (DIVA) is a protocol that utilizes Whitenoise keys (DRNG) as a one-time-pad.

Dynamic Distributed Key Infrastructures (DDKI) is a security framework of devices and persons with DIVA. It may be used within existing PKI network frameworks to fix PKI vulnerabilities.

- The key data source is an exponential deterministic random number generator (DRNG).
- Client entity receives a UNIQUE master key (DRNG).
- The entity can make an unlimited number of client account keys and distribute them to their customers or network endpoints one time.
- The unique, private account keys create key streams of exponential 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 within the key stream by tracking current dynamic offsets.

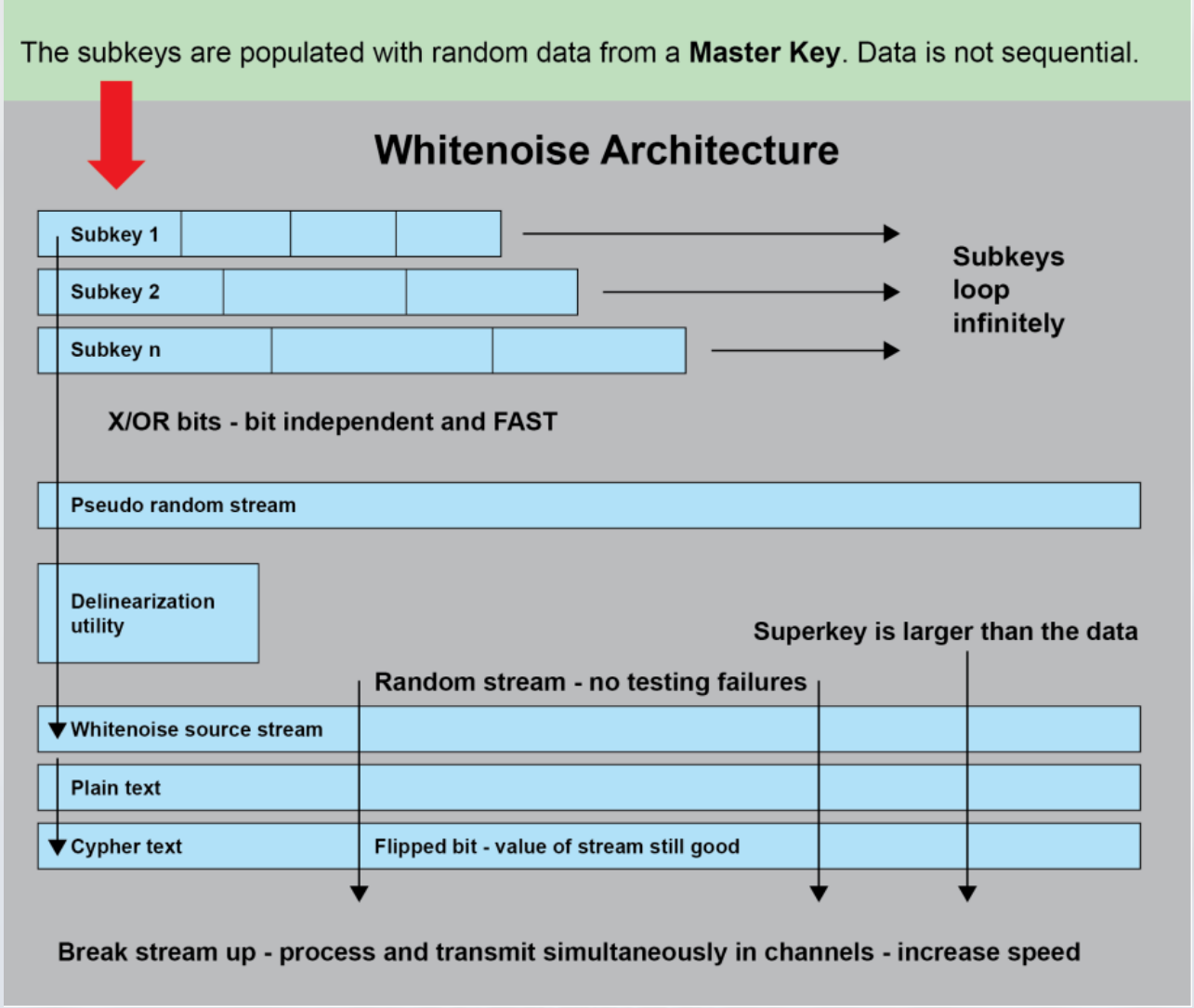
How it Works

White Noise Labs DIVA, DDKI and One-Time-Pads (OTPs)

The key data source is an exponential deterministic random number generator (DRNG).

An entity can make an unlimited number of client account keys and distribute them to users network end points one time.

The distributed private keys create an infinite number of unique one-time-pad tokens (small key subsets) from the one-time distributed key.



Applications of Whitenoise

Applications of Whitenoise Technology in Distributed Platforms

Whitenoise solves key problems in securing distributed systems:

Key storage

Because of the exponentialism of DIVA Identity Management and network security keys, a small key structure generates a large, random, deterministic key stream. Just 158 bytes of stored key structure information creates a key stream greater than 100 billion bytes long.

Key management

Historically the number of keys to manage is the square of the number of secure endpoints on a network. A ten endpoint secure distributed network would require managing 100 keys. Whitenoise does not have this requirement.

Key distribution

Whitenoise allows distributed keys to be used to securely generate and distribute more encrypted keys. Keys are distributed using ISO/ITU Level 4 identity proofing for person and nonperson entities. Keys cannot be stolen at enrollment without being detected.

Whitenoise Labs – Features

Features of Whitenoise One Time Pad Technology, DIVA and DDKI

The Whitenoise technology is a unique identity management, authentication and encryption system that generates effectively infinite length one-time pad (OTP) keys from a much smaller user key.

The nature of the OTP key makes it unbreakable by all currently known cryptographic techniques and supports user authorization, continuous verification, and network intrusion detection. Features include:

- Simple to deploy
  - One-time key download from server.
- Efficient
  - Little power consumption, fully supports mobile and IoT devices
- Friendly
  - No additional passwords for users to remember.
- Easy to Implement
  - No additional hardware, low cost to implement
- Secure
  - Not susceptible to quantum, man-in-the-middle, side channel, or bot-net attacks.

Whitenoise Labs – Benefits

Benefits of Whitenoise One Time Pad Technology, DIVA and DDKI

WNLabs' technology provides identity management, continuous verification and authorization, and encryption capabilities. Its unique design and functionalities are ideal in securing networks against a variety of common attack vectors used in PKI based systems.

Whitenoise may be used in place of or to supplement PKI installations. Benefits include:

- Instant intrusion detection and automated revocation
- Secure network access and secure identity management
- Multi-channel multi-factor authentication
- Continuous authentication in-session
- Data provenance with unique authenticated encryption
- Eliminates attack vectors including man-in-the-middle, spoofing, replay, and others

Sequor Systems – TLS Extension

Web and Application Server with Whitenoise TLS Extension

TLS-DIVA is a proposed extension to the Transport Layer Security (TLS) protocol to provide support for the enhanced peer authentication and data protection provided by Whitenoise Lab's DIVA, in compliance with the generic extension mechanisms of RFC 6066 for the TLS handshake.

TLS-DIVA is a product of collaboration between Whitenoise Labs and Sequor Systems developed by Mr. Laurie Perrin. It is intended to provide the basis for further development into an IETF standard. Following owner revisions it will be offered for public review.

The goal of the proposed extension is to enhance the security provided by the transport layer security (TLS) protocol with the authenticated encryption provided by Whitenoise Lab's DIVA security platform.

TLS-DIVA Extension

Whitenoise Labs and Sequor Systems TLS-DIVA Extension

The WNL DIVA cryptographic system provides unbreakable security by virtue of its operation as a one-time-pad. Modifying TLS to encipher session particulars with DIVA augments TLS security with dynamic client and server identity validation.

Support for DIVA integration with current and future versions of TLS enhances transport security by requiring an additional secret known only by the client and server. Knowledge of this secret establishes the trustworthiness of both connection endpoints.

TLS security may be further enhanced by incorporating WNL DIVA at the TLS ciphersuite level. By integrating DIVA in this way, successful encryption and decryption of exchanged data is contingent upon knowledge of the DIVA particulars. This requirement conveys the important advantage that any compromise in the TLS session key does not, on its own, permit successful decryption of the session data.

How TLS-DIVA Works

TLS-DIVA Extension Operation

To learn how the TLS DIVA works please review the following presentation and document:

Fort Meade How DIVA works
http://www.wnlabs.com/pdf/Cyber_Belt_Presentation.pdf

TLS extension specs and implementation
http://www.wnlabs.com/pdf/WNL-DIVA-TLS-Extension.pdf

Demonstration Video

OpenSSL Client connecting to Web Server via HTTPS using TLS-DIVA Extension

Please see on-screen for live demo.

https://drive.google.com/file/d/0B_YZK_4kDij7N1BHWjVuY2Radmc/view

Summary and Contact Details

Whitenoise Labs and Sequor Systems

This presentation has demonstrated secure network encryption and continuous, dynamic authentication through a Transport Layer Security (TLS) compliant extension using Whitenoise Labs security technologies.

Networks and PKI can be secured *even against quantum computing attacks* with a simple software upgrade. Key distribution and federation is a simple one-time process.

The technology can be offered as Security-as-a-Service; once configured no key exchange or transfer is required and networks are secured.

For more information please contact:

Mr. André Brisson, Director of Business Development
Telephone: 604-724-5094
Email: abrisson@wnlabs.com
Online: www.wnlabs.com

Attachments

Subject Matter Covered in this Presentation

Whitenoise Laboratories

Whitenoise Labs' Dynamic Identity Verification and Authentication (DIVA) and Dynamic Distributed Key Infrastructures (DDKI) are globally patented security technologies that provide unbreakable encryption while imposing identity of all persons / endpoints and provenance of all data. Whitenoise Labs delivers unbreakable authentication and encryption to public key infrastructure. These features may also be added within existing PKI and SSL/TLS infrastructure.

Sequor Systems

The server portion of this demo is running web server software developed by Sequor Systems. Sequor has developed the world's fastest PKI/TLS web server software based upon its' patented lock-free algorithms. In fact, Sequor's web server processes HTTPS (secure) traffic faster than other web servers process HTTP (normal) traffic. The demo web server is hosted on a server provisioned by Green House Data at their Tier III data center in Orangeburg, New York.

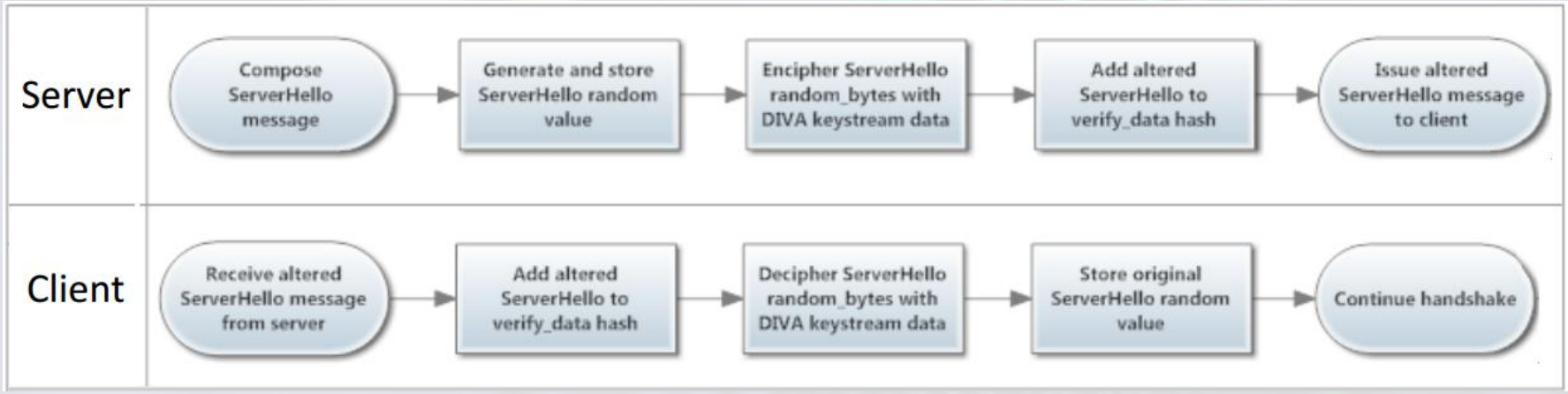
Attachments

TLS-DIVA Extension Overview

In order to support DIVA, a TLS implementation extends the specification as follows:

The server constructs and records the value of the ServerHello random field as described in TLS, however the value issued to the client is first enciphered by mixing the **random_bytes** sub-field with DIVA keystream data.

The client then uses the details provided by the DIVA extension of the (extended) **ServerHello** to compute identical keystream data for deciphering the original **random_bytes** value.



Attachments

Employing DIVA with TLS Ciphersuites

Support for DIVA dynamic authentication and continuous encryption within TLS can be achieved by incorporating the DIVA keystream into the encryption and decryption performed by a TLS session's selected ciphersuite.

Ciphersuites belong to one of three categories:

- chain-block (CBC) ciphers such as AES [AES];
- stream ciphers; and
- authenticated-encryption-and-data (AEAD) ciphers

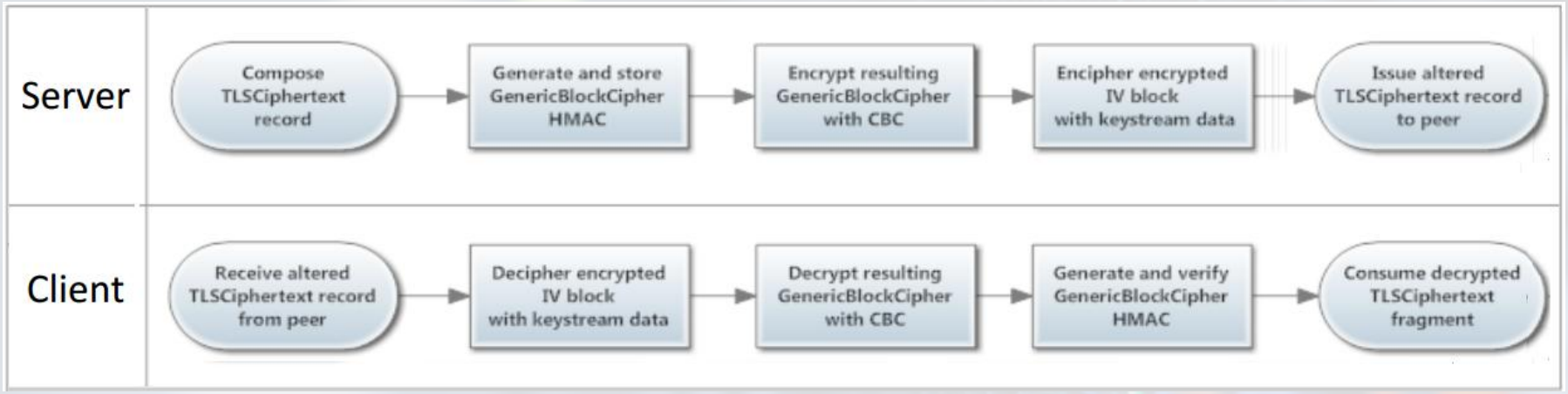
TLS mandates support for one particular chain-block cipher, namely **TLS_RSA_WITH_AES_128_CBC_SHA**.

Attachments

TLS-DIVA Support in CBC Ciphersuites

A TLS chain-block cipher assembles plaintext content and a message authentication hash [HMAC] into a **GenericBlockCipher**.

As of TLS 1.1 this construct includes an explicit **IV** (initialization vector) field, into which random data is assigned. The resulting **IV** becomes the first encrypted block of the block-chain. The number of bytes in the **IV** is identical to the particular cipher algorithm's cipher-key length.



Successful CBC deciphering requires the correct **IV** block, otherwise the ciphersuite will report an error resulting in a fatal alert having a "decrypt_error" alert description.