The 14th IEEE Conference on Advanced and Trusted Computing (ATC 2017)

August 4-8, 2017, San Francisco Bay Area, USA

IEEE CyberTrust workshop

Title: Enhancing Transport Layer Security with Dynamic Identity Verification and Authentication (DIVA) -Maintaining and Enhancing SSL/TLS Reliability

Laurie Perrin and Andre Brisson

Summary: This electronic document outlines an extension to the Transport Layer Security (TLS) protocol for incorporating the enhanced peer authentication and data protection provided by Whitenoise Laboratories' Dynamic Identification, Validation, and Authentication (DIVA) cryptosystem.

DIVA – client server paradigm

Earlier in this workshop we took a deep dive on the DIVA protocol.

DIVA is a highly configurable protocol. It is highly differentiated and operates as a one time pad because DIVA polls ahead in a key stream for a token that has never yet been created or used.

Client-Server – both the endpoint and server have a copy of the distributed key. One end (client or server) calls to the other to identify itself. The request is received and sent to the other party. The anticipated token for this account is created by the receiver and the token is compared bit by bit. If the tokens are identical then each end updates their current dynamic offset for this key independently by the length of the token plus one. There is no key information exchanged.

DIVA – single key for financial transaction

Another DIVA configuration approach allows the server to retain the only copy of a key.

A current dynamic offset in a key stream and the actual token it will begin are opposites sides of the same coin. The offset identifies the token and vice versa.

This configuration is used when a service provider wants to insure that a client CANNOT inadvertently give away their own key, and that their key does not reside on the endpoint like a credit card. (A thief would have to physically steal the device or card and this would be reported.)

In initiating a session the endpoint sends the next current token to the server for comparison and authentication.

At the end of the session the server sends the next token to be used at a subsequent session to the device or card.

http://www.wnlabs.com/pdf/Whitenoise_crypto_currency_mobile_payments_Tata_Innovation_2015.pdf

DIVA – at the data link layer

Another DIVA configuration approach allows the implementation at the data link layer.

An advantage of this approach is that no application even knows it is there acting as a sentry.

WN-DIVA-TLS

In order to harden and fix our global networks it is critical that the solutions are massively scalable and require only a single update.

Since the vast majority of security frameworks are asymmetric PKI there are two primary ways of fixing the security:

1. Update the cipher suites that applications use as NSA and NIST have indicated they are moving to in order to thwart quantum computing attacks and offer Whitenoise and DIVA as options for authentication and encryption.

2. Utilize the extensions provided for in PKI frameworks like OpenSSL and Microsoft LDAP/CAS to readily create secure hybrid networks.

WN-DIVA-TLS OpenSSL extension and cipher suite

In this configuration, DIVA is used as a one-time-pad not for authentication by token comparison but the token represented by the current dynamic offset is used to encrypt the Hello Message during single sign-on secure network access.

DIVA continues to authenticate the user throughout a network session in normal fashion thereafter.

The same extension technique can be used with LDAP/CAS and with that extension all of a user's Microsoft applications would be readily secured.

Video presentation by author Laurie Perris, lead author of the TLS paper.

http://www.wnlabs.com/Presentations/WN-DIVA-TLS.wmv