Dynamic Identity Verification and Authentication

In Dynamic Distributed Key Infrastructures (DIVA and DDKI)

André Brisson
Whitenoise Laboratories Canada Inc.
#701 – 1736 W. 10th Ave.
Vancouver, British Columbia Canada V6J 2A6
abrisson@wnlabs.com

Abstract—**Dynamic Identity Verification and Authentication (DIVA) is a protocol for identity management and intrusion detection. Dynamic Distributed Key Infrastructures (DDKI) is a virtual, distributed key framework of devices using DIVA. DDKI can be used in lieu of PKI. DDKI also works seamlessly with PKI to create a hybrid, secure two-channel, multi-factor system and challenge for bad actors. Hackers would have to break two keys simultaneously for each and every breach attempt and one of the keys is a distributed, one-time-pad key that is not transmitted in session.**

There is a defined need for large, dynamically authenticated, distributed platforms and services and large, distributed, on-line authentication systems where there is only partial disclosure of credentials. These are requirements necessary for secure cloud computing and securing critical infrastructures.

Keywords—DIVA, DDKI, authentication, authorization, encryption, identity, multi-factor

I. INTRODUCTION

"Technologies now exist to express scalable symmetric key authenticated encryption systems where no single trusted third party knows the final key." US National Cyber Leap Year Summit

"Robust cryptographic authentication would change the game by employing cryptographic methods which enable secure authentication without transmitting the raw credentials for validation." US National Cyber Leap Year Summit

Dynamic Identity Verification and Authentication (DIVA) is a robust, real-time identity manager and intrusion detector. Polling sections of random but determinist Whitenoise key streams that have never yet been created or transmitted is possible because of offset management. In this context it is non-cryptographic and not used to encrypt data. It provides one-time-pad authentication. (One-time-pad encryption can be done with the same key.)

Dynamic Identity Verification and Authentication (DIVA) compares segments of key stream that have never be created or transmitted. It can be used by itself to provide identity management, continuous dynamic authentication of a user throughout a session (not just at login), immediate hacking detection (the key offsets must remain in sync), and automatic denial of network access (revocation) to hackers and thieves without human intervention.

These are all significant security advancements that can be used in new and legacy topologies. The detection capacity is significant. There are no effective, real-time intrusion detection technologies that secure networks throughout entire sessions. It is simple – the offsets between the legitimate user and the server must remain in sync. It inherently detects intrusion or spoofing without human intervention.

Dynamic distributed key infrastructures [DDKI] is a network framework and dynamic identity verification and authentication [DIVA] is an identity based protocol that can be used in any digital context where dynamic and continuous authentication, authorization, revocation, repudiation, inherent intrusion detection, DRM, digital signature, secure network access and one-time-pad encryption are required. They address all security needs with a single key.

Distributed key secure systems are network topologies where network users are pre-authenticated and the keys are pre-distributed to network users. Use of distributed keys eliminates problems associated with key exchange during network sessions.

II. HISTORICAL CONTEXT

The safe exchange of keys is the challenge for electronic and digital communication. Distributed systems stagnated because key management, storage and distribution became onerous.

Networks evolved to asymmetric public key systems where session keys were created on the fly. Key storage problems were minimized by having public key databases. PKI is always vulnerable because the public keys are freely available and can be factored and because asymmetric systems are always vulnerable to man-in-the-middle attacks during key exchange.

PKI systems are complicated, expensive, and difficult to scale and implement. They eliminate the ability to be sure about the management of identity (authentication.)

Dynamic distributed key systems are a revolutionary return to the past by using solid, simple, distributed typologies. They are a revolutionary step to the future by offering all the security metrics with a single identity management key.

Historically the number of keys to manage in distributed systems was the square of the number of secure endpoints on a network. Dynamic distributed key frameworks have a one-to-one relationship between the number of keys and endpoints on a secure network.

Whitenoise creates key streams on the order of 10^{60} bytes (ten to the sixtieth power) in length. Only the internal key structure and the offset are required to recreate any key segment. This is a small amount of data for storage (i.e. 158 bytes of key structure information will generate a random key stream over 100 billion bytes long.)

Whitenoise topologies allow distributed keys to in turn securely generate and distribute more encrypted keys.

DIVA is an identity based key technology that can be used for any key based security function.

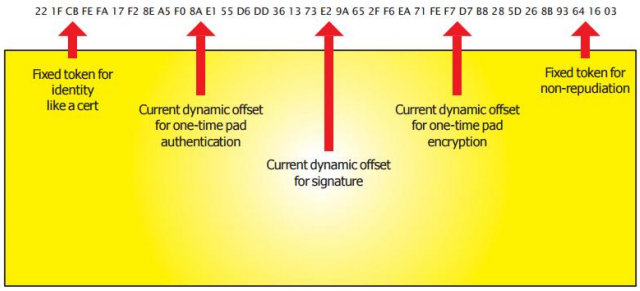
Keys are >250,000 bits in strength. The key will never be exhausted. The key structures are simple to store with a small footprint on any server or endpoint device.

Keys embed the characteristics of a one-time pad for the highest security.

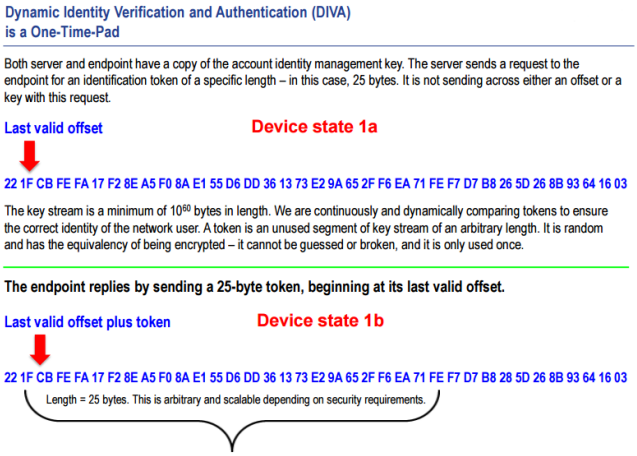
DIVA is self monitoring and requires no human intervention for intrusion detection, revocation and incident logging.

III. DIVA PROCESS

The server and the endpoint have a copy of the small key structure that creates key streams >1060 bytes long. It embeds characteristics of a one-time pad. Static tokens can be used to identify particular services and dynamic identity management tokens for authentication are never used more than once.

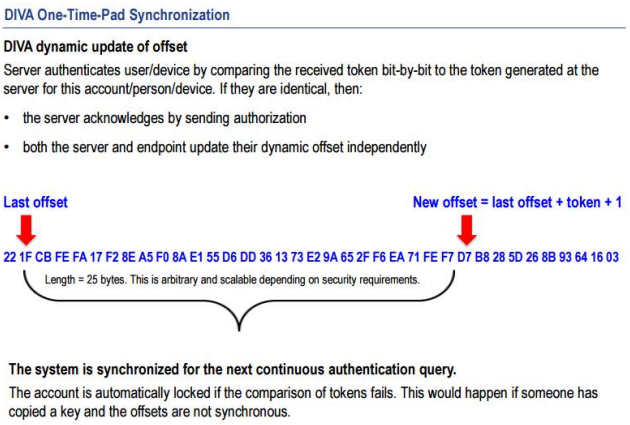


The server sends a request to the endpoint device/person for a token of a specific but arbitrary length. Neither an offset nor key is sent with this request.



DIVA and DDKI can be implemented at any level of networks all the w

The server receives the token from the endpoint and looks up the specific account. It generates a token from its copy of the key of the same length beginning at its last valid offset for that account. It compares the two tokens bit-by-bit. If the tokens are identical the endpoint is authenticated.

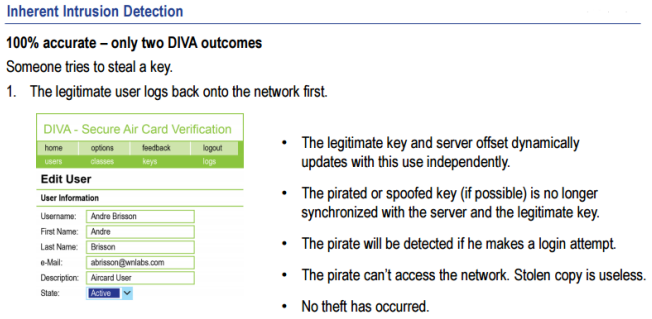


The server acknowledges the successful authentication and sends back an authorization to continue. Neither an offset nor key is sent with this authorization.

The endpoint and server update their offsets independently by advancing the offset by the length of the token just generated and compared plus one. The system is synchronized for the next request.

If the comparison fails, the account is automatically locked without human intervention.

A failed authentication call could only happen if someone was able to copy a key, and use it, prior to a legitimate network access attempt. It is a simple either/or process. The keys are either synchronized or not.



Dynamic authentication calls can be arbitrarily set according to security needs and processing contexts. For example, a call can be made with every page change in html or every five seconds if one desired.

The key structures and initial starting offset is generated by the system. The endpoint requires about 20k of memory/storage.

The look of an application interface is visually familiar to consumers i.e. user name and password. The underlying diva operates inherently and does not impact user interface.

The dynamic identity verification protocol can be deployed easily and electronically to any digital device with connectivity, storage and write back capacity. The protocol is started at single-sign-on network access and continues to do dynamic authentication throughout a network session.

In many contexts, it can operate without an interface (just inherently) i.e. machine-to-machine communications.

IV. Conclusion

DIVA and DDKI technology can be used in any digital context. They can run in parallel to public key systems; they can be integrated into public key systems; they can be used in lieu of public key systems.

It is painfully obvious from the 2016 US elections and Wiki leaks that security is under extreme duress.

The 50 largest telecoms could reach over 90% of the global population and provide secure communications and identity management.

They are well positioned to facilitate the distribution of a TLS-Whitenoise-DIVA extension for openSSL and LDAP/CAS (Microsoft) systems. An updated ciphersuite can also be distributed with this extension.

This will allow the rapid hardening of global communication systems and networks that operate critical infrastructures with a simple one-time-upgrade of servers and a simple one-time update to endpoints, devices and persons.

V. Acknowledgement

Stephen Lawrence Boren, Vancouver, British Columbia, Canada

VI. References

[1] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

[2] Albert Meyburgh, Distributed keys securely sharing session keys - http://www.wnlabs.com/downloads/Tunnel_Distributed_Keys_distributing_more_keys.pdf

[3] André Brisson Factorization of a prime number composite https://www.youtube.com/watch?v=GwkwgR_78dQ&feature=youtu.be

[4] André Brisson "Rapid Factorization of Semi Primes," http://www.wnlabs.com/pdf/Rapid_Factorization_of_semiprimes.pdf

[5] D. Wagner, "A Security Evaluation of Whitenoise," University of California, Berkeley, Oct. 2003. [Online]. Available: https://eprint.iacr.org/2003/218.pdf

[6] I. Traore and M.Y. Liu, "Evaluation of Whitenoise Cryptosystem. Part 1: Encryption Algorithm," Technical Report ECE03-3, University of Victoria, British Columbia, Canada, Feb. 2003. http://www.wnlabs.com/downloads/UVIC_Performance_Analysis.pdf

[7] A.J. Brisson,"Cyber Belt presentation for NSA/NIST 2016 – Quantum computing attack resistant security and the cyber belt." http://www.wnlabs.com/pdf/Cyber_Belt_Presentation.pdf

[8] S.L. Boren and DW (CSE), Mathematical rebuttal refuting false break technique, http://www.wnlabs.com/pdf/Response.pdf

[9] Laurie Perrin and A.J. Brisson, TLS Whitenoise DIVA extension, http://www.wnlabs.com/technology/WNL_TLS_extension.php

[10] André Brisson,"Key distribution method to shield service providers from key management - https://www.linkedin.com/pulse/key-distribution-paradigm-removes-management-from-carriers-brisson

[11] A.J. Brisson, "Factorization of a prime number composite" https://www.youtube.com/watch?v=GwkwgR_78dQ&feature=youtu.be

[12] A.J. Brisson, "Rapid Factorization of Semi Primes," http://www.wnlabs.com/pdf/Rapid_Factorization_of_semiprimes.pdf

[13] A.J. Brisson, "The Whitenoise Algorithm – A Visual Look," Technical Report, Whitenoise Laboratories, Vancouver, British Columbia, Canada, Nov. 2011. [Online]. Available: http://www.wnlabs.com/pdf/WhitenoiseAlgorithmVisualLook.pdf

[14] C. Coram-Mekkey, "Whitenoise Laboratories – An Overview," White Paper, Whitenoise Laboratories, Vancouver, British Columbia, Canada, June 2015. [Online]: http://www.wnlabs.com/papers/Whitenoise Overview Short.pdf

[15] S.L. Boren and A.J. Brisson, "Dynamic Distributed Key System and Method for Identity Management, Authentication Servers, Data Security and Preventing Man-in-the-Middle Attacks," U.S. Patent Application 2009/0106551 A1, Apr. 2009.

[16] A.J. Brisson, "Dynamic Identity Verification and Authentication, Dynamic Distributed Key Infrastructures, Dynamic Distributed Key Systems and Method for Identity Management, Authentication Servers, Data Security and Preventing Man-in-the-Middle Attacks, Side Channel Attacks, Botnet Attacks, and Credit Card and Financial Transaction Fraud, Mitigating Biometric False Positives and False Negatives, and Controlling Life of Accessible Data in the Cloud," U.S. Patent Application 2013/0227286 A1, Aug. 2013.