◂ Back to Search Results

Component: DARPA

Topic #: SB162-004

Title: Secure Messaging Platform

Technology Areas: Info Systems

OBJECTIVE: Create a secure messaging and transaction platform that separates the message creation, from the transfer (transport) and reception of the message using a decentralized messaging backbone to allow anyone anywhere the ability to send a secure message or conduct other transactions across multiple channels traceable in a decentralized ledger.

DESCRIPTION: There is a critical DoD need to develop a secure messaging and transaction platform accessible via web browser or standalone native application. The platform separates the message creation, from the transfer of the message within a secure courier to the reception and decryption of the message.

Legacy messaging and backoffice infrastructures, traditionally based on centralized, unencrypted hub-and spoke database architecture, are expensive, inefficient, brittle and subject to cyber attack. The overhead costs of maintaining such architectures is rising rapidly. Many organizations unknowingly keep duplicate information and fail to ensure synchronization thus amplifying the potential for data theft and data corruption/rot. Incorporating a truly transparent mechanism for conducting journaled transactions enables the DoD to leverage its distributed footprint for a reduction in latency of these transactions, their security and their integrity and assurance.

The messaging platform will transfer messages via a secure decentralized protocol that will be secured across multiple channels, including but not limited to: 1) Transport protocol, 2) Encryption of messages via various application protocols, 3) Customized blockchain implementation of message deconstruction and reconstruction, and decentralized ledger implementation. With this messaging platform the business logic of the DoD ecosystem would be mapped onto a network of known entities using distributed ledgers. By doing this significant portions of the DoD backoffice infrastructure can be decentralized, ‘smart documents and contracts’ can be instantly and securely sent and received thereby reducing exposure to hackers and reducing needless delays in DoD backoffice correspondance. As an example, Military Interdepartmental Purchase Requests (MIPR) could be implmented using the secure ledger. Regulators with access to the ledger could read the correspondance and thus easily verify that a MIPR transaction didn’t violate Federal Acquisition Regulations (FAR).

The messaging platform would act as the transport for a cyptographically sound record of all transactions whether they be MIPRs, contracts, troop movements or intelligence. Troops on the ground in denied communications environments would have a way to securely communicate back to HQ and DoD back office executives could rest assured that their logistics system is efficient, timely and safe from hackers. The benefits are broad and could even be applied to domains such as space. With crowded skies it’s important to maintain situational awareness of all satellites and those concerned with space situational awareness/telemetry or air traffic control could instantly share data between nations using a separate but equivalent ledger implementation thus removing questions as to the authenticity and integrity of the data.

PHASE I: Create a specific decentralized messaging platform built on the framework of an existing blockchain framework. There are several layers of complexity that will be explored in this phase from the messaging platform, to transport protocol, to end user application. Phase 1 goals include: creating a model for the decentralized messaging platform, experimenting with encryption schemes, evaluating hardware to be used in combination with the messaging platform to provide additional security, and defining the product feature set from the application and platform perspectives and finally, developing a blueprint of the platform architecture mapped to DoD constructs.

PHASE II: Develop, test and evaluate a working prototype with the following features:
- Decentralized back end blockchain implementation
- Data aggregation, reconstruction
- Data transport protocol implementation
- End user application implementation (alpha)
- Conduct simulated MIPR transactions using the decentralized ledger
- Allow transparent regulatory review of DoD legal findings and contracts
- Significant reduction in time for regulatory overview of various transactions
- Tracking of aircraft or satellites with simulated telemetry or air traffic control data
- System Admin and Monitoring tools and engine
- Integration of hardware or edge of network hardware components

PHASE III DUAL-USE APPLICATIONS: The DoD requires a secure messaging system that can provide repudiation or deniability, perfect forward and backward secrecy, time to live/self delete for messages, one time eyes only messages, a decentralized infrastructure to be resilient to cyber-attacks, and ease of use for individuals in less than ideal situations. Based on the outcomes and feedback from Phase 2, Phase 3 will focus on commercialization and full-scale implementation of the platform. This entails converting the alpha of the end user application into a beta application and increasing user testing and platform monitoring and industrializing the back-end platform in terms of decentralized ledger architecture and blockchain implementation.

REFERENCES:

1. Hyperledger Project https://www.hyperledger.org/

2. SoK: Secure Messaging http://cacr.uwaterloo.ca/techreports/2015/cacr2015-02.pdf

KEYWORDS: email, end-to-end encryption, privacy, security, secure messaging, repudiation, perfect forward secrecy

Technical Points of Contact:

Name: Frank Pound
Phone: 571-218-4344
Email: frank.pound@darpa.mil

SITIS Questions and Answers

Ask a Question

4/25/2016

Q1. Are applications of non-US based institutions/companies accepted?

A1. [Response Pending]

Q2. The criteria for "time to live/self delete for messages" is impossible to achieve with a Blockchain. Is that a problem for this challenge?

A2. [Response Pending]

Warning

This is the DoD Submission System for unclassified use only. Do not discuss, enter, transfer, process, or transmit classified/sensitive national security information.

Browser Requirements

This site is best viewed in all modern secure browsers (Firefox, Safari, Chrome and IE10+). JavaScript must be enabled to use this website.

Privacy Policy (/privacy)

2015-11-16

2015-11-16