WHITENOISE LABORATORIES INC.
701 - 1736 West 10th Ave
Vancouver, B C
V6J 2A6 Canada

www.wnlabs.com
info@wnlabs.com

OPERATIONAL REQUIREMENTS DOCUMENT

National Cyber Security Framework and Protocol for securing digital information in networked critical infrastructures and communications

Contents

1. General Description of Operational Capability 4

1.1 Capability Gap 4

Cyber, Interoperability, and Information Sharing Capstones IPT 4

1.2 Overall Mission Area Description 6

1.3 Description of the Proposed Product or System 7

The primary set of characteristics 7

- Vulnerability to Man-in-the-Middle attack classes 8
- Vulnerability to Side Channel attack classes 8
- Uncontrolled life of data 8

The second set of characteristics 9

The third critical set of characteristics 10

1.4 Supporting Analysis 10

1.5 Mission the Proposed System Will Accomplish 11

US National Leap Year Summit 2009 11

1.6 Operational and Support Concept 13

1.6.1 Concept of Operations 13

Tiered, hierarchical network of secure networks 14

1.6.2 Support Concept 15

2 Threat 16

3 Existing System Shortfalls 17

Cyber Security 17

Representative technology needs 17

Information Sharing 20

Representative technology needs 20

Interoperability 22

Representative technology needs 22

4 Capabilities Required 23

4.1 Operational Performance Parameters 23

The DDKI/DIVA network of networks: ... 25

Tunneling topology at IP data link layer ... 27

DDKI/DIVA: ... 27

4.2 Key Performance Parameters (KPPs) ... 28

4.3 System Performance. ... 30

4.3.1 Mission Scenarios ... 31

4.3.2 System Performance Parameters ... 31

4.3.3 Interoperability ... 33

4.3.4 Human Interface Requirements ... 34

4.3.6 Other System Characteristics ... 38

5 System Support ... 38

5.1 Maintenance ... 38

5.2 Supply ... 39

5.3 Support Equipment ... 39

5.4 Training ... 39

5.5 Transportation and Facilities ... 40

6 Force Structure ... 40

7 Schedule ... 41

8 System Affordability ... 42

10 Appendixes ... 45

Homeland Security High Priorities ... 45

11 Glossary ... 47

Example Application topology ... 48

1. General Description of Operational Capability

- Microprocessor that distributes identity and which is resistant to side channel and man-in-the-middle attack classes

- Distributed servers for managing Dynamic Distributed Key Infrastructures [DDKI] frameworks for key creation, key management and key distribution in dynamic, tiered, hierarchical networks in any existing network configuration

- Dynamic Identity Verification and Authentication [DIVA] - a single protocol for complete network security

Note: Wiki Leaks type breaches can be mitigated using Secure Session Manager, Secure File Interchange 2 and the Hard Disk Encryptor network solution. DIVA identity management keys can be distributed in several ways. Side Channel attack resistant chips solve a historical problem and are ultimately most efficient in distributing identity to digital devices and appliances.

1.1 Capability Gap

Cyber, Interoperability, and Information Sharing Capstones IPT

The Information Technology communications critical infrastructure and digital provenance fundamentally impact all DHS high priority areas because none can be effective without the secure, real-time sharing of information and the secure storage of data internally (or externally - “the cloud”). The highest order need is safeguarding and securing Cyberspace. In doing so we help facilitate secure communications, information sharing and data storage in all Capstone IPTs since they all rely on computer networks.

The overarching gap in Homeland Security operations is the limited ability to communicate and collaborate with other departments and personnel, in real-time, securely.

Fundamentally, it is impeded automatically because existing asymmetric communications is always vulnerable to man-in-the-middle attack classes and microprocessors have always been vulnerable to side channel attack classes.

Additionally, most networks often render previous technology investments obsolete or require a need for costly upgrades to legacy networks proving impractical or unaffordable. A system is required that creates an IT/communications framework enabling DHS to allow not only interoperability of disparate networks, but also the ability to interconnect legacy networks and new networks.

Another major DHS capability gap is in providing an affordable solution for the interoperability and interconnection of secure communication networks.

There must be a framework for enabling communications, interoperability and collaboration that is affordable.

1.2 Overall Mission Area Description

The overall mission area is any Homeland Security, government, military or intelligence networks that rely on digital communications which progressively include more broadband and mobile connected networks for efficiencies, cost and economies of scale.

DHS network security is currently comprised of a collection of ad hoc, layered security solutions that fail to effectively provide:

- Identification of all person and non-person network access points
- Continuous, dynamic authentication of all persons, non-persons and backbone components
- Inherent intrusion detection with 100% accuracy
- Automatic, faster-than-human revocation and isolation of incidents
- Complete logging of all network usage
- Authorizations
- DRM
- Repudiation/non-repudiation
- Chain-of-custody of data
- Chain-of-command of data
- Unique, identity-based encryption
- A large, scalable authentication platform where there is only partial disclosure of credentials
- Simple key creation, key management, and key distribution

- These are provided with one DDKI framework and one DIVA protocol.

The mission areas covered by this ORD outline the capabilities needed to enable secure communications and collaboration between all DHS Capstone IPTs so their commands can interoperate with mutual aid, support teams and other responding organizations within moments of any network, smart grid, or critical infrastructure incident.

This ORD also addresses the capabilities needed to provide secure interoperable voice and data networks to command in control of any incidents and increasing collaboration and extending the chain of command across jurisdictions.

Finally, this ORD identifies the requirements of the proposed system capabilities and provides a communications framework for the creation of a dynamic, interoperable system of networks: one microprocessor, one software framework for managing dynamic distributed key infrastructures and key creation, management and distribution, and one software developer kit to rapidly scale integration.

1.3 Description of the Proposed Product or System

The primary set of characteristics that the DDKI/DIVA network solution has that addresses the DHS capability gap and that accomplishes the mission is that DDKI/DIVA networks are dynamic, enabling interoperability between any combinations of different communication device types and converge any type or number of disparate networks on-demand. It is also thwarts all major cyber attack classes.

Dynamic Distributed Key Infrastructures is a key-based framework that works in any topology, on any kind of operating system, and in any digital context. It works alongside any other security topologies or protocols.

Dynamic Identity Verification and Authentication is a key-based protocol that provides complete network security: secure login, continuous dynamic authentication, inherent intrusion detection, faster-than-human automatic revocation, signature, non-repudiation, and unique identity based encryption. It eliminates the fatal flaws of network security and solves the historical problems attendant with distributed key crypto-identity networks.

The three fatal failings of network security have been:

- Vulnerability to Man-in-the-Middle attack classes
    - M-i-M-doesn't work against distributed networks because there is no session key exchange. There is only a secure acknowledgement of the current dynamic offset. (Patented.)
- Vulnerability to Side Channel attack classes
    - Side Channel attacks don't work against DIVA because after key load all operations are order one operations. This has been confirmed by a 17 month NSERC government funded project at the University of Victoria. (Patented.)
- Uncontrolled life of data
    - Life of data can be controlled by enterprises, governments or consumers who can now prevent access to their own data uploaded into the cloud with unique identity based encryption and control of a single dynamic offset. (Provisional filed - patent pending.)

The system is based on software (whether implemented as firmware into microprocessors or not) that converges network protocol types and provides network presence awareness. The system enables data interoperability among any combinations of ad hoc, terrestrial data, telephony or satellite networks that are available or will be introduced in the future.

The second set of characteristics **that DDKI/DIVA network characteristics have that address** the DHS mission is that these networks easily create a network-of-networks and provide connectivity to the interoperable DDKI tiered, hierarchical framework. Everything that is needed will be provided and are simple to install anywhere with the kit (physical components) or to install anywhere electronically to devices which have connectivity, write-back and storage. These network-of-networks can handle all voice, video, and data communications peer-to-peer.

These systems are human portable resilient communication networks that can provide connectivity to the interoperability framework. These networks, whether chip-based or software based, require only that devices have a minimal amount of storage, write-back capacity and connectivity.

The communication security capabilities required that DDKI and DIVA provide are:

- Perfect identity of persons and non-persons components using ISO/ITU level 4 identity proofing
- A micro-processor or firmware that distributes identity and identity keys.
- Secure network access
- Continuous dynamic authentication (moving target defense)
- Inherent intrusion detection (self defending networks)
- Automatic, faster-than-human revocation
- DRM
- Repudiation/non-repudiation
- Signature

- Unique, identity based encryption
- Resistance to man-in-the-middle attack classes
- Resistance to side-channel attack classes
- Ability to control data life cycle
- One-to-one relationship between endpoints and the server
- One-to-many communications capability
- It works in any topology or configuration
- It works on any operating system
- It works in conjunction with any other security technologies
- It works in any medium - wireless, wired, RF, storage etc.
- It provides secure, two-way, peer-to-peer communications
- Simple network management software
- Simple operation and use without experience
- Simple to add IP-based devices and peripherals allowing on-the-fly scaling

The third critical set of characteristics **that DDKI/DIVA network-of-networks** have which satisfy the DHS mission is that it is an affordable, interoperable and scalable cyber network. DHS can afford to distribute enough network servers to create a National Communication Cyber Secure Network-of-networks to provide the infrastructure for the DDKI framework.

1.4 Supporting Analysis

- Canada funded an NSERC Side Channel Attack project at the University of Victoria ECE Labs. Whitenoise is side channel attack resistant.

- Global Patenting of DDKI and DIVA has been successful.
- Communications Security Establishment (references)
- Presented to the US National Cyber Leap Year Summit
- Presented to the United Nations International Telecommunications Union
- Members of every pertinent national and international standards group
- ATT Certification (SFI2)
- It is being presented to the European Telecommunication Standards Institute workshop in January 2012.

1.5 Mission the Proposed System Will Accomplish

US National Leap Year Summit 2009

"… defend our information and communications infrastructure, strengthen public/private partnerships, invest in cutting edge research and development and to begin a national campaign to promote cyber-security awareness and digital literacy." President Barrack Obama

″…it is imperative that we achieve a "leap forward" in cyber-security through development of "game changing" technologies." Aneesh Chopra, U.S. Chief Technology Officer

- US National Leap Year Summit
- The Whitenoise Vision
- The National Leap Year Summit Top 100 Cybersecurity Experts
- Whitenoise Laboratories (Canada) Inc. Digital Provenance Vision

Specifically the proposed system will *defend our information and communications infrastructure and* accomplish this mission because it:

- Provides a dynamic distributed key framework that can operate in any existing environment and alongside any existing technologies or with any legacy system and create a simple means of securing data at rest or in motion in our network and telecommunications networks
- Provides an identity based protocol that provides secure network access, continuous dynamic authentication, inherent intrusion detection, automatic revocation, DRM, signature, non-repudiation, logs and identity-based encryption.
- Provides a system that manages identity and allows secure, dynamic, interoperable communications and data sharing with anyone tasked by the Department of Homeland Security and who has data or telephony capability anywhere in the country. There is no need for additional equipment.
- Enables a secure network server and system to be implemented in under 4 hours (including system administration training).
- Enables the training of employees to use a secure network in minutes. There is no training for components that comprise our critical infrastructures and smart grids.
- Creates a system for voice, data and video interoperability.

- Provides the ability to log all network usage and identify all persons and non-person entities accessing the network

- Provides peer-to-peer communications that enable instant alerts, warnings and advisories that can be viewed and responded from anywhere in the country.

1.6 Operational and Support Concept

1.6.1 Concept of Operations

Dynamic distributed key infrastructures are tiered, hierarchical, peer-to-peer(s) frameworks that allow scaling and interoperability. The following graphic shows one way the government could issue master keys to telecommunication providers and link keys for those providers to interoperate securely between that tier. The telecommunication providers in turn distribute keys to their clients in that tier. Any configuration is simple either vertically, horizontally or in a mesh.

WHITENOISE LABORATORIES INC.

Whitenoise Labs

DIVA

Dynamic Identity Verification & Authentication

Standards Council of Canada
Conseil canadien des normes

isacc
cccnt

ICT Standards Advisory Council of Canada
Conseil consultatif canadien sur les normes de TIC

```
ERROR: stackunderflow
OFFENDING COMMAND: ~

STACK:
```