POC: Soto Triantafillou
Email: soto@nutstechnologies.com

AOC: Yoon Auh
Email: yoon@nutstechnologies.com

DIGITAL BODY ARMOR

Automatic Cryptography & Data-Centric Security

EXECUTIVE SUMMARY

The advent of data-centric security solutions will revolutionize the cybersecurity landscape for defense, government, and business organizations by significantly easing the burdens of safeguarding critical information while mitigating both external and insider threats. By prioritizing the protection of data at its core, burdensome activities like advanced encryption, access controls, and key management (Figure 1) will seamlessly integrate into enterprise level systems. Providing robust defense against unauthorized access, data leaks, and malicious activities. This transformation will empower operators to focus more effectively on their strategic objectives confident that their sensitive data is fortified to keep operational integrity intact.

KEYWORDS:

DATA Transport, DATA Management, Cyber Security, Network & DATA Management, Information Operations, Defensive Cyber Operations, Cyber, Data-Centric Security, Automatic Cryptography, & Command, Control, Communications & Computers

TECHNOLOGY

eNcrypted Userdata Transit & Storage (NUTS) is a decentralized technology that protects data both at-rest and in-transit in the form of a portable capsule called a nut, a secure data structure that is operable across multiple domains and contested environments. The NUTS approach allows for Insider Threat mitigation, ease-of-use for operators, no single point of failure, secure computation on protected data, and shifts the economic burdens onto the adversary.

The nut capsule is a JSON cryptographic data structure which can easily integrate with and operate on existing legacy, cloud, and proprietary systems. The nut capsule and NUTS ecosystem are based on viewing DNA as a data model. DNA is data and each cell containing DNA can process that data. DNA reveals the following operating principles: 1) identity, 2) protection, 3) replication, 4) history, 5) completeness, 6) instructions to create itself, 7) self-healing, 8) scalability, and 9) adaptability. We created a secure data capsule (data structure) called a nut (Figure 2) and infused it with these characteristics. Then we designed and implemented a data ecosystem that can transport, manage, and replicate these nut capsules, called the NUTS ecosystem. A simple analogy is to compare what a nut does for data to what standardized intermodal (shipping) containers did for freight transport: it transformed the bulk cargo landscape significantly and permanently.

NUTS uses all standard NIST ciphers and can easily expand to use any future approved ciphers with built-in backwards compatibility on a per document basis. There are two major issues when it comes to applied cryptography in the real world: first, there is a lack of consistent methods of applying ciphers in the field; second, we observed that ciphers change over time as they age and become vulnerable to newer technologies and attacks; methods that anticipate the change of ciphers over time are virtually non-existent and/or too limiting for practical use. Both issues are major sources of cyber weaknesses and/or costly project budget and time overruns. Consistency of cipher usage and adaptability of ciphers on a per nut capsule basis were primary design goals for NUTS. What we created is a cipher agnostic secure data capsule (nut) capable of expressing any degree of security on a single data object (document) in a purely cryptographic way (only data is used in the makeup of the capsule).

CAPABILITY INTEREST

ALL USE CASES: Capability to enforce NTK cryptographically in any environment on operationally sensitive data from insider threats by drastically shrinking the internal attack surface to maintain operational integrity. This mitigates the insider threat risks where administrative staff can read content due to their security clearance. The capsule allows for the administrative staff to authenticate secure data without the ability to read the content, further reducing the attack surface.

USE CASE: Command, Control, Communications, and Computers (C4): Small Form Factor Cross Domain Solution. Capability to automatically secure and transfer data (Figure 3) across domains helping the operator by automating encryption/decryption tasks, automatically managing combinations of NIST approved ciphers, and automatically sending the payload on data defined networks regardless of the type of network.

USE CASE: Command, Control, Communications, and Computers (C4): Edge Computing Devices. Benefits operators by having edge computing devices streamline the process of automatically encrypt/decrypt and share data without the need to stand up or maintain any back-end server connectivity. Capability to reduce the time to setup and deploy connections to a centralized network to authenticate.

USE CASE: Command, Control, Communications, and Computers (C4): Protected, Congested, Contested Communications (PCCC). Data is protected in cryptographically secure capsules which can reside in any environment AND continue to operate with the same access controls as in a non-contested environment. The secure capsules are managed automatically and monitored by a threat detection system assuring the operators can work with tamper-free data.

USE CASE: Command, Control, Communications, and Computers (C4): Mobility Communications (MC). Our technology is a decentralized and distributed system that can enable the operator to effortlessly traverse and leverage any combination of links for secure data transfer from local, to cloud, to a dedicated connection. This benefits the operator by assuring that their operational data is protected in a consistent way across the spectrum of communication links and cloud environments that the data may traverse.

USE CASE: Cyberspace Operations: Information Assurance. Capability to provide information assurance for any documents and file types and seamlessly integrate into worldwide enterprise systems with our distributed model. A major benefit is the reduction/removing of repetitive data operator tasks, IT management, and maintenance overhead.

USE CASE: Cyberspace Operations: Advanced Computer Forensics Tools. We can offer operators the ability to easily review the provenance, audit, and exchange of data files managed in capsules on computer systems like desktops and laptops. Capability to expand into securing any computer operating environment by encapsulating critical system configurations and executables in tamper-proof secure capsules.

USE CASE: Information Operations (IO): Military Information Support Operations (MISO) Advanced Techniques: Empower the operator to easily integrate with other operational units to securely share information via data defined networks. These are cryptographically defined groups that are transparent to the operator and does not require specialized training past the basic operations of the technology.

USE CASE: Information Operations (IO): Operations Security (OPSEC): Ability to create unique identification and classification for every document ingested into a capsule. This can generate unique URIs per document providing structure to unstructured data. These reference URIs can in turn be communicated and shared in databases, messaging systems, and references in other documents. This provides an automated and systematic approach for a program or data manager to identify and control sensitive electronic information from its inception as a capsule.

USE CASE: Information Operations (IO): Computer/Cyber Network Operations (CNO): Provide access controls at the data layer empowering the data owners to determine access while operators administer systems. Provide information assurance through our cryptographic management of metadata and classifications that enforces audits, tracking, and provenance. Automated cryptography removes the burden of operators encrypting and decrypting data.

USE CASE: Intelligence, Surveillance, and Reconnaissance: Advanced Data Management: Assist in the automation, identification, classification, and management of data across a multi-domain environment.

USE CASE: Irregular Warfare: Military Information Support Operations (MISO) Preparation of the Environment/Persistent Engagement: Provide support operations the ability to specifically identify and control access to individual documents or file types allowing for the controlled dissemination of information securely while minimizing data leaks.

USE CASE: Mobility: Increased Operational Capacity and Capabilities: Participate in enabling actions by providing "data logistics" to easily create and manage storage points, data inventory, reliability, and accuracy. The benefit to the operators is data replication and synchronization is securely and automatically initiated. Only connectivity on the edge device or server is needed.

TECHNOLOGY STATE

DUAL-USE: We currently offer a commercial data management platform at TRL 9 that implements this data centric security technology. We can demonstrate today the use of this platform to ease an operator's workflow and technical skillset requirements. Furthermore, integration is seamless between disparate domains and organizations. If a file system can store a JSON file, then nut capsules can reside on that system and be operated upon.

All transmissions are done using secure TCP/IP sessions and currently all nuts are saved as JSON-base64 files (this is dynamically configurable within a nut). The NUTS platform is written in C# on .Net on Windows OS, and Python. (Python is slated to be transitioned to C# for performance and integration in the near future). Our goal is to operate on all operating system platforms including mobile and web.

SUMMARY

NUTS reimagines how secure information systems can be designed for improved usability, integrability and interoperability. The underlying technology of NUTS offers significant technological advancements in automating the application of routine cryptography. Privacy Enhancing Technologies (PETs) by NIST are exploring data-centric security concepts. Characteristics of the NUTS framework satisfies many of the most aggressive goals of the National Cyber Moonshot, National Cybersecurity Strategy, and CISA principles for Security-by-Design and Security-by-Default. Our uniqueness is further underscored by MIT Lincoln Lab researchers with DoD funding (FA8702-15-D-0001) which have begun studying data centric security models (ACDC2) and have reached the same conclusions on the immense benefits of such an approach.

We can provide new capabilities for Insider Threat mitigation at a document level removing layers of IT & administrator access while simplifying the operator's workflow and reducing technical skill set requirements. These are the long sought after technical controls to allow IT admins to do their work while strictly enforcing a NTK policy on sensitive data. NUTS also provides a consistency of security that travels with the data so that the security profile of the data is enforced in any computing node whether there is cloud connectivity or not thus allowing maximum flexibility for the operator.

LIST OF FIGURES

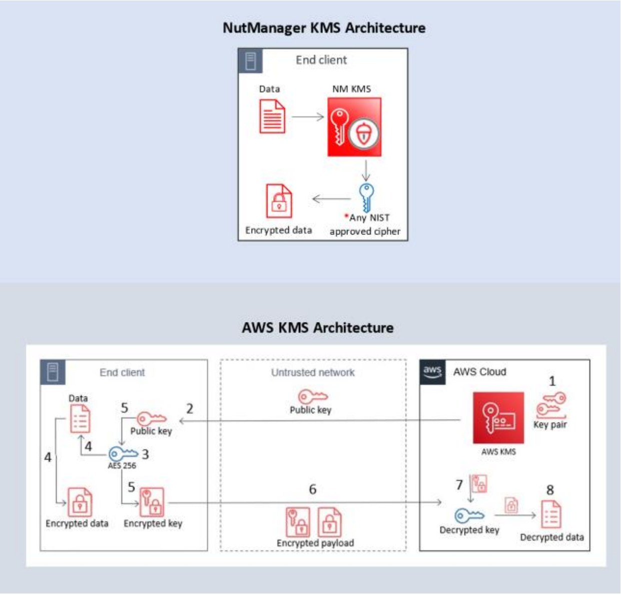

Figure 1

Key Management System

NOTE: An example of the systems Key Management System as compared to a traditional centralized key management system.

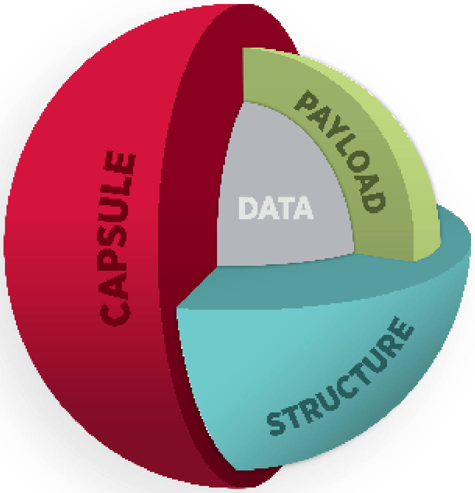

Figure 2

Nut data structure

NOTE: A representation of a nut data structure with its various cryptographic layers. Each layer can contain 1: n variable locking mechanisms.

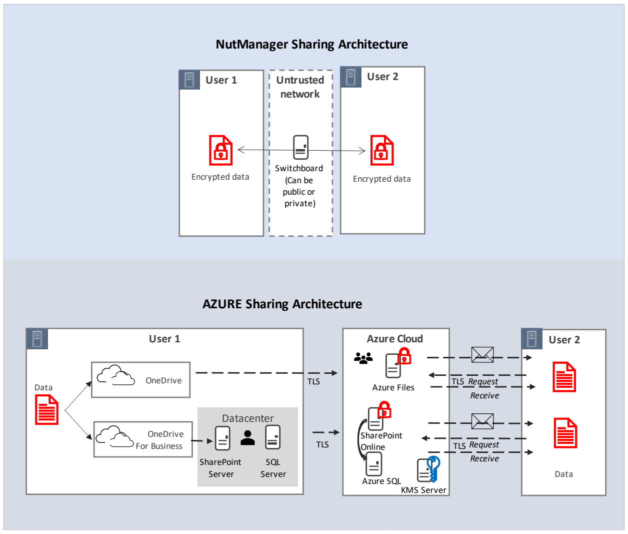

Figure 3

Data Sharing Architecture

NOTE: An example of the systems distributed document sharing architecture as compared to a traditional centralized cloud sharing solution.