Department of Homeland Security Battle Insider Threats   
and Maintain National Cyber Security  
V M Naveen Chatlapalli

Gaurav Sharma

Preeti Preeti

Sai Kiran Kumar Rayanapati

ITS 834 – FALL 2018

**University of the Cumberlands**



Abstract

Department of Homeland Security or simply DHS is the nation’s first lines of defense. DHS goal is to protect America. That means if DHS is compromised in anyway the national infrastructure of America is compromised. It is incomprehensible to imagine what all could happen if that statement comes true. Therefore, it is very vital to keep DHS secured at all times & cost. However, with 240,000 employees and a number of connected systems, it is not an easy task. In this paper, we have tried to address the concerns of an entity of this magnitude to keep its infrastructure safe every day from cyberattacks so that DHS can do what it does best: protecting the nation.

Keywords: DHS

Department of Homeland Security Battle Insider Threats   
and Maintain National Cyber Security  
V M Naveen Chatlapalli

The sections are organized into the order we tried to address the concerns of DHS given in the problem.

# Unifying access control with Single Sign-On

One of the major problem for the DHS is to unify its 21 component agencies and simplify the access to their online applications to the users; to achieve this, there is no better option than Single Sign-On (SSO). SSO is an enterprise integration technique where the user is asked only once to provide his credentials (username & password), and upon his or her first successful authentication the user session is created, and in return, the user may be presented with a token that the same user need to use in every subsequent request. From here on, the user session is managed by an SSO server. Once all the apps under the same component agency are onboard (AD/LDAP integration) under the SSO server, then users only need to log in once to the SSO server, and the user can access all applications without even a need to re-enter their credentials again and again for each systems login. This centralized access management technique also works as a centralized control technique as well because to revoke the privileges of any user only requires updating his privilege in a single AD/LDAP store. Once the user is disabled in the SSO server via AD/LDAP configuration, then he cannot access any of the systems. User’s rights to log in and access can be revoked as soon as it is needed. That means team handling an insider attack can act very quickly. The entire beauty of this technique is its simplicity. On the other hands, it also results in cost savings from chores like password reset or enabling the user account because these controls are now centralized so no need to go on each app to request or to reset the password or access.

Nowadays product like Okta is present in the market which allows users to configure multi-factor authentication (MFA) with predictive technologies based on policy violations, location, device, network contexts which get automatically triggered as needed by the solution like Okta. According to their website, okta.com, “Okta also has 1000+ integration framework to work with existing tools, technologies like VPNs, cloud, and operating systems”. Okta does not just allow 2-factor authentication, but it goes beyond that by providing multi-factor authentication (MFA) ranging from OTP on email and on cell phones, soft & hard tokens, digital certificates, and even biometrics. Even though, use of MFA with SSO makes the system harder to crack while keeping the user experience better because of SSO. Therefore, we believe that this solution will work perfectly well to solve the unifying problem of the DHS.

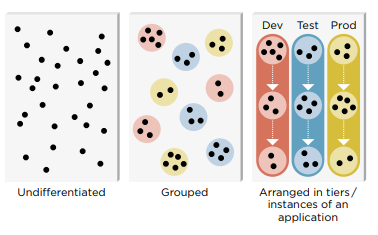
# Hardening the components & watchful Administration

Micro-segmentation is one of the security implementation that empowers easy structured security arrangements to be brought out to server farm applications, down to the remaining task at hand level. This methodology empowers security models to be conveyed somewhere inside a server farm, utilizing a virtual programming approach. One critical advantage of micro-segmentation is that it incorporates security straightforwardly into a virtualized outstanding task at hand without requiring an equipment based firewall. This implies security arrangements can be synchronized with a virtual system, virtual machine (VM), working framework (OS), or other virtual security targets. Security can be relegated down the level of a system interface, and the security approaches can move with the VM or remaining task at hand, in the event of relocation or reconfiguration of the system. Advantages of micro-segmentation are straightforwardly identified with numerous server farm virtualization innovation merchants, including Cisco, Nuage, and VMware have been touting the advantages of micro-segmentation as leverage of system virtualization (NV). VMware itself has been particularly dynamic in making micro-segmentation part of its NV showcasing system. Micro-segmentation is regularly done in programming, which makes it simpler to characterize fine-grained portions. Furthermore, with micro-segmentation, IT can work to bring together system segmentation approach and diminish the quantity of firewall rules required.

Using concepts of Machine Learning, we can automate the critical challenges in micro-segmentation (Interset et al., 2013).

* Network discovery
* workload grouping and policy assignment, and visualization of the micro-segmented network.

Source: 1



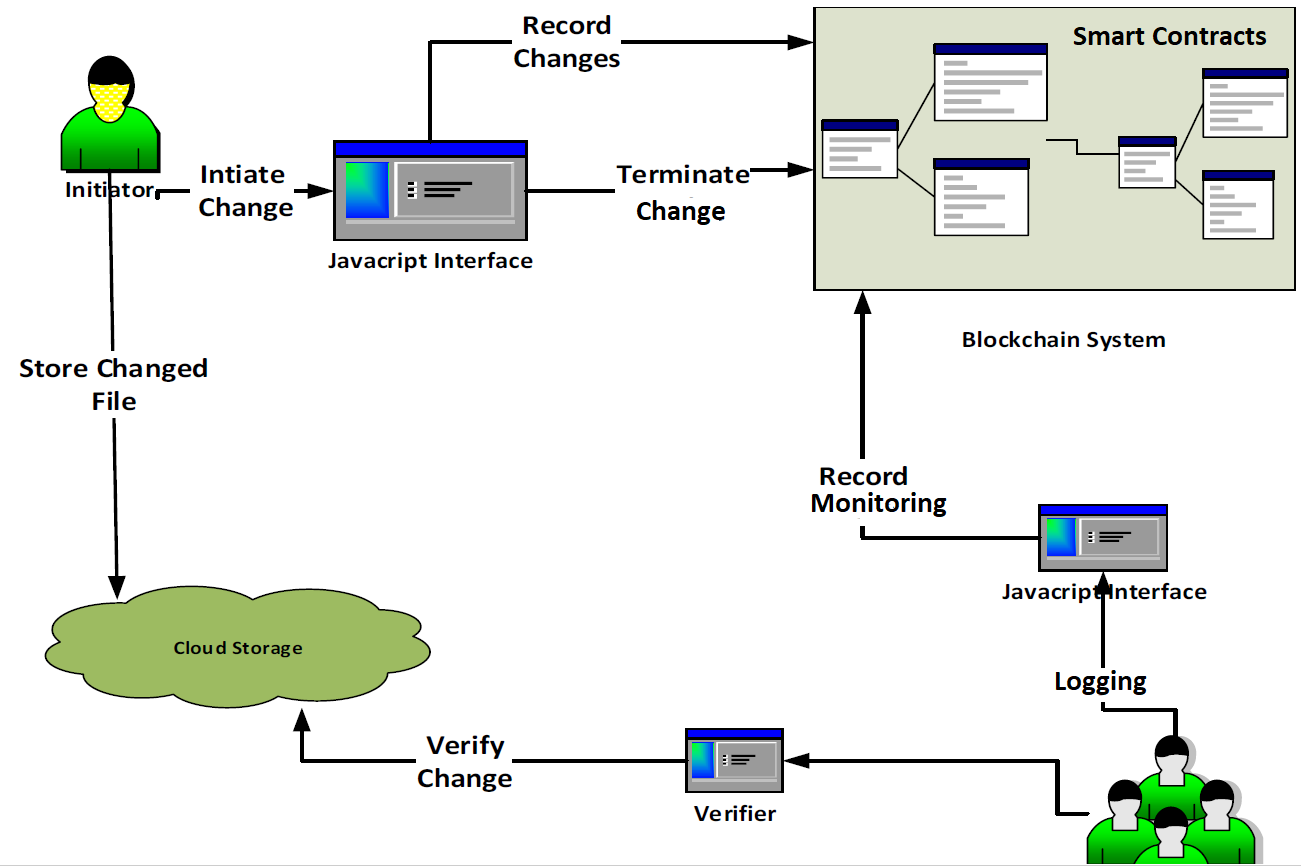
DHS needs to facilitate unified, incorporated exercises crosswise over parts contained access and checking, logging and following every managerial change to its frameworks will be settled by the blockchain innovation, and it obviously gives the entrance and observing, logging and following every authoritative change to its frameworks. The smart contracts composed on the blockchain actualized in a system will trigger all the key log occasions required by the managers. Ethereum, a dispersed open blockchain arrange. As the smart contracts dwell over the Ethereum blockchain, executions of the smart contract are likewise recorded in the blockchain.

Desktop virtualization and supported remote access with easy organizational network auditing can be achieved with the de-centralized architecture using block chain.

Key features provided are:

* Identity management
* Distributed Consensus
* Redundancy by design
* Network Segmentation and access control
* Vulnerability and Threat management

We consider a logical research setting where scientists keep their exploration records as a report put away in the cloud. The report (e.g., any information record) is scrambled by the proprietor of the archive. Access to the record is confined utilizing open key encryption. The proprietor of the exploration archive gives access to the record to clients by giving the key. For a client to log the provenance data in the Blockchain framework, the proprietor of an archive needs give access to the record to the client. In the Blockchain framework demonstrate, the progressions to the records are made through forming. Each change identified with an archive is put away as a different new form. The framework expect that just the most recent rendition of the report/information record is utilized for alteration. The framework checks the condition that any record which contains changes not signed in the provenance information is disregarded. The framework energizes honest conduct by punishing the clients who submit wrong change provenance points of interest. The information clients are remunerated in the occasion they locate a blemished change submitted with a part of the store sum for the change. The clients log legitimate changes to the framework utilizing customer applications running in every one of the individual client's program. Every one of the customer applications stores constant information about the reports that the present client approaches utilizing a back-end database (ShieldX Networks et al., 2013).

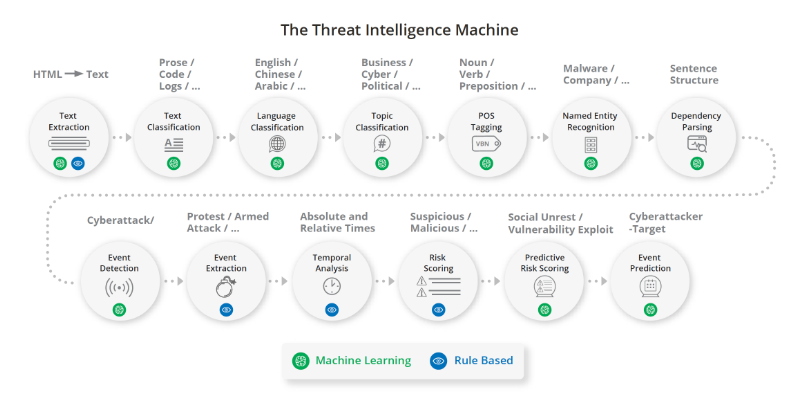
Source: 1

**Future of Cyber Security**

The future of cyber security is with the advancement of the latest technologies being developed in Artificial Intelligence and Machine Learning. There are many advantages because of the AI techniques being implemented in the Cyber Security space.

1. Predictive Threat Intelligence – Preventing attacks before they occur.
2. Automatic Anomaly Detection – Identifying the vulnerabilities about the network identified attacks.
3. Data Ex-filtration – Which is clearly observed and implemented using the Machine Learning techniques using the DNS tunnelling.
4. Risk Score Analysis – Proving the expected risk score based on the individual software bundle or a package.
5. Content Classification – Which will be best used in government data processings or defense-related data content monitoring.
6. Destination Classification – This is the new feature of AI, by predicting the end point destination classification by many neural network algorithms.

A sample use case of predictive threat intelligence is explained in the below diagram. This has both rule-based, and machine learning approaches and clearly explains which will give the accurate results.

Source: 2

# Securing network & efficiently managing data centers

Logical Weapons: Logical tools or weapons that are a set of tools used to perform reconnaissance checks, there are many free open source tools available in the market to perform such tasks. Open source intelligence (OSINT) refers to intelligence that has been obtained from publicly available sources. With the help of OSINT tools, the reconnaissance process gets streamlined, enabling a more efficient narrowing-down to the target. Using open source intelligence tools drastically reduces the number of permutations and combinations to be dealt with, in respect of information gathered. (Andress, 2014).

**CheckUserNames** This tool can help us find usernames across over all social networks. This is especially useful in case of running an investigation to determine the usage of the same username on different social networks. Also, other use case is check for brand company names, not only individuals.

**Unicornscan** is one of the top intel gathering tools for security research. It has also a built-in correlation engine that aims to be efficient, flexible and scalable at the same time.

**nmap** : With the help of this tools we can perform these tests like ip spoofing, port scanning and can also help in knowing what system/firewall is being used.

Scanning tools like **PeekYou** and **Lullar** websites enable the gathering of information about a person that is available on various social networking sites.

**SAMRi10** comes in handy for securing networked computers connected through Windows domains. SAM, or the Windows Security Account Manager, is a database that holds information about all user accounts. SAMR is the act of querying a remote SAM database. Every Windows computer supports SAM. Computers assigned to a network domain, store information about their accounts in the domain's SAM database. They then use SAMR to perform remote queries on the SAM database and get information on their users, or the users on other computers/servers. If the computer is not part of a network domain, then the computer stores information on all local accounts into a local SAM database. These computers don't need SAMRi10 since the attacker is usually contained only on the infected computer.

The idea of cloud computing brings in a wide range of possibilities & opportunities but at the same time has its risks. Here we are focusing on one such industry leading cloud platform called Microsoft Azure.

Azure has one solution for information protection service called Azure Information Protection (AIP), its a cloud-based solution that helps an organization to classify and optionally, protect its documents and emails One of the biggest benefits of using the Azure Rights Management service for data protection is that it supports business-to-business collaboration without you having to configure explicit trusts for each partner organization, because Azure AD takes care of the authentication for you. There is no administration option to prevent users from securely sharing documents with specific organizations.

Azure MDM tool helps in giving you freedom for you to work from any device any where. These new DLP policies enforced will be adding more security controls to your devices or application in order to be accessed and provide the convenience of single sign-on access to thousands of cloud and on-premises applications with one unified identity.

**Federal Desktop Core Configuration Compliance(FDCC)**

   Federal Desktop Core Configuration Compliance(FDCC) is a group of standards for devices which runs on Windows XP or vista, which provides compulsory guidelines by the Office of Management and Budget (OMB) to agencies for setting desktop configuration which is proposed by National Institute of Stands and Technology(NSIT) with a purpose to create security baselines to improve the security. The goal of the Federal Desktop Core Configuration Compliance(FDCC) is to create a security parameter with a defined baseline to improve the security and to smoother the administrative task such as scheduling and patch management at reducing cost.  Federal Desktop Core Configuration Compliance(FDCC) is based on guidelines of several OMB agencies such as US Air Force, Microsoft, National Institute of standards and Technology, Department of Homeland Security and National Security Agency. Federal Desktop Core Configuration Compliance was developed by the National Institute of Standards and Technology (NIST) by combining together Office of Management and Budget (OMB), Department of Homeland Security(DHS), Defense Information Systems Agency, National Security Agency, US Air Force and Microsoft.  Applications included in FDDC are currently only for Windows XP/ Vista, Xp/Vista Firewall and Internet Explorer 7 with a service pack, but in future, it can comply with windows 7, Mac OS and Linux.

The tool which is used by federal agencies to verify that the desktop system is as per the Federal Desktop Core Configuration Compliance complaint and guidelines on vendor products is known as Security Content Automation Protocol (SCAP). Security content Automation Protocol (SCAP) is a validation program with a standardized format which helps to communicate information and is used to verify the correct and successful implementation of Federal Desktop Core Configuration Compliance (FDCC) setting on windows XP, Vista, XP firewall, Vista Firewall, Internet Explorer 7. Security content Automation Protocol (SCAP) helps to automate the vulnerability management with an evaluation of the compliance. A checklist has been maintained by the NSIT for Federal Desktop Core Configuration Compliance(FDCC) configurations to check whether it has been deployed as per the guidelines or not. These checklists are in Xml document which uses the Security Content Automation Protocol (SCAP).  To enable to automated vulnerability management, six security standards have been put in by Security Content Automation Protocol (SCAP) to state that how these standards are combined. One of the Security Content Automation Protocol (SCAP) compliant tool is Tenable security center and Nessus vulnerability scanner. This can be used by the Federal departments to verify the configuration before deploying which is follows by monitoring the compliance with Federal Desktop Core Configuration Compliance(FDCC). Common Vulnerability Enumeration (CVE) has identified the security concerns using the checklist of Federal Desktop Core Configuration Compliance(FDCC), and these security concerns can be resolve by patching. Concerns which are recognized by Common Configuration Enumeration (CCE) can be solved by checking configurations settings. Some SCAP Validated Products are BMC Client management, McAfee Policy Auditor, Red Hat OpenSCAP, Configuration Assessment Tools and Tripwire Enterprise.

Federal Desktop Core Configuration Compliance(FDCC) was replaced by the United States Government Configuration Baseline (USGCB) in 2010. United States Government Configuration Baseline (USGCB) has the same goal as Federal Desktop Core Configuration Compliance(FDCC) to standardize the IT configuration which can tell them what to do, which can help them to improve their security by improving the efficiency of the system against the known and yet to known threats. It also provides several other benefits such as reduce the IT cost, maintaining beneficial configuration, to save the energy it makes it compulsory to use the power management. United States Government Configuration Baseline (USGCB) minimize the complexity at the management level of the organization and all the agencies either national or non-national who uses windows XP or vista are obliged to use the United States Government Configuration Baseline (USGCB) and follow proper guidelines.

**Solution tool for virtualization, web browsing and access control**

Ericom Software is a one stop solution which provides a solution for secure browsing, desktop and application access which is virtualization along with remote access management. It is really important to keep the digital workspace safe and secure from the internal and external attack, and this can be achieved by installing Ericom software into the system for securely connecting the digital workspace as it provides Secure web browsing using the remote browser isolations with several solutions to provide the secured and continous connectivity. Ericom helps the organization to centrally manage the access of the application, desktops and database to the custom which is accessing globally.  Ericom has a variety of product to perform several functions to provide solutions such as

1. **Ericom Connect** which provides scalability and security with ease of use along with browser-based end-user access.
2. **Ericon AccessNow** which provide browser based access to the device and system which are running on HTML5 Compliant browser.
3. **Ericom Shield** for secure browsing provides security without installing any software by detouring, containing and disposing of all the possible risk using the borrower borne threats to protect both networks and end users in the remote safe zone.
4. **Ericom Blaze** this product is to provide the solution for Remote Desktop connection while reducing the consumption of RDP bandwidth.
5. **Ericom AccessToGo Mobile RDP Clients:**provides anytime and anywheresecure access to windows terminal server/RDD/ virtual desktops along with physical desktops.

References

1. IAM (Identity and Access Management). (n.d). Retrieved from <https://www.okta.com/iam-identity-and-access-management/>
2. Single Sign-On. (n.d). Retrieved from <https://www.okta.com/products/single-sign-on/>
3. Adaptive Multi-Factor Authentication - New Q2 FY19. (n.d). Retrieved from <https://www.okta.com/products/adaptive-multi-factor-authentication/>
4. Kukic, A., Gontovnikas, M., Totten, N., & Pace, E. (2015). What is and how does Single Sign-On Authentication work?. Retrieved from <https://auth0.com/blog/what-is-and-how-does-single-sign-on-work/>
5. ShieldX Networks. (n.d.). Retrieved from <https://www.shieldx.com/wp-content/uploads/2018/02/ShieldX_White_Paper-Machine_Learning_for_Micro-Segmentation-WEB_0202>
6. [1709.10000v1] Using Blockchain and smart contracts for secure data provenance management. (n.d.). Retrieved from <https://arxiv.org/abs/1709.10000v1>
7. Andress, J., & Winterfeld, S. (2014). Cyber Warfare : Techniques, Tactics and Tools for Security Practitioners (Vol. Second edition). Waltham, Massachusetts: Syngress.
8. Retrieved from https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security. (n.d.).

Image Source:

**Source** 1: [1709.10000v1] Using Blockchain and smart contracts

**Source 2:** Machine Learning: Practical Applications for Cybersecurity. (2018, March 14). Retrieved from <https://www.recordedfuture.com/machine-learning-cybersecurity-applications/>