**Lecture: Network Security**

**Content Author:** Dr. Michael J. Simko

Graphical user interface, application

Description automatically generated

When implementing network protection, several factors come into play. The cost to protect the network, the availability of required services and the data handling regulations are a few of these factors. The best way to achieve sufficient network security is to design the network with segmentation while utilizing the defense in depth strategy. Let's talk about some best practices for achieving an adequate baseline of network security.

Logo

Description automatically generated with medium confidence

**Network Layer Security**

* Protect the network components, applications, and services from outside attacks. This is where we would use the intrusion detection, intrusion prevention, and firewall devices to safeguard our network. Doing so will achieve perimeter security.
* Ensuring the confidentiality, integrity and availability of data is crucial. This is where we would utilize virtual private networks to assist in achieving overall communications security.

Logo

Description automatically generated with medium confidence

**Infrastructure Security**

* Negate single points of failure and ensure availability of each device. In other words, implement platform security to include a network security plan. The plan should include at minimum methods for intrusion detection, vulnerability management, endpoint compliance and scanning of devices to ensure compliance.
* Audit user access to ensure least privilege. Access security will provide the means for ensuring users or employees have access to only what is required for their particular role or job.
* The worst security breaches can occur if someone with malicious intent has access to the network or systems on the network. Physical security helps prevent a nefarious actor from modifying, infecting or destroying physical network hardware components.

Logo

Description automatically generated with medium confidence

**Network Life Cycle Security**

* Ensure security is discussed during the planning phase of network hardware procurement. Determine how a security breach specific to this device may be prevented. Harden systems and operating system the devices use to prevent intrusion. Maintain these security requirements throughout the full duration of the hardware's life cycle.
* Determine how to detect different types of breaches on the network. Utilize vendor knowledge and advanced persistent threats to determine common attacks and trends that may be applicable to the systems you use. Always check for misconfigurations of network hardware, as this is one of the most common mistakes that lead to breach.
* Establish incident response procedures applicable to different scenarios and devices that pertain to the network as a whole. Ensure that all staff is educated and aware of how to operate during an incident. Use tabletop exercises and real life simulations to fully predict possible issues and document lessons learned.

Logo

Description automatically generated with medium confidence

**Layered Defense**

* A layered defense is just another way of describing network segmentation. Establishing VLANs are one way to accomplish this. The primary objective behind a layered defense is to ensure if one device is compromised, not all devices on the network are. For example, our printers may be breached but they should be on a printer VLAN. Our users and switches should be on VLANs of their own. Each VLAN will have specific security settings and access control lists configured.

Logo

Description automatically generated with medium confidence

**Network Security Planning**

* Develop network security policy, procedure and baseline configuration documentation. Doing so will identify both requirements and expectations pertaining to each part of the network.
* Ensure all employees, whether user or network admin understand and acknowledge policy statements, acceptable use policies (to determine what can and cannot be done on the network) and service level agreements (so there is a thorough understanding of what services the network is providing).
* Offer awareness training to educate users on best network practice.
* Provide mandatory employee training and security awareness requirements.

Logo

Description automatically generated with medium confidence

**Roles and Responsibilities**

* Update and maintain position descriptions and clearly articulate differences in roles. Enforce separation of duties.
* Separate group network administrative access. For example, grant a network administrator the ability to manage switches and routers while a system administrator can manage server network settings, configuration and management. You can further expand upon this by tasking one network administrator to only have the ability to configure access control lists, while another network administrator only has the ability to run IOS upgrades and so on.

Logo

Description automatically generated with medium confidence

**Network Integrity**

* Ensure network devices are patched when new patches are released. Test patches in a secluded environment to ensure there are no issues that could break a device or hinder network availability.
* Disable ports, protocols and services that are not necessary. Leaving unnecessary services open provides additional attack vectors for attackers.

Logo

Description automatically generated with medium confidence

**Endpoint Compliance Strategy**

* Develop a security plan for wireless and wired devices. Do not forget to include cell phones (company or personal use), tablets, smart watches and other devices that have network capabilities. You don't want to run into the situation where all of your company owned assets are secure, but an attacker is able to gain access to your network through a vulnerable smart phone and so on.

Logo

Description automatically generated with medium confidence

**Network Management & Security**

* Ensure network security such as IP Security, SNMPv3, TLS, SSH and so on are utilized to keep network equipment and infrastructure safe.
* Create and secure baselines, backup configurations, configuration files, snapshots, etc. to ensure they are readily available if needed, and secure from those who could use the information to harm your network.
* Use a change management procedure to ensure all applicable technicians are aware of modifications and able to review maintenance, updates, replacement and more pertaining to each device.
* Monitor network traffic and establish normal trends to differentiate suspicious activity.

Logo

Description automatically generated with medium confidence

**Data and Personal Identifiable Information**

* Ensure the confidentiality and integrity of data. Encrypt data at rest and in transit while using non-repudiation to validate integrity.

Logo

Description automatically generated with medium confidence

**Internal & External Awareness**

* Block external threats through security configuration, but do not forget insider or internal threats. Most of security incidents deal with disgruntled employees who experienced privilege creep.
* Stay current on cybersecurity news and attacks. Staying in the know can help identify potential vulnerabilities that other organizations fell victim to, applicable to your organization. Both Information Technology and Cybersecurity are constantly evolving. It is imperative to research network vulnerabilities, exploits and systems commonly compromised on a frequent basis.

Logo

Description automatically generated with medium confidence

**Log Review & Audits**

* Establish a logging initiative and review logs regularly. This is a great detective measure for identifying attacks or exploits that are silent or go undetected on the network. This also helps hold administrators with privileged access accountable for their actions.
* Logs should be analyzed daily to identify, react to and stop any types of threats that may arise on the network.

# Lecture: Wireless Networking Standards & Security

**Content Author:** Dr. Michael J. Simko

Your textbook identifies several networking standards to include the standard 802.11a-n wireless standards. The 802.11n or Wi-Fi 4 standard seemed great, but let's dig deeper. In this week's lecture we are going to dive a bit further into newer wireless standards and the differences between each. Furthermore, we will discuss several basic wireless network security standards you should implement both at home and in the work environment.

## Modern Wireless Networking Standards

|  |  |
| --- | --- |
| **What is 802.11ac?**  The 802.11ac standard, also known as Wi-Fi 5, offers rates of up to 3.46 Gigabytes per second. Wi-Fi 5 utilizes a 5 Gigahertz frequency band and makes use of Multiple Input, Multiple Output (MIMO) capabilities. MIMO is a technology that assists with error reduction and enhancing speed. Usually, 802.11 routers are backwards compatible meaning they operates at the 2.4 Gigahertz frequency band and are backwards compatible with 802.11b, g & n devices. | **What is 802.11ax?**  So, 802.11ac sounds like quite an upgrade to 802.11n, no? Well, how about 802.11ax or Wi-Fi 6? This is an even better enhancement including improved performance and speed, especially in large public areas such as an airport or sports stadium. Similar to 802.11ac, this standard also supports the 2.4 and 5 Gigahertz frequency bands while it is said to implement four times the efficiency and speed as its predecessors. |

Graphical user interface, application

Description automatically generated

## Wireless Networking Security Standards

Wireless internet access is a great feature negating the necessity for physically plugging in cables and being restricted on the location of your computing devices. Implementing security to protect your wireless network is a must, as many times the radio frequency your router or access point produces, travels well outside the walls of your home. Security made available for protecting Wi-Fi has evolved over the years. You should be familiar with old standards to not use and newer standards that are recognized as the best security solution.

|  |  |
| --- | --- |
| **WEP** | WEP stands for the Wireless Encryption Protocol. WEP was one of the original forms of wireless security associated with 802.11b. WEP is an older technology that used RC4 stream ciphers along with sixty-four and one-hundred and twenty-eight bit keys for encryption. WEP is not recommended to use as a security solution as it can be hacked very easily. It is vulnerable due to not only its inadequate authentication features, but also due to its twenty-four bit initialization vector. |
| **WPA** | WPA is the abbreviation of Wi-Fi protected Access. It also uses the RC4 stream cipher but possesses more advance initialization vectors and two-hundred and fifty-six bit encryption keys. Every client is issued new keys with the Temporal Key Integrity Protocol, which was included as an addition to the 802.11i standard. It possesses stronger authentication through means of 802.1x and the extensible authentication protocol. WPA is a better solution than WEP, but you should really utilize WPA2 instead. Let's talk about WPA2 now. |
| **WPA2** | The Wi-Fi Protected Access 2 or WPA2 is the latest and greatest security standard. It used more advanced encryption techniques than its predecessors which does not hinder performance. WPA2 no longer uses RC4 or TKIP like WPA, but utilizes the Counter Mode CBC-MAC Protocol in conjunction with the Advanced Encryption Standard. This is the security standard you want to implement at home and the office. WPA2 offers personal and an enterprise mode configuration options. Let's take a moment to compare and contrast personal and enterprise modes.  Personal Mode:   * Used for home network configurations. * All users are required to enter password on specific devices they use (one password for everyone). * PSK Mode doesn't allow wireless access to be centrally/individually managed. * Password are stored on devices connecting to the wireless network.   Enterprise Mode:   * Primarily used for business network configurations. * Individual and centralized management. * Login credentials specific to each user are used. * Supports 802.1x RADIUS authentication (RADIUS Server required). * Users do not deal with encryption keys which are based on each session. |
| **WPA3** | Wi-Fi Protected Access 3 provides even further improvements to version 2 (WPA2). Pre-shared Key (PSK) authentication is replaced with Simultaneous Authentication of Equals (SAE). Many devices are not built to support WPA3, so it may be a while before this standard fully replaces WPA2. If you have a newer router, you may notice you have the option to use WPA3, however, it is not recommended as of yet. |
| **WPS** | So now that you briefly understand WEP, WPA and WPA2; let's talk about Wi-Fi Protected Setup (WPS). You may have noticed WPS buttons on your home router or other networking peripherals you dealt with in the past. The main intent of this feature is simply to use a pin, rather than your Wi-Fi password to configure a device. It was meant to hasten and simplify the tedious process of adding network equipment to an existing configuration, however, it is not the best security solution. Although the device is most likely inside your home and cannot be physically tampered with (unless an intruder or hacker breaks in); WPS can also fall victim to brute force attacks, making it not the best solution. |

# Lecture: Network Security Technical Implementation Guides (STIGs)

**Content Author:** Dr. Michael J. Simko



## STIGs

An import aspect of hardening both hardware and software is utilizing STIGs. **STIGs are security configurations that apply either a technical, administrative, or physical control.** We can use many STIGs to provide a specific desired level of a protection on a switch, server, router or even networked printer. Microsoft Window's servers commonly can be scanned for STIG compliance while network printers, switches and routers typically have to be checked manually against a list of applied STIGs. There are STIG lists available for specific devices such as switches, routers, servers and more. Additionally, there are STIG checklists for software such operating systems, internet explorer and Microsoft Office Suites. In Windows based systems, multiples STIGs can be configured together in Group Policy Objects (GPOs).

## SCAP Scanner/STIG Viewer

**SCAP scanner is a tool that uses pre-defined STIGs to scan a system or piece of software for security compliance.**For example, a baseline STIG list provides best recommended security settings. The list is uploaded into the SCAP scanner which is then used to scan the said named device. The scanner searches for the configuration of these STIGs and outputs a report of security settings that are currently configured. The report will also include security settings that are not configured and associated vulnerability severity in the form of Category 1, 2 or 3 ratings. You should also be aware of the Open Vulnerability and Assessment Language (OVAL) which is another available standard for security services, tools, and assessments. Similar to SCAP, OVAL provides a baseline configuration of best-known security settings. OVAL content can actually be utilized with the Security Content Automation Protocol and provides means to assess machine state (configured or non-configured security settings), along with reporting results.

CAT1 is a high or critical finding while CAT2 is a medium finding. Category 3 findings are rated as a low vulnerabilities but should still be mitigated to an acceptable level based on the organization's risk appetite. Both STIG checklists and SCAP content are essential to Blue Team methodology. **STIG Viewer is simply the program that you can use to view STIGs.** STIG Viewer will sort vulnerabilities by severity (CAT1-3) and also provide the ability to color code STIGs for tracking completion. A STIG checklist can be created with each STIG marked green for completion, yellow for pending a configuration and red for not yet complete.

A picture containing icon

Description automatically generated

## Network Specific STIGS

Now that we have a basic understanding of STIGS, SCAP and STIG Viewer; let's review a few examples of basic STIGs. We will be looking at specific security setting examples for switches and routers, as they pertain to network security. Note: These are just a few examples, as there are hundreds of STIGs for each.

**Table 1**

Sample of DISA Network STIGs

|  |  |  |  |
| --- | --- | --- | --- |
| **STIG ID #** | **Severity** | **Title** | **Description** |
| V-14642 | High/ CAT I | The organization must implement a deep packet inspection solution when protecting perimeter boundaries. | Deep packet inspection (DPI) examines the packet beyond the Layer 4 header by examining the payload to identify the application or service. DPI searches for illegal statements, predefined... |
| V-12072 | High/ CAT I | Unclassified wireless devices must not be allowed in a Sensitive Compartmented Information Facility (SCIF) unless approved by the SCIF Cognizant Security Authority (CSA) in accordance with Intelligence Community Directive (ICD) 503, ICD 705, DIA SCIF policy requirements, the Authorizing Official (AO) and local Special Security officer (SSO). | Emanations from computing devices in the secured area may be transmitted or picked up inadvertently by wireless devices. |
| V-8066 | Medium/ CAT II | When protecting the boundaries of a network, the firewall must be placed between the private network and the perimeter router and the Demilitarized Zone (DMZ) | The only way to mediate the flow of traffic between the inside network, the outside connection, and the DMZ is to place the firewall into the architecture in a manner that allows the firewall the... |
| V-8046 | Medium/ CAT II | Network topology diagrams for the enclave must be maintained and up to date at all times. | To assist in the management, auditing, and security of the network infrastructure facility drawings and topology maps are a necessity. Topology maps are important because they show the overall... |
| V-18490 | Medium/ CAT II | An Intrusion Detection and Prevention System (IDPS) sensor must be deployed to monitor all Demilitarized Zone (DMZ) segments housing public servers. | The initial step in IDPS deployment is determining where sensors should be placed. Because attacks originate at the enclave perimeter and within the enclave boundary an IDPS implementation at the... |

Note: The content in the table was adapted from ["UCF STIG Viewer"](https://www.stigviewer.com/stig/network_infrastructure_policy/) (2018).

We briefly discussed a few common network STIGs that relate to content we discussed within this course. As you can see, a STIG in simple terms is telling you what to configure and then explaining why to do so. When viewing STIGs in STIG Viewer, you will commonly have the step-by-step procedure required to implement the STIG. In some cases, this information is not provided as you may have a different configuration on your network. If this is the case, you must research into how to configure the STIG based off your network setup and requirements.

|  |  |
| --- | --- |
| Icon  Description automatically generated | Visit the [DoD Cyber Exchange Public STIGs Document Library](https://public.cyber.mil/stigs/downloads/) to find more in-depth STIGs along with complete lists. |

Using STIG recommendations and requirements are a great strategy for introducing network security to a newly developed network.

## STIG Terminology

Use the following interactive flip-card activity to define some STIG terminology. Alternately, you may review a [printable/accessible version of the STIG terminology activity](https://ool-content.walshcollege.edu/CourseFiles/IT/IT204/MASTER/Week08/activity-FA22-NetworkSTIGs/printable.html).

Please **click on the boxes** below to reveal a description of each term.

© Walsh, All rights reserved