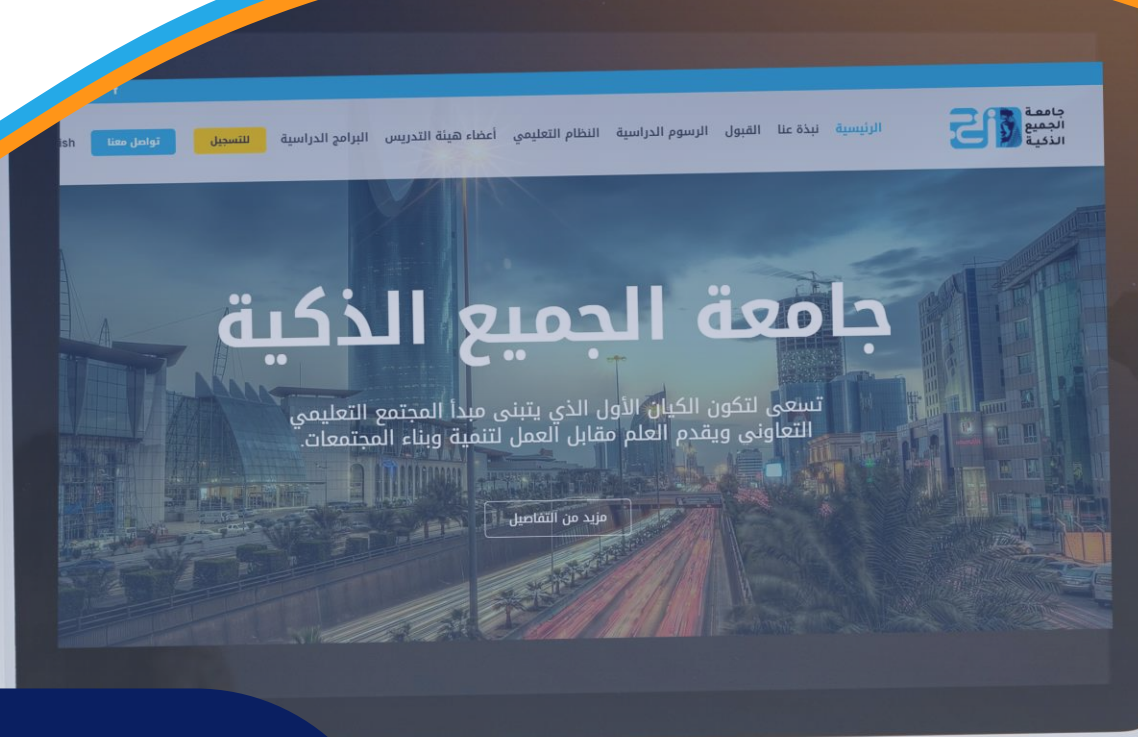




جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



IoT Security
Prepared by Dr. Abdelrhman Ahmed
Lecture 7

Promoting Physical Security

- **Intelligent Monitoring**

Video surveillance, while generally effective enough to supply evidence of a security concern, has many shortcomings. In the instance of a crime caught on tape, a guard will have to sift through upwards of 48hrs of video to find relevant video clips. There could also be 10 or more different cameras in the area that contain relevant video, making the process even more strenuous. With the implementation of motion detection, audio detection and alert systems, a security concern can be managed much easier and faster. A video feed that only shows activity allows a security guard to more easily detect a concern. Operation costs go down, storage needs decrease and relevant video retrieval simplifies.

- **Tampering Alerts**

Using smart cameras equipped with sensors or software that can detect misplacement surely increases the effectiveness of a security system. These tampering alerts are ideal for places with a high chance of vandalism like public places and schools. When a camera can alert any sign of tampering, the possibility of missing suspicious activity goes down. Without an alert system that uses sensors or intelligent video, a camera could be turned in the wrong direction for days and even weeks.

- **Perimeter Protection**

Building security can use beacons, RFID badges and even radio waves to secure the perimeter and allow access to specified individuals. Security can be notified in real-time about perimeter breaches and approaching threats.

- **Facial Recognition**

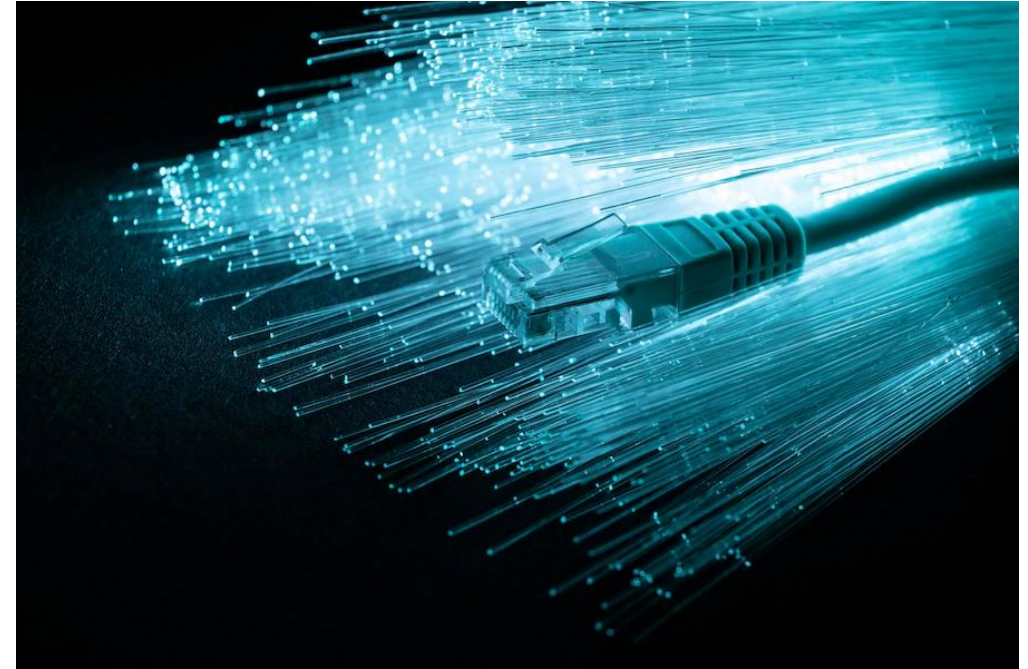
Perhaps one of the most intelligent advents in video surveillance is facial recognition. This software can not only identify individuals, it can even find signs of a possible threat by measuring key identifiers such as a high heart rate or nervous facial expression. These tactics can be used in places like casinos and high traffic situations such as sporting events. If these facial recognition techniques can use the internet of things to create automated alerts and events, such as notifying casino floor security of a suspicious character, threats can then be identified and addressed immediately.



- **Automobile Tracking**

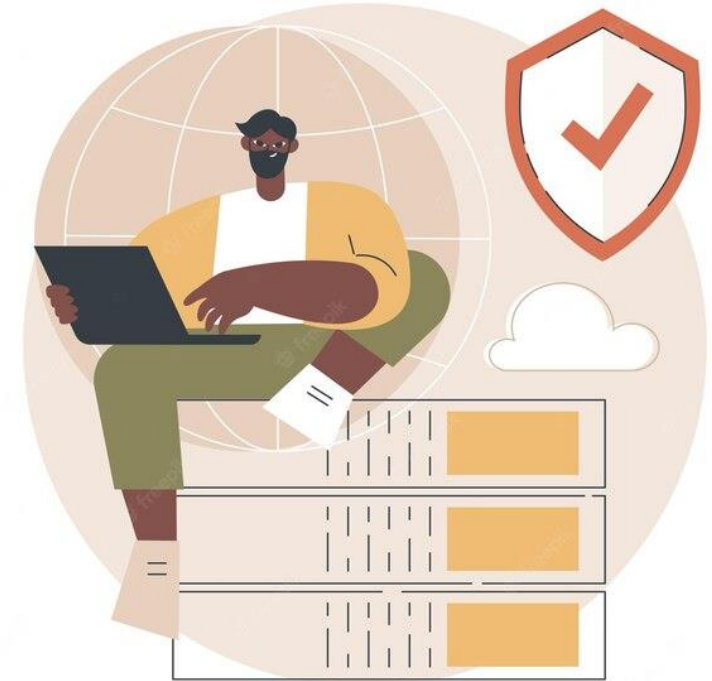
Intelligent systems such as License Plate Recognition software can elevate physical security effectiveness using automation and IoT. Law enforcement officers can connect license plate databases with automatic license plate recognition systems to more effectively identify drivers and locate offenders. A similar system could also be used very effectively in a secure entrance gate or smart parking garage to allow entry and track traffic coming in and out.

Attackers' task is comparatively very easy when they can enter the network they want to attack. Ethernet LANs are very much vulnerable to attack as the switch ports are open to using by default. Various attacks such as Dos attack at layer 2, address spoofing can take place. If the administrator has control over the network then obviously the network is safe. To take total control over the switch ports, the user can use a feature called port security. If somehow prevent an unauthorized user to use these ports, then the security will increase up to a great extent at layer 2.



Users can secure a port in two steps:

1. Limiting the number of MAC addresses to a single switch port, i.e if more than the limit, Mac addresses are learned from a single port then appropriate action will be taken.
2. If unauthorized access is observed, the traffic should be discarded by using any of the options, or more appropriately, the user should generate a log message so that unauthorized access can be easily observed.



Chapter 07

Physical Port Security

Port security

Switches learn MAC addresses when the frame is forwarded through a switch port. By using port security, users can limit the number of MAC addresses that can be learned to a port, set static MAC addresses, and set penalties for that port if it is used by an unauthorized user. Users can either use restrict, shut down or protect port-security commands.



Switch port security is a crucial element of network security. By following these 10 best practices, you can help keep your network safe from unauthorized access and malicious activity. It helps protect against unauthorized access to the network, as well as malicious attacks. By following the best practices outlined, you can ensure that your network is secure and protected from potential threats.

We will discuss 10 physical switch port security best practices, including disabling unused ports, using port security, and configuring access control lists. By following these best practices, you can ensure that your network is secure and protected from potential threats.



1. Utilize 802.1X authentication

802.1X authentication is a port-based network access control protocol that provides an additional layer of security to the physical switch ports. It works by requiring all devices connected to the switch port to authenticate themselves before they can gain access to the network. This ensures that only authorized users and devices are allowed on the network, while unauthorized ones are blocked from accessing it.

The way 802.1X authentication works is that when a device connects to the switch port, the switch sends out an Extensible Authentication Protocol (EAP) request for authentication. The device then responds with its credentials, which are verified against an authentication server such as RADIUS or TACACS+. If the credentials match, the device is granted access to the network; if not, the connection is denied.

1. Utilize 802.1X authentication

This makes 802.1X authentication an effective tool for preventing unauthorized access to the network, as well as protecting against malicious attacks such as man-in-the-middle attacks.

Additionally, since the authentication process happens at the port level, it is more secure than other methods such as MAC address filtering, which can be easily bypassed.



2. Implement port security features

Port security features allow administrators to limit the number of MAC addresses that can be connected to a port, as well as restrict which MAC addresses are allowed. This helps prevent unauthorized users from connecting to the network and gaining access to sensitive data or resources. Additionally, port security features can also detect when an unauthorized device is connected to the switch port and alert the administrator.

Port security features can be implemented in several ways. The most common way is by using static MAC address binding, where each port is configured with a specific list of authorized MAC addresses. This ensures that only those devices with the specified MAC addresses can connect to the port.

2. Implement port security features

Alternatively, dynamic MAC address binding can be used, which allows any device to connect to the port but limits the number of MAC addresses that can be associated with it. Lastly, port security can also be enabled through 802.1X authentication, which requires all devices attempting to connect to the port to authenticate themselves before being granted access.



3. Limit switch access to authorized personnel only

By limiting access to only those personnel who have been authorized, organizations can ensure that the switch is not accessed by unauthorized individuals. This helps protect against malicious actors attempting to gain access to the network and its resources. To limit access, organizations should use authentication methods such as passwords or two-factor authentication. Additionally, they should also implement physical security measures such as locks on the switches themselves, as well as restricting access to the area where the switches are located. By implementing these measures, organizations can help ensure that their networks remain secure from unauthorized access.

4. Utilize MAC address filtering

MAC address filtering is a security measure that allows only devices with specific MAC addresses to access the network. This helps prevent unauthorized users from connecting to the network, as each device has its own unique MAC address. To use MAC address filtering, an administrator must first create a list of approved MAC addresses and then configure the switch port to accept only those addresses. The switch will then compare incoming MAC addresses against the list and deny any traffic from unrecognized sources. This provides an additional layer of protection beyond basic authentication methods such as passwords or certificates.

Additionally, since MAC addresses are hard-coded into hardware, they cannot be easily changed or spoofed like other forms of authentication.

5. Enable the DHCP snooping feature

DHCP snooping is a security feature that helps protect against malicious DHCP traffic. It works by monitoring and validating DHCP messages on untrusted Layer 2 networks, such as those connected to user access ports. The switch will only allow DHCP responses from trusted DHCP servers, while all other DHCP requests are dropped. This prevents rogue DHCP servers from being used to attack the network or assign incorrect IP addresses to devices. Additionally, it can also be used to prevent DHCP starvation attacks, where an attacker sends out numerous DHCP requests in order to exhaust the available IP address pool. To enable DHCP snooping, you must first configure the switch with one or more trusted DHCP servers. Then, you need to enable DHCP snooping globally on the switch, and then enable it on each port where DHCP traffic is expected. Once enabled, the switch will start monitoring and validating DHCP messages on these ports.



6. Use private VLANs for additional layer of isolation

Private VLANs are a type of virtual LAN that can be used to segment traffic within the same physical switch. This is done by assigning each port on the switch to one or more private VLANs, which creates isolated broadcast domains for each port. By isolating ports from each other, it prevents malicious users from gaining access to sensitive data and resources on the network. Additionally, using private VLANs allows administrators to control which ports can communicate with each other, further increasing security. To configure private VLANs, an administrator must first create a primary VLAN and then assign secondary VLANs to individual ports. The primary VLAN acts as a trunk line between all the secondary VLANs, allowing them to communicate with each other while still maintaining their isolation. Private VLANs also provide additional benefits such as improved scalability and better performance due to reduced broadcast traffic.

7. Disable unused ports and services

Unused ports and services can be a security risk because they are often left open, allowing malicious actors to exploit them. By disabling unused ports and services, organizations can reduce the attack surface of their network and prevent unauthorized access.

To disable unused ports and services, administrators should first identify which ports and services are not being used. This can be done by using port scanning tools or manually checking each port. Once identified, administrators can then use the switch's configuration settings to disable those ports and services. Additionally, it is important to regularly monitor the switch for any changes in its configuration settings, as this will help ensure that all unused ports and services remain disabled.

8. Monitor switch port activity regularly

Monitoring switch port activity helps to identify any unauthorized access or malicious activities that may be occurring on the network. It also allows administrators to detect and respond quickly to any suspicious behavior, such as a sudden increase in traffic or an unexpected change in the type of traffic being sent through a particular port.



8. Monitor switch port activity regularly

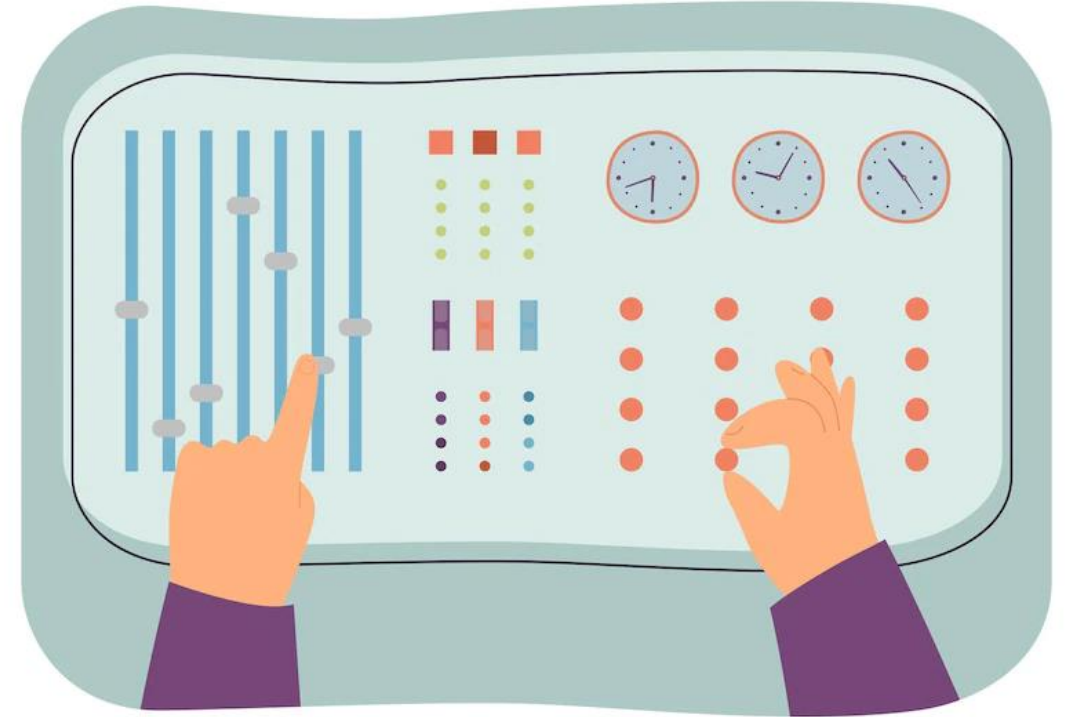
To monitor switch port activity, administrators can use tools like Network Access Control (NAC) systems, which allow them to set up rules for each port and track all incoming and outgoing traffic. This information can then be used to create reports that show who is accessing what ports, when they are doing so, and how much data is being transferred. Additionally, NAC systems can alert administrators if there is any suspicious activity detected on a port.

Administrators should also regularly review logs from their switches to look for any unusual patterns or anomalies. These logs can provide valuable insight into the types of traffic flowing through the network, allowing administrators to spot potential security threats before they become serious issues. By monitoring switch port activity regularly, administrators can ensure that their networks remain secure and free from malicious actors.



9. Configure storm control settings

Storm control is a feature that monitors traffic on the switch port and can detect when too much data is being sent or received. When this happens, it will automatically shut down the port to prevent any further damage from occurring. This helps protect the network from malicious attacks such as Denial of Service (DoS) attacks, which are designed to overwhelm the system with large amounts of data.



9. Configure storm control settings

Configuring storm control settings is relatively simple. The administrator must first determine what type of traffic should be monitored and then set thresholds for both incoming and outgoing traffic. For example, if the administrator wants to monitor broadcast traffic, they would set a threshold for how many broadcasts per second the port can receive before it shuts down. Once these thresholds have been set, the administrator can enable storm control on the port. If the port ever reaches the configured thresholds, it will automatically shut down until the administrator manually re-enables it.

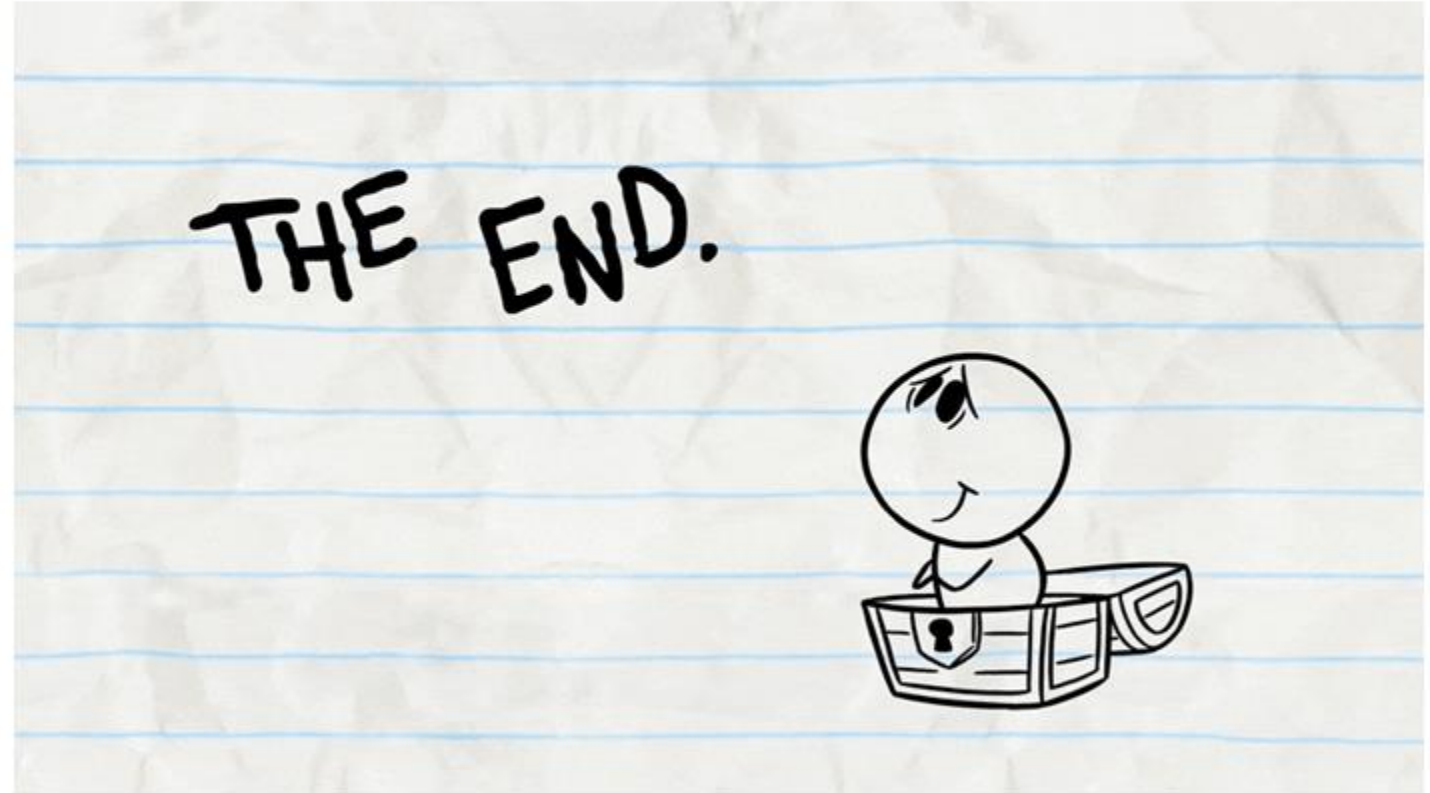
10. Utilize Virtual LANs (VLAN) to segment traffic

VLANs are used to logically segment a network into multiple broadcast domains, which can be based on department, application, or user. This allows for better control of traffic and improved security by isolating different types of traffic from each other. By using VLANs, it is possible to limit the scope of broadcasts, as well as restrict access between different segments of the network. Additionally, VLANs provide an additional layer of security by allowing administrators to set up port-based authentication, such as 802.1X, which requires users to authenticate before they can gain access to the network. Furthermore, VLANs allow for more granular control over who has access to what resources, making it easier to identify suspicious activity. Lastly, VLANs also make it easier to monitor and audit network traffic, since all traffic within a given VLAN is contained in one place.

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY