ADVANTECH

Enabling an Intelligent Planet

Technical Note

May, 2018

Why Security is Becoming More Important

Software Manager: Roger Cheng

Why Security is Becoming More Important

In the IoT world, the number of devices being connected to networks is growing. This is because in vertical markets such as automation, transportation, oil and gas, and power and energy, all operations and maintenance require constant observation in order to ensure consistent workflow. Real-time monitoring and prediction ability via the detection of abnormal events has become a trend in many industries.

As the most widely implemented standard and based on IEEE 802.3, Ethernet is being run on increasingly more instruments in addition to legacy I/O devices. Coinciding with this development, industrial IoT (IIoT), which utilizes industrial Ethernet and shares all mature components and technologies developed on the basis of Ethernet, is becoming the most common platform for connecting devices and creating convergence between information technology (IT) and operational technology (OT).

However, there is a tradeoff that must be considered when seeking to connect everything together. In this case, the tradeoff is between connectivity and security.

Although connectivity allows one to more easily access all network components, perform monitoring tasks, and troubleshoot any problem on a network, it also provides a means for unscrupulous attackers to obtain trade secrets or even money. Such open connectivity also means that even local networks are no longer closed and safe, and as the number of people relying on a network to perform their job duties increases, the level of remote access permission that is required will continue to grow as people become more dependent on cloud services.

Information shown on monitors and panels in control rooms is derived from data received from upstream edge components. This provides an opportunity for hackers to intrude a network via the edge components or switches/routers in a typical bottom-up intrusion, which, in addition to potential loss of trade secrets, can lead to a range of system problems resulting from zombie attacks, distributed denial-of-service (DDoS) attacks, or spoofing. This is why security continues to be of great concern in IIoT applications. Hence, determining the means to detect, predict, and prevent an intrusion or attack is the key point of cyber security.

Trending of IT/OT convergence

The convergence of IT and OT is driven by trends in IIoT.

In general, OT networks are transparent connections between machines/instruments (local site) and panel screens (control center). Such networks exchange traffic and signals that control the physical state of a system. Since transmitted data can be critical for monitoring and management applications (e.g., tunnel smoke detection and fire alarm control), real-time monitoring is critical to checking that there are no problems. To prevent malicious attackers from paralyzing a network or stealing confidential information during transmission, it is crucial to ensure that at least part of the information is encrypted.

IT networks, on the other hand, largely deal with data, with various logics and algorithms employed to make the data meaningful. This is then used as an input for any possible reference models to yield new market and business insights and to generate new revenue.

Basically, after big data are compiled, what is useful is classified so that norms and abnormalities can be identified. This provides intelligence that is then utilized to form rules as a knowledge base to provide a foundation for making predictions. This knowledge base is usually run on a super computer.

Given that such a computer would be physically protected by a cabinet and door locks (or even finger or face identification in high-security systems), the easiest way to intrude the computer thus becomes via the network. And so the most pertinent question from a system security perspective is thus: what is the most appropriate entry point?

In OT networks, it is difficult to control network access because the security is less stringent than it is in an IT network. In fact, an OT network is analogous to a superhighway that gives hackers access an internal IT network, which is precisely why the convergence of OT/IT networks raises substantial security concerns.

Considerations on Security

Cyber security is a broad topic that can be discussed from various perspectives. Generally, security threats can be categorized as either external or internal. External threats require protection measures such as firewalls, which can be implemented using a combination of hardware and flexible software in order to prevent attacks.

Internal threats can be more difficult to predict and prevent due to the wide scale of network infrastructure. Because everything is interconnected, there are various exploitable points and means to intrude a network internally. As such, a threat could come from any device or computer on the network edge.

As the access point or first bridge of a wide-range network, switches have long been a primary target for exploitation and are thus a key point for system security. When a threat arises, a switch is typically the first line of defense. It is therefore necessary that switches be equipped with various authentication, authorization, and accounting mechanisms to protect both the network and the switches themselves.

Intrusion prevention is thus the most critical objective of cyber security. To achieve this, the border nodes of a network should be capable of handling threat prediction and prevention, and since switches are usually deployed as the backbone of network infrastructure, they can serve as the ideal multi-level security mechanism.

Intrusion Motives and Types

Theft of Confidential Information

Confidentiality is particularly relevant to military and business networks but also to general personal privacy. Critical data are usually leaked due to illegal network connections, raw data capture, redirection, and snooping.

Network Disabling

Hackers can cripple a network by infecting computers with a virus or Trojan in order to create a network of zombie computers. Malicious software on the zombie computers can then be auto-launched or controlled by hackers to create a botnet storm to exhaust network resources.

Network Spoofing

Attackers can intercept field camera data and then transmit fake surveillance images to the intended destination of the original feed. The monitoring is thus spoofed because those monitoring the feed would not see anything wrong on their screens.

Intrusion Targets

A network is formed by a number of nodes and the links between the nodes. A network node plays the role of traffic exchange and path control and can be obviously considered the best target for intrusion because it is only these devices that provide a physical link to the network (by either a wired or wireless connection).

Network Node

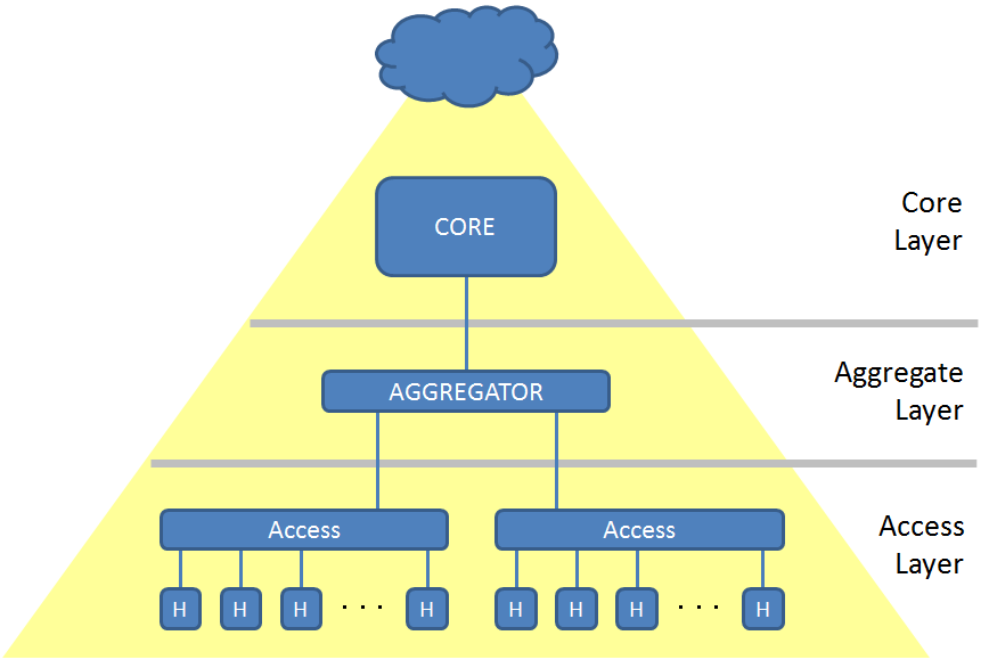
If a network node can be managed without strict protection measures (i.e., a user name and password), then it becomes easy to log into the user interface of the network node and change parameters to affect the traffic exchange and data routes. Once a switch has been compromised, hackers can reroute traffic or even create a bridge loop and then a broadcast storm by changing the switch's parameters.

Terminal devices in the network

Hackers can compromise both wired and wireless connections to access a network if there is no mechanism to distinguish an unauthorized user from an authorized one. Therefore, there's no ways to stop the intrusion to each terminal device like personal computers and data servers.

Security Concerns in Individual Network Segments

A network can be separated into different segments based on the traffic direction and data hierarchy. With this in mind, it is like a pyramid structure (see the image below). The bottom layer comprises an increasing number of end devices or sensors that collect data for transmission to a central control room. The middle layer is responsible for data aggregation and path definition. It is here that different types of traffic are classified and data routing is performed. The top layer is typically the core network. In addition to high bandwidth traffic exchange, it is responsible for transmitting large volumes of data to the cloud for analysis or some specific operation.



Access Layer

The access layer connects end devices or smaller-sized LANs. Since the scale of such networks is not relatively large, basic Layer 2 security functions are generally sufficient to prevent illegal access; this is achieved by using a limited number of hosts or performing authentication procedures.

The access layer presents a potential entry point that hackers can easily connect to with a laptop due to this network segment being deployed near the end user. Intrusions may be made via wired switches or wireless access points, and it is essentially “leaving the door open” if no security actions are performed on said switches and access points.

To reduce this risk, identification-checking procedures, such as username/password checking or MAC address inspections, are useful for limiting access by untrusted hosts.

Aggregate Layer

To be a data collector and exchange hub, an aggregate layer needs high-grade security functions such as IP or service-level data authentication and filtering.

The access layer is connected to the aggregate layer to send traffic upstream for data relay or exchange. This means that all traffic exchanges in this segment have already passed inspection in the access layer, even if no security checks were made in that layer.

This makes the aggregate layer a second line of defense by performing inspections of all frames, which usually means verifying the source/destination IP address and source/destination MAC address.

Core Layer

Threats to a core layer switch are generally external threats and can be observed and filtered by a firewall device. This is particularly a concern for WANs.

The core layer plays the role of a gateway and connects to WANs or well-known clouds. This layer denies access to external threats as a means to protect internal traffic exchanges rather than performing internal security measures. The security scope in this layer is relevant to cyber security but not bottom-up intrusion.

Cases and Applications

User Permissions in Switch Management

In switch management, user permissions are critical because once an unauthorized user has access to a switch, he or she can easily execute data redirection, snooping, or even a botnet storm.

Typically, a switch stores configuration data, including user account and password data, and this is often visible and can be copied by malicious users. Password encryption is intended to make such data unreadable by utilizing a security key that is known only to the switch. This prevents passwords from being leaked and provides a strict level of security for switch management.

In remote access contexts, data are not logged for devices that use an authorized account and password. To provide a second line of defense against unauthorized users, switches should be configured to approve network access only for specific IP hosts and to control which protocols (e.g., HTTP, TELNET, and SNMP) are allowed.

Furthermore, switches should store user operations and instructions in a record and generate event logs with synchronized time. This makes it easier to identify who has modified a system in the event of problematic switch or network behavior. For this, a time synchronization protocol as NTP/SNTP should be made available. SYSLOG and SMTP are also essential items that can publish a text log/e-mail to a remote server and record changes in a situation for a specific period of time.

To perform basic user control, implementing a timeout and maximum number of retries for a user session are common means for preventing illegal activity.

Data Confidentiality

SSL encryption/decryption can be utilized to ensure confidentiality during data exchanges.

The most critical content is encrypted at the egress stage and then decrypted at the ingress stage, for which algorithms applied to TCP/IP applications (e.g., HTTP, TELNET, and SNMP) are utilized. Corresponding to these services, HTTPS, SSH, and SNMPv3 are defined to encrypt the frame payload with AES/DES/3DES algorithms defined in the SSL library.

In the event that traffic is intercepted by hackers and critical information is leaked, the encryption/decryption between the two access ends improves the level of security.

At the transmission end, data packets are encrypted so that the information therein is unidentifiable. At the receiving end, the packets are then decrypted with negotiated security key, thus making the content identifiable. If packets are intercepted, a hacker may spend an inestimable amount of time trying to crack the encryption algorithm or may be unable to crack it ever.

System Availability

Responsiveness to Events

To ensure network availability, switches use different methods to notify supervisors of irregular network behaviors, the most simple of which is the flashing of LEDs in the event of a critical event. This might also be accompanied by follow-up procedures such as a system reset/reboot.

For example, if a network loop appears for unknown reasons, apart from generating a log and triggering a flashing LED, the only follow-up action performed by the system would be to disable the port in which the loop was detected in order to isolate the loop. This, however, is only a work-around to stop the critical situation from continuing—it does not really solve the problem.

To ensure an appropriate level of responsiveness, continuous monitoring must be performed around the clock. This routine task involves polling the status of switches and performing sampling for a given period. After records have been collected and computations performed, “normal” situations are defined and “abnormal” situations are assessed on the basis of user-defined thresholds.

For example, assume that the traffic on a port (port utilization) is less than 10M for the last 2 weeks but it increases to 100M immediately in the most recent sampling. By computation, the average port utilization for last 2 weeks leads to the conclusion that 10M is normal, and so the 100M traffic peak can be considered abnormal.

In its simplest form, the average of each sample value over time is computed and compared to determine whether the new sample value differs significantly from the previous average.

Resource Availability

Bandwidth is the most critical concern when discussing network resources.

The mechanism of limited and guaranteed bandwidth keeps the network operating efficiently. For lossless traffic, guaranteed bandwidth makes all critical connections stable, whereas limited bandwidth drops invalid and dangerous frames as a preventative measure against network storms. Switches are equipped with storm control and rate control functionalities to secure the bandwidth availability.

DDoS attacks also pose a significant threat to resource availability, but such attacks can be prevented by using a filter to identify and drop illegal frames.

Restricted data flow

Restriction by Port

The most basic way to prevent illegal access via port connections is to disable any not-in-service ports. While this approach is always simple and effective, there may be difficulties or delays when a system administrator is required to enable a port once the port is needed. Thus, although it seems feasible, it may prove to be quite inconvenient.

802.1X remote authentication solves this problem with a trusted authorization process by a professional security server such as RADIUS. When an unauthorized host issues an EAP process to exchange account information with network components, this issues a follow-up RADIUS process with a RADIUS server. When authentication is completed, the connected port is unlocked.

Restriction by MAC Address

A simple way to deny access to unauthorized users is to add the MAC addresses of trusted users to a switch's MAC address table and then disable the learning mechanism of this port.

Another way is to limit the maximum number of MAC addresses that can be learned for a port. To maintain the appropriate learning status, a log of MAC learning violations is generated and the system administrator is actively notified of any violations.

Restriction by IP Address

Each illegal access method is based on a peer-to-peer connection via TCP/IP and is concealed in various services or applications (e.g., HTTP, TELNET, and FTP). Hackers can connect to critical data servers by using an illegal IP address. An efficient way to defend against this and only allow trusted IP addresses to obtain network access is to create a whitelist so that connections with illegal addresses are dropped.

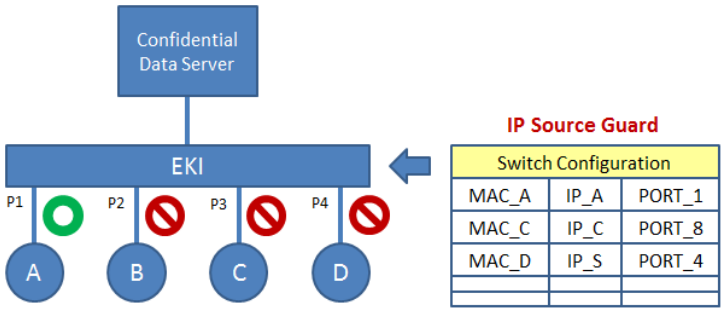
To ensure that untrusted hosts are not given access, a whitelist of trusted IP addresses—otherwise known as an IP permit list—can be manually configured, and only hosts with these addresses are given access. In a network with DHCP, security checking procedures are generally performed on the DHCP server (e.g., specific MAC addresses are allowed to be allocated specific IP addresses). DHCP Option 82 can also be utilized so that only fixed IP addresses are assigned.

To assist the DHCP server, a mechanism snoops legal DHCP assignments and automatically adds the MAC address, IP address, and connected port of trusted hosts to the whitelist. This prevents illegal access from privately configured IP addresses. In short, if a host has not been allocated an IP address by the DHCP sever, this means that it is not on the whitelist. Thus, network access would be denied for that host.

Following the description above, if an untrusted host cannot be allocated an IP address from the DHCP server, a fixed IP address cannot be used as an alternative because it would not be in the whitelist and thus would still not be allowed to access the network via this switch. We create a procedure to snoop DHCP protocol and automatically add a valid IP–MAC–port combination to the whitelist. This mechanism is called DHCP snooping.

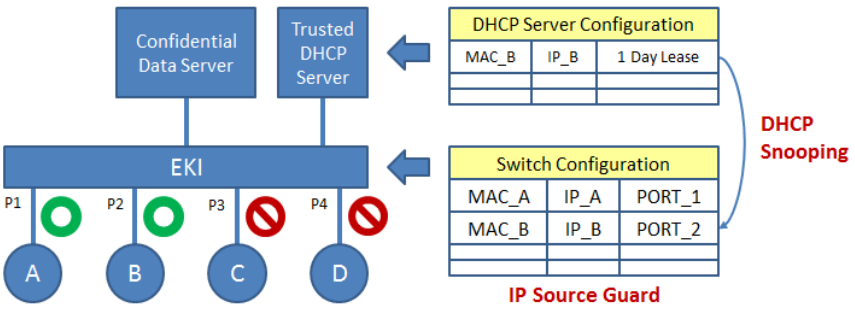
Theory of IP-based security

Legal host with known IP and MAC address is bundled on a specific port to access the network



- A is in trusted list and connect to correct port (P1), permit to access the network
- B is NOT in trusted list, deny to access the network
- C is in trusted list but connect to incorrect port (should be P8), deny to access the network
- D is in trusted list but IP address is incorrect (should be IP_D), deny to access the network

Either in switch trusted list or in DHCP server allocate list and allocate IP address from it could be allowed to access the network



- A is in trusted list and connect to correct port (P1), permit to access the network
- B allocates IP address from DHCP server and which info. is recorded into trusted list
- C and D cannot allocate IP address from DHCP server and aren't in trusted list

Restriction by Flow Content

Traffic is a constant in computer networks and it is impossible to know when new traffic will appear. For this reason, security measures are essential to protect against malicious attacks such viruses or attempts to disable the network. At this time, it is more flexible to implement user-defined content filters as a gatekeeper.

Such filters are designed according to an Ethernet frame's architecture and are divided into Layer 2 (MAC level), Layer 3 (IP level), and Layer 4 (service/application level). This distinction also provides a means for different actions to be taken to grant or deny permission for traffic seeking access to a network.