Securing Network Infrastructure and Switched Networks

Richard Wagner

Securing Network Infrastructure and Switched Networks

Richard Wagner,
August 21, 2001

Overview

It seems that the attacks that get most of the attention in the media are borne from the creative minds that exploit limited resources by attacking from afar through the Internet. While there are many reasons behind an attack, proving ability, earning recognition and achieving a level of notoriety certainly inspire many of them.

If causing harm to a company and/or stealing their intellectual property are the primary goals, more efficient attacks can be launched against the company's infrastructure. The infrastructure resources vulnerable to attack are not as limited as those available to the Internet hacker. Often, more attention is paid to protecting intellectual property from the Internet hacker while the data flows freely across infrastructure that lacks simple protection.

Enhancing infrastructure security can simply be an extension to a good network design that applies network availability principles such as monitoring, redundancy, effective disaster recovery and protection of assets from damage.

Fundamentals

In protecting the infrastructure, the data security foundations of integrity, availability and confidentiality can be taken to extremes. The implementation of strong infrastructure can carry an enormous price tag, whereas being thrifty can make one a more susceptible target. A balance risk and cost must be set at all stages, from the purchase of infrastructure to the labor required to maintain the watch.

Availability

The most vulnerable aspect of a network infrastructure is also the primary reason for its existence, the flow of data. This infrastructure is often complex, interdependent and can be spread across miles of internal company territory. These components form a chain, of which the breaking of any link can get an attacker the desired effect.

Common availability attacks relating to infrastructure include the following:

- Tampering with physical media as it crosses non-secure areas;
- Causing network access devices to become inoperable;
- Disturbing routing protocol information.

A key principle to ensure availability is redundancy. Without critical analysis of how a network can fail, the investment in redundant equipment will not be fully realized.

Confidentiality

More difficult attacks involve unauthorized eavesdropping of network traffic because it typically requires physical access. If the infrastructure is compromised in such a way that eavesdropping can occur, most of the work to attack the integrity of a network has already been done.

Common confidentiality attacks relating to network infrastructure including the following:

- Inserting a host into the network that eavesdrops on traffic;
- Modifying switch configurations to bypass network security devices;
- Giving an inside host an external path to illegally export data.

Integrity

Altering the data streams crossing the network infrastructure compromises integrity. The damaged caused can include the corruption of data, sabotage of core business plans and impersonation of legitimate users to gain even further access to the target.

Common integrity attacks relating to infrastructure include the following.:

- Inserting a host into the network or compromising an existing host that causes network traffic to be sent to it, forwarding an altered data stream to the original recipient.
- Cracking eavesdropped passwords.

As each topic is presented in this text, codes are appended to the titles to indicate what aspect of security is affected: (A) Availability, (C) Confidentiality, (I) Integrity.

Protecting the Environment

- Physical Security [ACI]

Network devices are usually easy targets due to a lack of human presence in their storage locations. A locked door on cable distribution facilities and wiring closets won't be enough if the space is shared with other uses such as telephone, power and storing office supplies. If exclusive access to the cable distribution facility is not possible, install an enclosed rack that has a unique lock and key. Everyone has a copy of the key that comes pre-installed on the rack. Since it might not be feasible to put a security camera on every wiring closet, consider putting switches on doors to the room and the cabinet itself that will alert the Network Management System (NMS) or security personnel that the location is being accessed.

Data Centers typically have the best physical security. Since personnel ranging from email administrators to the cleaning crew use this room, an enclosed rack should be used to protect network infrastructure. Again, it is crucial to make sure the factory lock is changed. Since many valuable and vulnerable points exist in the Data Centers, security cameras are easier to justify in these locations. Access to the Data Center should be controlled and recorded for auditing purpose with a card key system.

In the Data Center, raised floors offer great hiding places for eavesdropping laptops or devices that tap into cable infrastructure. Consider using floor tiles that are physically fastened to the supporting framework and periodically inspect the area for devices that should not be there. Documentation of the approved existing conditions will make inspections more convenient.

Once physical access is obtained, many network devices can easily be compromised to recover passwords, learn/change configurations, disable equipment or open up a back door for later use. Hosts can be added to the network and additional links can be installed to bypass security devices. Reporting, configuration audits and documentation also help detect these types of tampering and will be covered later in this paper.

For extremely valuable systems, rooms or devices can be completely enclosed in an electronic shielding. For rooms, this is a massive undertaking where simple progress of the cable plant can render the protection ineffective.

Interpol's document "IT Security and Crime Prevention Methods" tells us:

> Despite all precautions, it is still possible for a determined intruder to eavesdrop on information by picking up and interpreting electromagnetic emissions from the Personal Computer or workstation. In a manner somewhat similar to the way in which it is possible to detect the operation of a television receiver and determine which channel is being watched. This type of eavesdropping is most likely to occur when very sensitive information, such as that of high commercial value or dealing with matters of national security is involved.
>
> Use equipment with no or limited signal leakage ('tempest') or put the equipment in a shielded room. Although effective, those methods are expensive and are only to be recommended when there is an extremely high risk. Optical fibres can be used to prevent emission leakage from the lines running between peripherals and the Local Area Network (LAN).
>
> Encryption of the Wide Area Network (WAN) will not stop electromagnetic emissions but the eavesdropper will not be able to use the information without the encryption key.[1]

A sample of a supplier of room shielding systems can be found at http://www.intpro.co.uk/room.htm.

- Utilities [A]

Networking equipment often exists in areas that lack dedicated climate control, diverse power or well-planned fire protection. These systems run the risk of failure even without tampering.

[1] Interpol, IT Security and Crime Prevention Methods: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp#51 (section 5.1.5)

Power

Uninterruptible Power Supplies (UPS) can be used to keep equipment communicating in case of power failure.[2] Small UPS units can be used to provide power to network equipment, but they are worthless if there is no way to notify someone to restore power prior to depleting the batteries. UPS units can report status via Simple Network Management Protocol (SNMP) and SYSLOG functions (described later) to report supply-power failures, failed batteries or batteries nearing depletion. UPS units also can have "dry contacts", which are discrete switches that can be used as input to alarm and notification systems.

If the UPS does not support SNMP or SYSLOG, use a single managed network device that has redundant power supplies. If one of the power supplies is wired directly to the power source, a power outage will cause that power supply to fail and the switch itself can notify NMS of a failed power supply. Be sure that the remaining power supply/supplies can sufficiently power the unit else the message may never get out.

Cooling

In some situations affecting the temperature control of the infrastructure's environment may lead to overheating and malfunctioning. This can be as simple as blocking airflow to the device or disabling the cooling system. Many networking devices have temperature sensors that can report via SYSLOG or SNMP. Also, a temperature sensor or cooling unit alarm indicator can be installed that will alert the NMS.

In critical areas such as Data Centers, redundant cooling systems should be in place and monitored closely. The physical security of the cooling system is extremely important. As the cooling system works to remove heat from the Data Center and exhaust it outside, vulnerable parts of the system exist outside to the building. If this external presence is damaged, overheating can occur quickly with repairs taking many hours or days to complete.

While the UPS units in a Data Center may keep the equipment running before the backup generator can operate, the cooling units typically do not run on UPS power. Disabling the generator may lead to overheating in the Data Center even before the UPS depletes its batteries!

Fire Protection

Exploiting fire protection is an extreme measure of a desperate attacker. Activation of this system can easily knock a whole Data Center down! Unfortunately, there are not many options once a fire protection system is in place. The key is to prevent activation of the system by requiring multiple events to trip it while providing means to delay or abort activation. Understanding the operation of the fire suppression system can prevent it from affecting the availability of the systems it protects.

A "staged" dry-pipe system is less likely to shower your equipment with water before the presence of a fire can be verified or eliminated. These systems don't store water directly above the equipment until certain conditions are met and the actual delivery of water requires multiple events to take place. During a false alarm or quickly rectified situations, the activation of the system can be manually aborted. An expensive alternative is computer-friendly FM-200. Even

[2] Additional information about UPS units can be found at http://www.jetcafe.org/~npc/doc/ups-faq.html.

though equipment won't be damaged, fire protection systems can also cut off power and instruct UPS units to shut down.

Protecting the Network Media

- Crossover Cables vs. Switches [ACI]

At the Ethernet network segments where only two hosts exist, a simple crossover Ethernet cable can take the place of a hub or switch. Eliminating the complexity of the hub or switch makes it harder to eavesdrop, alter the data flow or cause communications between the two devices to fail.

Without a switch to notify NMS of port state changes, the host(s) on the crossover cable should provide that reporting. Constant monitoring of that link or a service provided through that link could also be performed at frequent intervals. If the connection were interrupted to place a hub or switch between the hosts, the change could go unnoticed if it occurs between monitoring intervals.

- Wireless Networks (IEEE 802.11) [ACI]

Wireless communication can be eavesdropped and unauthorized hosts can transmit data on your network. Many SANS articles exist that discuss the security of wireless LANs.[3]

- Copper vs. Fiber [ACI]

As the premise cabling snakes its way through the building, it is extremely difficult to ensure its security. While either type of media can be easily cut, fiber optic media is harder to "tap" for eavesdropping than copper media.

The most vulnerable location is the cable run between campus buildings. Fortunately the distance requirements usually eliminate copper media from being usable. Secure conduit access points (hand-holes) outside the building for these critical data paths.

The use of fiber optic media for all end-user workstations is expensive in both cable plant and network device costs. A good compromise is to use fiber optic media only for connectivity of critical hosts. To save costs, a single fiber optic run could be used to connect a network device located near a cluster of end users. Copper media could then be run in the immediate area and not through unprotected common areas. The protection of that switch could then become an issue.

- Diverse Redundant Physical Paths [AC]

The enhanced availability of redundancy can be rendered completely useless if the only conduit leading to/from the location is severed. Effective cable plant design with high availability in mind will have alternate paths to/from network device locations. Be sure that the network's logical design will properly use these alternate paths in case of partial failures. Traffic balanced across multiple diverse links can also hinder effective eavesdropping. For the intended eavesdropping by intrusion detection, be sure to somehow get both paths.

[3] Refer to http://www.sans.org/infosecFAQ/wireless/wireless_list.htm and Bob Szacik's report at http://www.sans.org/infosecFAQ/wireless/homerf.htm

Managing Network Devices

- Authentication, Authorization and Accounting: TACACS/RADIUS [CI]

  Authentication
  Managed network devices can be configured to authenticate users that attempt to change the configuration. Alerts can be generated that inform NMS of any attempts to connect and any changes to the configuration.

  Authorization
  Authorization levels can be set so that users can be limited to certain commands per job their function and the company security policy. Cisco's online documentation covers this feature thoroughly.[4]

  Accounting
  The changes to the system can be attributed to a certain user's activity.

Systems used to provide these functions include Terminal Access Controller Access Control System (TACACS) and Remote Authentication Dial-In User Service (RADIUS).

The Internet has valuable information on TACACS[5] and RADIUS[6] along with specific documentation on the Cisco web site.

- Out-of-Band Management [ACI]

Network devices often participate as an IP host in the networks they service. This IP host is used to inform NMS of events via SNMP traps or SYSLOG. This address can also be used to change the configuration via TELNET or SNMP. This IP host can be attacked to affect the functionality of the device by configuration changes or exploiting a vulnerability to cease its operation. An availability attack on the IP host can prevent it from reporting events to NMS, possibly hiding other activity.

Placing this IP host in a separate "management network" from the production network makes it much more difficult to reach or attack. The successful disabling of the production network will be less likely to affect the independent management network. This network can be completely isolated, protected by a firewall or filtered with router Access Control Lists (ACL).

Eavesdropping of traffic used to manage the network infrastructure can have sensitive information such as password sent in clear text. Segregation of this traffic can help prevent eavesdropping.

---

[4] http://www.cisco.com/warp/public/126/NMS_bestpractice.html#securityman
[5] http://www.de.easynet.net/tacacs-faq/tacacs-faq.html
http://www.sans.org/infosecFAQ/netdevices/TACACS.htm
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt2/sctcacs.htm
[6] http://www.livingston.com/marketing/products/radius.html

Attacks on the IP host in the network device and network switch security are presented in Aaron Turner's SANS article.[7]

- SYSLOG [ACI]

Managed network devices can be configured to report events via SYSLOG. Reported events can vary by the configuration of the device. If an event occurs that should be reported, the management processor will send a one-way message via a connectionless IP message (UDP port 514). Another IP host, typically a NMS, will receive, evaluate and possibly alert personnel based on the content of the SYSLOG message. These messages can be easily spoofed, intentionally causing false alarms and making legitimate messages hard to believe or find.

- Simple Network Management Protocol (SNMP) and SNMP Traps [ACI]

SNMP can be used to change device configuration or query devices to get status and build statistics. Since SNMP version 1 is intrinsically insecure, security-minded planning is a must. Consider using out-of-band management and SNMP version 3.[8]

Much like SYSLOG messages, managed network devices can be configured to report events via SNMP traps. These messages can also be spoofed, blocked or altered. Additional information is necessary to properly identify the reporting device. Again, out-of-band management can help prevent these issues.

Increased Availability Through Redundancy

- Design with Redundancy and Security in Mind [ACI]

Implementing redundancy in a network is much more than ensuring that you have two of every device. Often, the network is designed to withstand the total loss of a redundant device where the loss of a single link can impair availability. Evaluate and predict the data flow based on many types of failures, from the loss of a link to the loss of a routing protocol peer. Proper reporting to NMS can alert to these events and proper design can eliminate these often-overlooked weak spots. The event can be completely separate from your equipment yet still affect your availability. Be sure that the loss of a peer device not under your control will not affect availability in your own network.

- Balance for Capacity [AC]

To better resist denial-of-service (DOS) attacks and make more efficient use of resources, design the network so that redundant equipment is used simultaneously. As enhanced capacity is explored as a way to minimize the effects of a DOS attack, be sure to consider the capacities of all equipment involved. A small data stream can cause big trouble on a vulnerable server. The balancing of traffic across different parts of the network infrastructure also makes eavesdropping difficult.

- Load Balancing Devices [A]

[7] http://www.sans.org/infosecFAQ/switchednet/switch_security.htm

[8] Jose Luis Camacho, SNMP and security: http://www.sans.org/infosecFAQ/netdevices/SNMP_sec.htm
Charles Carter, SNMP with Cisco Routers: http://www.sans.org/infosecFAQ/netdevices/router.htm

Load balancers can operate at all layers of the OSI model. These devices typically execute their operation code in hardware rather that software, giving them much better performance over software-based servers. These devices can translate and redirect specific traffic while dropping all others. With its involvement in the communication between clients and servers, some attacks won't work properly without direct access to the server. While a load balancer is no replacement for a firewall, it can effectively filter traffic and manage TCP connections so that web servers are not directly hit by certain DOS attacks.

The integration of firewalls and load balancers can provide secure and highly available networks.[9]

Another feature of network infrastructure devices that interact with data streams is Cisco's TCP Intercept feature. While not a load balancer, it uses similar techniques to combat SYN floods.[10]

- Diverse Chassis [ACI]

Using VLANs can make more efficient use of switches, especially when the cost of redundant switches is considered. Do not allow the same switch or mesh of switches provide connectivity to networks segregated by security devices such as firewalls and routers. Several attacks can affect the configuration of the switch or overwhelm it so that it does not properly segment VLANs. The separation of switches that provide connectivity to these segregated networks also makes it easier to spot moved or added cables.

Better security is achieved by using separate switches for networks that are segregated by a firewall, router with ACL or an isolated out-of-band management network.

Securing Ethernet Switches

Unfortunately, the features that offer the most flexibility and ease of configuring a network offer many opportunities for attackers to compromise networks. Generally, static configurations of protected devices in small transit networks are much harder to compromise than a dynamic protocol making decisions based on external input. Most of these exploitable features are enabled by default.

- Switch Trunk Links [ACI]
  - Inter-Switch Link (ISL) Trunking
  - IEEE 802.1q Trunking

[9] Gregory Yerxa: http://www.networkcomputing.com/1102/1102ws1.html
[10] Cisco Systems' TCP Intercept: http://www.cisco.com/warp/public/cc/pd/iosw/iore/prodlit/576_pp.pdf

VLAN Trunking is the use of one link between switches to carry traffic for more than one VLAN.[11] This replaces the need of running multiple physical media between switches, each carrying an individual VLAN. ISL is a Cisco-proprietary trunking protocol and 802.1q is standards-based.

The default behavior of Cisco ports is to negotiate a trunk if the connecting device initiates a trunking protocol.[12]

If a connecting device negotiates a trunk with a switch, it can participate in any VLAN present on that switch and possibly any VLAN in the entire network! This gives an attacker a way to influence traffic in order to capture or alter it. Hosts can be attacked directly, possibly bypassing security devices such as intrusion detection, firewalls and router ACLs.

This is a case where static configuration and manual administration prevents problems. Trunk links are entirely predictable in a planned network. The trunking capabilities should be explicitly disabled on non-trunk ports. Trunk ports should be enabled to prevent negotiation problems or connections to non-trunk hosts.

- Trunk VLAN Membership and Pruning

The default behavior of trunk links is to allow all VLANs on the network to cross it. A performance feature of some switches will remove ("prune") VLANs from a trunk if there are not any VLAN member ports on the other side of the trunk link.

If the default behavior is permitted, taking control of a trunk link will allow access to all VLANs in the switched network. Placing ports in the previously pruned VLANs can reverse the automatic pruning of VLANs from trunks. Also, if a VLAN carrying sensitive information is only allowed in certain areas, default trunk settings will allow the presence of that VLAN on any switch in the network. This could give access to the Accounting VLAN in a remote cable closet across the campus!

In order to prevent such attacks, it is recommended that all trunk links be manually configured. Trunk links can be manually pruned to only allow certain VLANs. Since trunks are backbone links to the network, their manual configuration is feasible even in large LANs.

---

[11] Cisco Systems, VLAN Trunk Links:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_2/config/e_trunk.htm#xtocid155051

[12] Default Trunking behavior of Cisco Switch ports:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_2/config/e_trunk.htm#xtocid155056

- Virtual Trunking Protocol (VTP) [ACI]

VTP is a proprietary protocol that provides administrative ease-of-use for managing VLANs on switches.[13]
VTP must be configured/enabled before any additional VLANs are configured on the switch. Its only security is the VTP domain name, which it broadcasts that information out when trying to discover VTP-enabled devices on its trunk link.

Devices whose VTP domain names match will work together to maintain a list of VLANs in the domain, allowing changes to be propagated per their set mode. Each switch can be set to one of three modes:

- Server: This switch can add and remove VLANs and will implement VLAN changes from other servers.
- Client: This switch will implement changes from VTP servers, but cannot add/remove VLANs, even on itself.
- Transparent: This switch ignores all VTP messages, but will pass them along other trunks. The VTP domain need not match for this switch to propagate VTP messages between foreign domain members.

The default behavior of a Cisco switch is to negotiate a trunk link if the connecting device initiates a trunking protocol. If a device or host negotiates a trunk link with a Cisco switch, it can use VTP to:

- Learn the VTP domain name
- Learn of all VLANs configured in that domain
- Become a server and effect VLAN changes on that domain
- Participate in any VLAN within that domain (this is achieved via trunking alone)

Extending trunk links or the VTP domain to devices that under some other administrative control can make their vulnerabilities your own. This also means that one compromised switch in any VTP domain can have its configuration altered to participate in all aspects of VTP.

The benefits of VTP must be weighed against the risk of having all VLANs compromised or deleted. In a configuration-controlled environment with competent personnel, VTP's benefits are minimal. The most secure setting is Transparent Mode. Static configuration and manual administration present fewer opportunities for exploitation.

- VLAN Membership Policy Server (VMPS) CI

VMPS[14] is a proprietary protocol that uses the MAC address of a LAN host to determine which VLAN it should belong. Properly deployed, this is an effective means to discourage unauthorized hosts on a LAN.

---

[13] Cisco Systems, VTP: http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb2/vlan.htm#xtocid299187
[14] Cisco Systems, VMPS:
http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35wc/sc/swgvlans.htm#xtocid1196655

The system can place previously unknown MAC addresses into a default VLAN or shut the port down, denying all access. This protocol also restricts which VLANs are available on a certain switch, preventing the existence of a sensitive VLAN in an insecure area.

This feature is hard to maintain in dynamic LAN environments where MAC addresses change often. This administrative overhead can be justified for conditions where security must be tight. The database for this protocol is stored on a server and is retrieved via TFTP, which is vulnerable to spoofing, alteration or denial of service.

- Etherchannel [AI]

Etherchannel[15] is a proprietary method of port aggregation. Multiple links (Fast Ethernet or Gigabit Ethernet) are bound together to form a single logical link with higher throughput. This feature is typically used to enhance throughput on backbone links that would otherwise be over-subscribed.

The default behavior is to automatically create an Etherchannel if the connecting device initiates negotiation. This allows the port to operate in either mode. When used as backbone links, the physical media might cross through less secure areas. If one of the multiple links is removed, it can operate as a normal LAN host or trunk, possibly using the ISL and VTP features to participate in the network. This can be a way to introduce an attacking host into the network. Use NMS to report the link loss because the loss of throughput might not be noticed during low traffic periods or on links that are not sufficiently loaded.

The manual configuration of all links to explicitly allow or deny Etherchannel operation will prevent standard Ethernet hosts from properly communicating on individual links in an aggregated set.

- Port Security [CI]

Cisco's Port Security feature[16] restricts the allowed MAC addresses on a per-port basis. A specific MAC addresses are specified so that no others can transmit on that port. This can prevent attacks such as overloading the bridge table to confuse the switch into behaving like a hub or ceasing communication.

This is easier to implement on small transit networks such as firewall boundaries where the hosts' MAC addresses don't vary. This solution does not scale to any but the smallest of LAN environments.

---

[15] Cisco Systems, Etherchannel:
http://www.cisco.com/warp/public/779/largeent/learn/technologies/fast_echannel.html
[16] Cisco Systems, Port Security:
http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35xu/scg/kiconfig.htm#xtocid57457

- Cisco Discovery Protocol (CDP) ACI

Another proprietary convenience feature of Cisco devices is the CDP.[17] This protocol is enabled by default on all Cisco devices. It broadcasts detailed information about the device across all supported network types once every minute by default. This information can be used to enumerate the network.

Here is sample output from a Cisco switch that has two switches attached:

```
Console> (debug-eng) show cdp neighbor
Port Device-ID              Port-ID          Platform       Capability
---- ---------------------- ---------------- -------------------- -----------
4/2  000041770(Workgroup Swi 5                WS-C1201             T
4/4  000102703              2/2              WS-C2900             S

Detailed information can be gained by performing a detailed query:

Switch# show cdp entry *

-------------------------
Device ID: talSwitch14
Entry address(es):
  IP address: 172.20.135.194
Platform: cisco WS-C3548-XL,  Capabilities: Trans-Bridge Switch
Interface: GigabitEthernet0/1,  Port ID (outgoing port): GigabitEthernet0/1
Holdtime : 121 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.2)XU, MAINTENANCE IN
TERIM SOFTWARE
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 17-Jul-00 18:29 by ayounes

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=0000000
0FFFFFFFF010121FF0000000000000030946CD740FF0001
VTP Management Domain: ''

------------------------
```

From the output shown above, the following information can be obtained.

- Device name
- IP address(es) in use on the device
- Hardware platform and capabilities
- Software operating system
- Local port in use and the remote device's port used to connect it.
- VTP management domain

This information could easily be used to attack known vulnerabilities, map out the physical layout of the network, possibly remove VLANs from the network and hit the IP address with any generic attack intended to disturb the operation of the switch.

In a stable, planned and implemented network, this protocol only helps determine if devices are alive and operational. This is a task that is better handled by NMS because there is no alert generated when a CDP neighbor ceases to exist.

[17] Cisco Systems, Cisco Discovery Protocol: http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/1214ea1/3550scg/swcdp.htm

- Spanning Tree Protocol (STP): [ACI]

Spanning Tree Protocol (STP) prevents infinitely looping data in switched LANs. These "bridge loops" bring down entire networks, including other VLANs that reside on the affected switches. Redundant topologies often include multiple paths where the possibility of a loop exists. Switches use STP to elect a "root bridge" from which all switch links branch out. Links that create a loop have the port disabled at one end, making it a stub segment instead of a transit segment. STP is enabled by default on Cisco switches and likely many others.

A vulnerability in some Cisco Catalyst switches' handling of STP can be used for DoS attacks. Ironically, it exploits the IEEE 802.1x security protocol for 802.11 wireless LANs to bypass STP-blocked ports. [18]

Some interesting information regarding 802.11 with 802.1x for WindowsXP can be found on the Microsoft web site.[19]

STP has no authentication, therefore any host can generate STP traffic that can affect the topology of the network. If any network change causes STP to recreate the loop-free tree, network connectivity is negatively affected from 30 to 60 seconds after the change. Constant changes, either by changing transit switch-to-switch links or spoofing STP messages to causes a recalculation can seriously impair availability. Additionally, the loop prevention can be disabled to allow a bridge loop to form, also impairing availability.

An attacker can add a bridge to the network and designate it as the root bridge. This can reduce performance and influence data flows for capture and alteration.

The best way to prevent attacks using SNMP is to employ redundant network designs that do not require STP. STP must be disabled manually. If STP must be used, managed switches can be configured to send SYSLOG messages or SNMP traps to alert NMS of a STP topology change.

- MAC Hardcode [CI]

Similar to Cisco's Port Security feature, associating MAC addresses with particular switch ports will prevent foreign MAC addresses from using the switch to communicate. This feature is useless if the switch still retains its ability to dynamically learn MAC addresses.

- ARP Hardcode [CI]

ARP is used to associate logical IP addresses with physical MAC addresses in the network. If a host has to deliver an IP packet to another host on the same network, a broadcast is sent out to identify which physical host is configured with the destination IP address.

Every host on the network receives the broadcast and any host on the network can generate an answer. An attacker could impersonate the destination IP address by answering the ARP request, receive the data and pass it on to the original destination host. The conversing hosts would not be aware of any redirection of the data. The data stream can then be examined for data and the

[18] Cisco Systems, Security Advisory: http://www.cisco.com/warp/public/707/cat5k-8021x-vuln-pub.shtml
[19] Microsoft, 802.11 Wireless Security http://www.microsoft.com/HWDEV/wireless/IEEE802Net.htm

forwarded content could be altered. If a router or firewall were impersonated, all traffic entering/leaving that segment can be captured or altered.

Again, this is a case where a dynamic protocol can be replaced with a static configuration. Each host on the network can be configured with static MAC-to-IP entries of any or all hosts in the network. This obviously is not practical for a LAN, but is ideal for the networks surrounding firewalls or access routers.

Hardcoding MAC-to-IP associations is one way to protect against dsniff, an attack program.[20]

- Disabling Ports CI

The default setting of most (if not all) switches is to have all ports enabled.

This may lead to the insertion of a host into the network that can attempt many of the attacks discussed in this document. Preventing this is not practical in a LAN environment where hosts are constantly added and removed, so one must rely on physical security. On the other hand, an end-user host can be removed and an attacker's host put in its place. This can be prevented in the small networks surrounding firewalls and access routers because they typically don't change.

If all unused ports are administratively disabled, it will be more difficult to insert a host. To prevent an existing host from being removed and replaced with an attacking host, use the NMS to alert when the link state of the switch port changes. This, along with static MAC-to-IP entries and Cisco's Port Security can make it much more difficult to insert attacking hosts.

Network Security and Management Systems

- Intrusion Detection Systems (IDS) and Protocol Analyzers (Sniffers) CI

These systems capture traffic and analyze it for detecting nefarious network activity or troubleshooting network issues. The can be used for both good and evil in networking, from altering to intruders to capturing users' passwords.

Much information about IDS can be found on the SANS site.[21]

These devices operate in "promiscuous mode" where they accept all traffic, not just broadcasts and frames specifically addressed to their MAC address. In switched networks where traffic only crosses the ports necessary to allow communication, use of these units becomes more complex.

Switches can be configured to "mirror" or "SPAN" (Cisco's Switched Port Analyzer) traffic crossing a particular VLAN or port to another port where an IDS or Sniffer resides. While this is

[20] Dug Song, dsniff FAQ: http://www.monkey.org/~dugsong/dsniff/faq.html#How%20do%20I%20protect%20my%20network%20against%20dsniff

[21] SANS, Intrusion Detection: http://www.sans.org/infosecFAQ/intrusion/intrusion_list.htm

done intentionally for troubleshooting and intrusion detection, an attacker could change the switch configuration to capture traffic for their use.

These devices can also use a shared-media hub to capture traffic. While explicitly setting Ethernet ports' speed and duplex settings are often required for reliability, it can also prevent the insertion of a hub.

Tools exist that can detect IDS units and Sniffers. Antisniff, by L0pht Heavy Industries, attempts to scan your network and determine if a computer is running in promiscuous mode. This tool can be used by your security team to detect sniffers, but can also be used by attackers to identify, circumvent or avoid your IDS units.[22] Another tool, "dsniff", captures data and can affect network data flow.[23]

- Reporting Events ACI

SYSLOG and SNMP are protocols that network devices can use to alert users of events. Many events can be reported, including:

  - Port link-state changes
  - High temperature conditions
  - Access-lists denying traffic
  - Configuration changes
  - Dynamic routing protocol events (neighbors added or lost)

The events to be reported must be set carefully, else too many or too few events will be reported. Dynamic LAN environments should not report port link-state changes where users' desktops will create constant messages at the beginning and end of each day. Border networks (firewalls and border routers) should report them because the addition and removal of every host should be recorded. Attacks on the network device itself may prevent it from reporting events via SYSLOG or SNMP.

This function can be used with NMS or it can be set up on its own. The IP host on the network device is used to generate the messages should be connected to an Out-of-Band network to help prevent an attack on the switch itself. To make sure the reporting ability of the switch is not blocked, use NMS or some other program to regularly check the availability of the switch IP host.

---

[22] SANS, Jason Drury, Sniffers and AntiSniff: http://www.sans.org/infosecFAQ/switchednet/sniffers.htm
[23] Dug Song, dsniff FAQ http://www.monkey.org/~dugsong/dsniff/faq.html

Network Layer Devices

There are many documents that discuss the proper installation and protection of networks using routers and firewalls in security-conscious network designs. Apply the basic principles of infrastructure security described in this document and refer to the abundance of specific information for securing these devices.[24]

External Services

The enterprise network relies upon many things for proper operation. It is rare to find a network that is entirely under the control of a single entity. Consider the security of external hosts that provide critical services, such as your presence on the Internet.

- Internet Service Provider Cooperation [A]

Internet Service Providers' (ISPs) support staff constantly endures the utter mayhem of the Internet. Regardless of whether you're a big customer or a small customer, the time to learn how to navigate the support options and discover limitations of the ISP's support policy is not when you're suffering an outage or attack. Learn the proper support escalation path and learn the ISP's policy regarding their assistance with incidents such as DOS attacks before you're struck at 5:30pm on a Friday. The phrase "you get what you pay for" can apply to your ISP. The best possible price can come at the expense of the support you need to maintain your presence on the Internet while the mayhem ensues.

A good example of ISP cooperation in time of need (and how it took 17 hours to get the right person on the case) is Steve Gibson's account of a DOS attack on Gibson Research Corporation's web site.[25] This also includes a great example of the Internet mayhem.

- Border Gateway Protocol (BGP) Peers [A]

Routers on the Internet use BGP to exchange information about reachable networks. With the explosive growth of the Internet, the information carried by BGP now comes from many sources. While it is impossible to guarantee security of remote networks' advertisements via BGP, you can control what you advertise and what you receive.

Be sure to secure access to the configuration of the router. Consider using access lists to limit which prefixes/networks you will advertise. This will help prevent the advertisement of networks that do not belong to you. ISPs often filter incoming advertisements from their customers to prevent this.

Routers have a finite amount of memory in which to store BGP routing information. If your external peer is compromised and excessive data is sent to your router, it could cease operation.

---

[24] SANS, Firewalls: http://www.sans.org/infosecFAQ/firewall/firewall_list.htm
SANS, Protocols: http://www.sans.org/infosecFAQ/protocols/protocols_list.htm
Cisco Systems, Security on Routers: http://www.cisco.com/warp/public/707/21.html

[25] Steve Gibson, DoS against GRC: http://grc.com/dos/grcdos.htm

If you only have one link to the Internet, consider static routing and have your ISP advertise your network for you.

A critical analysis of BGP vulnerabilities and best practices for implementing BGP can be found on the Internet.[26]

Administration, Management and Disaster Recovery

Administration

- Change Control [ACI]

A Change Control process should be in place that allows careful review of changes to the network architecture. Including a security evaluation can help prevent introducing vulnerabilities into the network.

- Configuration Auditing [I]

While backups of network configurations help with disaster recovery, they can also be used to compare approved configurations with running configurations. Establish a plan to periodically review device configurations and investigate the source of inconsistencies. Some NMSs perform this function automatically, such as CiscoWorks.

- Documentation [AI]

Documentation of the system is vital to configuration management, configuration auditing and change control. It can aid in the identification of hosts and cables that should not be there. Thorough documentation of the approved existing conditions will make inspections more convenient.

- Network Management Systems (NMS) [ACI]

Discussed previously as the target of SYSLOG and SNMP Traps, the NMS provides constant monitoring of a network. Real-time visibility of network events is crucial to network security!

This can be as simple as a host that stores SYSLOG messages and constantly tests connectivity to network hosts. Complex systems cover all aspects of configuration control and availability for all IT devices including servers, network infrastructure and environmental features (door security, temperature)

Disaster Recovery

- Configuration Backup [AI]

Should a network device be compromised, a quick way to restore original security is to restore the configuration of the affected devices. Since this does not prevent additional compromises using the same attack, the breach must be evaluated for preventative action.

[26] X. Zhao, BGP4 Fault Analysis: http://shang.csc.ncsu.edu/bgp/www/BGP-vulnerability-analysis.html

- Storage of Data Backups [ACI]

The information contained in configuration backups could be used to enumerate the network, allowing an attacker to better focus their efforts. The security of these backups is extremely important.

Also consider the offline storage of this information. If the network is compromised to the point that the configuration backups are obtained, they could be modified to keep an audit from finding changes that allow the attacker access to your network.

Conclusion

Thorough attention to the security of the infrastructure is one of the least expensive means of preventing successful compromises of the system. While stronger security appliances and extensive infrastructure choices help make more secure networks, careful design and implementation is a must.

Competition between network infrastructure suppliers constantly improves their products. Many of the new features allow convenient use for both administrators and attackers. Keep the administrative staff trained and aware of the new technologies that appear on newer equipment as the network evolves.

References

•Interpol. "IT Security and Crime Prevention Methods." http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp#51 [section 5.1.5] (25 Aug. 2001)

•Various Authors. "UPS FAQ" http://www.jetcafe.org/~npc/doc/ups-faq.html (25 Aug. 2001)

•SANS. "Wireless Access Security Issues" http://www.sans.org/infosecFAQ/wireless/wireless_list.htm (25 Aug. 2001)

•Szacik, Bob. "HomeRF: Wireless with Security, for the Rest of Us?" http://www.sans.org/infosecFAQ/wireless/homerf.htm (25 Aug. 2001)

•Cisco Systems. "Network Management System: Best Practices White Paper" http://www.cisco.com/warp/public/126/NMS_bestpractice.html#securityman (25 Aug. 2001)

•Kiessling, Robert. "TACACS FAQ" http://www.de.easynet.net/tacacs-faq/tacacs-faq.html (25 Aug. 2001)

•Huckins, Peter. "Vulnerabilities of Router Management Utilizing TACACS+ for Authentication, Authorization, and Accounting (AAA)" http://www.sans.org/infosecFAQ/netdevices/TACACS.htm (25 Aug. 2001)

•Cisco Systems. "Configuring TACACS and Extended TACACS" http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt2/sctcacs.htm

•Lucent Technologies. "RADIUS" http://www.livingston.com/marketing/products/radius.html (25 Aug. 2001)

•van den Hout, Koos. "Software Vulnerabilities in Switches" http://www.hal2001.org/pipermail/fhq-switches/2001-June/000008.html (25 Aug. 2001)

•Turner, Aaron. "Network Insecurity with Switches" http://www.sans.org/infosecFAQ/switchednet/switch_security.htm (25 Aug. 2001)

•Camacho, Jose Luis. "SNMP Security Enhancement" http://www.sans.org/infosecFAQ/netdevices/SNMP_sec.htm (25 Aug. 2001)

•Carter, Charles. "Securing your Cisco Router when using SNMP" http://www.sans.org/infosecFAQ/netdevices/router.htm (25 Aug. 2001)

•Yerxa, Gregory. "Firewall & Load-Balancer: Perfect Union?" http://www.networkcomputing.com/1102/1102ws1.html (25 Aug. 2001)

•Cisco Systems. "The Cisco IOS TCP Intercept" http://www.cisco.com/warp/public/cc/pd/iosw/iore/prodlit/576_pp.pdf (25 Aug. 2001)

•Cisco Systems. “Configuring VLAN Trunks on Fast Ethernet and Gigabit Ethernet Ports” http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_2/config/e_trunk.htm#xtocid155051 (25 Aug. 2001)
•Cisco Systems. “Token Ring VLANs and Related Protocols “ http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb2/vlan.htm#xtocid299187 (25 Aug. 2001)
•Cisco Systems. “Configuring VLANs, How the VMPS Works” http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35wc/sc/swgvlans.htm#xtocid1196655
•Cisco Systems. “Etherchannel Technologies” http://www.cisco.com/warp/public/779/largeent/learn/technologies/fast_echannel.html (25 Aug. 2001)
•Cisco Systems. “Managing Switches, Enabling Port Security” http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35xu/scg/kiconfig.htm#xtocid57457 (25 Aug. 2001)
•Cisco Systems. “Configuring CDP” http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/1214ea1/3550scg/swcdp.htm (25 Aug. 2001)
•Cisco Systems. “Cisco Security Advisory: Catalyst 5000 Series 802.1x Vulnerability” http://www.cisco.com/warp/public/707/cat5k-8021x-vuln-pub.shtml (25 Aug. 2001)
•Microsoft Corporation. “Enabling IEEE 802.11 Networks with Windows "Whistler"” http://www.microsoft.com/HWDEV/wireless/IEEE802Net.htm (25 Aug. 2001)
•Song, Dug. “dsniff FAQ” http://www.monkey.org/~dugsong/dsniff/faq.html (25 Aug. 2001)
•SANS. “Intrusion Detection” http://www.sans.org/infosecFAQ/intrusion/intrusion_list.htm (25 Aug. 2001)
•Drury, Jason. “Sniffers: What are they and How to Protect From Them” http://www.sans.org/infosecFAQ/switchednet/sniffers.htm (25 Aug. 2001)
•SANS. “Firewalls & Perimeter Protection” http://www.sans.org/infosecFAQ/firewall/firewall_list.htm (25 Aug. 2001)
•SANS. “Protocols” http://www.sans.org/infosecFAQ/protocols/protocols_list.htm (25 Aug. 2001)
•Cisco Systems. “Improving Security on Cisco Routers” http://www.cisco.com/warp/public/707/21.html (25 Aug. 2001)
•Gibson, Steve. “DoS against GRC” http://grc.com/dos/grcdos.htm (25 Aug. 2001)
•Zhao, X. “BGP4 Fault Analysis” http://shang.csc.ncsu.edu/bgp/www/BGP-vulnerability-analysis.html (25 Aug. 2001)