# Lesson 2: Securing Network Cabling



Most networks utilize network cable in some form. In this lesson you learn ways in which network cable can be compromised and methods for securing it. This lesson investigates three major types of cabling: coaxial, twisted-pair, and fiber optic.

Although wireless networks are increasing in popularity, network cabling is still used in most organizations. Physical cable currently provides a more secure, reliable, high-speed network connection than wireless. Wireless networking is discussed in Lesson 3.

---

### After this lesson, you will be able to

- Document ways in which network cabling can be compromised
- Secure network cabling

---

Coaxial Cable

There are several different types and grades of coaxial (coax) cable, but the same basic structure applies to all of them. All coaxial cable has a center conductor, an outer conductor, and an outer sheath. Electronic transmissions (representing data) travel through the center conductor. The remainder of this section focuses on how coaxial cable can be compromised and ways to protect it.

Sabotaging Coaxial Cable

Coaxial cable is more difficult to cut than the other types of cable discussed in this lesson, but a pair of wire cutters can quickly cut through it nevertheless. Cutting coaxial cable isn't necessary to disrupt communications on a coaxial network. A heat or energy source placed near coaxial cabling can also impede communications. Because coaxial cable is typically used in bus topologies, a cut wire or severe electromagnetic interference (EMI) or radio frequency interference (RFI) could bring down the entire network. EMI and RFI are types of noise that can affect the reception of electronic transmissions, including those carrying data on a network. EMI and RFI can lead to the malfunctioning of other sensitive electrical and electronic equipment. Physically removing a terminator, which can be found at each end of a coaxial bus network, is yet another way to disrupt communication on the network.

To protect your coaxial network segments from sabotage, you should be sure to protect the physical cable. Any point along the network is vulnerable to compromise and sabotage due to the bus nature of a coaxial network segment.

Eavesdropping on Coaxial Networks

Because coaxial networks utilize a bus topology, signals traverse the entire segment on their way to the destination host. Any connection along the coaxial network is susceptible to eavesdropping, which can also be achieved by tapping into the coaxial cable at almost any point on the network. However, eavesdropping usually involves disruption of service because the bus network must be temporarily disconnected to insert a new station.

To help prevent eavesdropping, protect your network cable as much as possible by burying it underground, placing it inside walls, and protecting it with tamper-proof containers. For maximum protection, you should do the following:

- Document your cable infrastructure.

- Investigate all outages on your coaxial network.
- Physically inspect your cable infrastructure on a routine basis.
- Investigate all undocumented hosts and connections.

Twisted-Pair Cables

You should already be familiar with twisted-pair cabling standards. All twisted-pair cables have one or more pairs of wires that are twisted together inside a cable sheath. The wires themselves are made of copper and covered by a plastic coating to prevent them from making an electrical connection to each other. The cable sheath itself is typically a plastic tube containing the wires. The individual wire pairs are twisted inside the cable sheath to help prevent the loss of electrical signals traversing the cable pairs. The remainder of this section focuses on ways in which twisted-pair cable can be compromised and methods for securing it.

Sabotaging Twisted-Pair Networks and Countermeasures

Twisted-pair networks can also be sabotaged. The cables can be easily cut with a pair of wire cutters or regular office scissors, or a heat or energy source could disrupt communications. However, twisted-pair networks typically utilize a star configuration, so the loss of a single cable should not disrupt the entire network, unless the cable that was cut provided connectivity to the central server or gateway router. In a mesh configuration, cutting a single network cable might not even interrupt network communications.

To protect your twisted-pair network segments from sabotage, you should be sure to protect the physical cables. Protecting central connectivity devices such as hubs and patch panels is more important than protecting individual twisted-pair segments. The next priority is to protect crucial segments, such as those going to central servers, routers, or connecting hubs and switches. Finally, you should physically inspect your network cable infrastructure routinely.

Eavesdropping on Twisted-Pair Networks and Countermeasures

Electronic signals traverse the twisted-pair cable. Someone spying on your network could listen to these passing signals. There are three main ways in which a twisted-pair network might be compromised by eavesdropping:

- Physically attaching a protocol analyzer to a twisted-pair connection point. A protocol analyzer is a device or computer software program that allows its user to capture and decode network traffic. Other names for it are data sniffer, network sniffer, or packet sniffer.
- Splicing into the twisted-pair cable.
- Using escaping electromagnetic signals to eavesdrop on signals passing through the wire.

Physical security is the main method of protecting twisted-pair networks from eavesdropping, and you should protect your central network devices before focusing on individual hosts. Using switches instead of hubs can make eavesdropping more difficult because switches direct network traffic bound for a specific host directly to that host, whereas hubs direct traffic bound for a specific host to any host attached to the hub. However, there are tools that attackers can use to compromise switches, as discussed in the next lesson.

Managed devices (such as hubs, switches, and routers) can alert you when a cable is unplugged or a new connection is created. Such warnings can also alert you to the presence of an eavesdropper.

Fiber Optic Cable

You should already be familiar with fiber optic cabling standards. Fiber optic cable utilizes a glass or plastic filament that conducts light pulses to transfer data. Outside of the fiber optic core, there is a glass cladding, a plastic spacer, protective Kevlar fibers, and then a protective outer sheath.

Fiber optic cable is the most secure cable because it cannot be affected by electromagnetic interference and

does not leak electrical signals. However, of the cable types discussed in this lesson, fiber optic cable is the most expensive and most difficult to install. The remainder of this section focuses on ways in which fiber optic cable can be compromised and secured.

Sabotaging a Fiber Optic Cable

Sabotage of a fiber cable is easier than sabotage of any other cable type. Fiber cables can be crushed, bent, snapped, and often inadvertently damaged. Any damage to the fiber cable disrupts the signal between the two points to which the cable is attached.

To protect your fiber optic cable from sabotage or the possibility of eavesdropping, protect the physical cable. If there is an outage between two points on the fiber cable, you must determine why that outage occurred to ensure that it was not due to sabotage.

A power outage could also be used to insert rogue devices. Consider that an attacker might create a situation to insert a device. After a power outage, you should ensure that your network cables are still properly routed and that no rogue devices are present.

Eavesdropping on a Fiber Optic Connection

Electronic eavesdropping is virtually impossible on fiber optic cables because they emit light pulses. To eavesdrop on a fiber network you must disrupt the communications between two hosts. The fiber cable must be cut, the ends polished, and a fiber optic card inserted between the connection. During the insertion, the connection between the two hosts is unavailable. The difficulties involved and possibilities for detection make such an exploitation highly unlikely.

Exercise: Identifying Cable Vulnerabilities

Match the cable type in the left column with the compromise it's susceptible to in the right column. More than one compromise might apply to any given cable type.

| | |
|---|---|
| 1. Fiber optic | a. EMI and RFI |
| 2. Twisted-pair | b. Breaking or cutting |
| 3. Coaxial | c. Eavesdropping |

---

Lesson Summary

- Network cabling is a vulnerable part of your network infrastructure. However, an attacker or spy must have physical access to your cable (or at least be able to get close to the cable) to exploit or attack your network cable infrastructure.
- Sabotage is a simple matter for a saboteur who is able to gain physical access to your network cable infrastructure. The saboteur could cut a coaxial or twisted-pair cable to disrupt network communications. Also, coaxial and twisted-pair cable are susceptible to EMI and RFI, so a source of EMI/RFI placed near a cable or wire bundle could be enough to disrupt communications. Fiber optic cable is impervious to EMI and RFI, but is easily broken.
- Use the following techniques to protect your cable infrastructure:
    - Document your entire cable infrastructure. Keep that documentation current.

- Investigate all hosts and connectivity devices that are not documented.
- Protect your network cable as much as possible by burying it underground, placing it inside walls, and protecting it with tamper-proof containers.
- Check the physical integrity of your network infrastructure cabling on a regular basis. Verify your network infrastructure after power outages.
- Enable managed devices to alert you of the presence of disconnected cables or unauthorized connections. Investigate all alerts and outages.