SPaRC

Secure Pathways for Resilient Communications

Summary

Operational Technology (OT) networks [e.g., industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems] have unique cybersecurity challenges due to their decades long service life, high availability requirements, and limited visibility. OT networks often take credit for being "**air gaped**" (i.e. disconnected from the Internet) and all devices within the OT network can "talk" to each other—even if they should not. This SPaRC Technical Bulletin describes how the unique limitations of OT networks can become strengths when it comes to cybersecurity.

Any "Port" in a Storm

The proverb, "Any port in a storm" is a common saying. In times of trouble, any source of refuge is welcome. But a computer network port could be the cause of your troubles. This SPaRC Technical Bulletin will give you an appreciation for what network ports are and how adversaries use unsecured network ports to gain access to a network. This SPaRC Technical Bulletin will also provide actionable checklists for all skill levels to help secure OT network ports.

Network Ports

The **OSI network model** (Open Systems Interconnection) divides network communications into seven distinct layers (see Table 1 below). The sender and receiver each create a *socket*, which is used to communicate with each other. A **socket** consists of an address from layer 3 of the OSI model and a port from layer 4 of the OSI model.

TABLE 1. The OSI Network Model

Layer	Name	Group
1	Physical	Physical
2	Data	
3	Network	Network
4	Transport	
5	Session	Application
6	Presentation	
7	Application	

For example, Google's name server can be found at the IPv4 (Internet Protocol version 4) address of 8.8.8.8 on UDP port 53 (User Datagram Protocol). [N.b. DNS defaults to UDP but may use TCP (Transmission Control Protocol) in some situations.].

There are 65,535 possible port numbers for each socket. IANA (Internet Assigned Number Agency) manages a number scheme[1] for network ports. **Source ports** are typically chosen at random from the range of 49,152 to 65,535 and are sometimes called *private*, *dynamic*, or *ephemeral* ports. Operating system may implement random source port selection differently and observing how source ports are chosen over time can reveal the underlaying operating system. **Well-known destination ports** range from 0 to 1,023 and include officially assigned, unofficially assigned, and reserved port numbers for specific services such as FTP (File Transfer Protocol) on port 21. **Registered destination ports** range from 1,024 to 49,151. Although there is nothing special about this numbering scheme and any service may be bound to any port. A system administrator may try to "hide" remote access via SSH (Secure Shell) on port 2,022 instead of the IANA assigned port of 22. This technique will not fool a hacker and can be a source of frustration for legitimate users.

Network Segmentation

It is a best practice to physically separate networks with different purposes within the same organization. Networks can also be logically separated via *subnets* or *VLANs*. **Subnets** use different network IDs and subnet masks to logically separate network traffic. **VLANS (virtual local area networks**) separate network traffic by adding a VLAN ID to each network packet. Multiple separation strategies can be combined as a defense-in-depth approach, which is also a best practice. This ensures continued network segmentation if any one technique fails.

Externally Facing Networks

Networks that are reachable from the Internet are said to be **externally facing**. It should go without saying that no OT network should be externally facing. Given the confidentiality, integrity, and availability requirements of OT networks, which often support critical infrastructure, network segmentation is a key concept in protecting OT networks. A network of networks that is not reachable from the Internet is said to be **internally facing**.

A certain degree of trust (i.e. authentication and authorization) may be required for devices to participate in an internally facing network.

[1] https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

However, legacy OT devices may not support authentication or authorization, or these security controls may add unacceptable latency to an OT network. There is often an implicit degree of trust between devices in OT network design. Unfortunately, this implicit trust can lead to insecurity.

A False Sense of Security

Many OT networks take too much credit for being *air gapped*. It is unlikely that such a network is truly disconnected from all external threats. Rogue employees may install commodity wireless routers to bypass restrictive security policies. Third-party access granted to vendors and managed security service providers, should be temporary, but is seldom revoked and has been abused by adversaries many times[2 3]. Cybersecurity researchers have demonstrated the transmission of malware using computer speakers[4]. No speaker, no problem—researchers have found a way to turn a computer's fan[5] or power supply[6] into a speaker[7]. The confidentiality of private encryption keys has been violated using an iPhone camera recording of a computer's power LED[8].

Many OT networks allow any host address on the same network to communicate with any other host using any port. This implicit trust can be abused by an adversary by taking advantage of a host that is not the intended target of an attack. Using a technique called **vulnerability chaining**, the adversary first exploits a vulnerability on any host they can compromise, then they *pivot* from the compromised host to the intended target host. Using another vulnerability on the target, the adversary escalates privilege to perform their actions on the objective, including loss of confidentiality, loss of integrity or loss of availability.

Cleartext protocol such as TELNET (port 23) and FTP (port 21) should never be used if vendors offer secure options like HTTPS or SFTP. If your organization uses a password scheme such as [dev|test|prod] + [3-letter system abbreviation] + [complex password], e.g., devPDC$S#Uk95q, a cleartext protocol could *leak* your password scheme, allowing an adversary to correctly guess or easily brute force the password to another system. (If your organization uses a password scheme like this, you should immediately switch to random, complex passwords.)

If you are forced to use a cleartext protocol like TELNET or FTP, ensure these devices are not *externally* facing (i.e. reachable from the Internet). A common technique is to use network segmentation (see above), then place the network behind a bastion host, VPN, and network-based firewall.

---

[2] https://www.sipa.columbia.edu/sites/default/files/2022-11/Target%20Final.pdf

[3] https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack

[4] https://arstechnica.com/information-technology/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/

[5] https://www.sciencedirect.com/science/article/abs/pii/S0167404820300080

[6] https://thehackernews.com/2020/05/air-gap-malware-power-speaker.html

[7] https://arxiv.org/abs/2005.00395

[8] https://arstechnica.com/information-technology/2023/06/hackers-can-steal-cryptographic-keys-by-video-recording-connected-power-leds-60-feet-away/

Static vs. Dynamic

One benefit of OT networks is that they tend to be relatively small (i.e. a manageable number of devices). Network devices tend to be homogeneous. There is a relatively slow pace of change as devices are added, changed, or removed from OT networks. The same devices tend to communicate with each other at the same time, and the same way, with similar sized messages using the same protocols. OT networks are low entropy (i.e. there is little surprise) when the network traffic is analyzed, because most of the network protocols transmit machine-to-machine or machine-to-human messages.

- ✓ Consider using static network addresses [as opposed to the Dynamic Host Configuration Protocol (DHCP)].
- ✓ Consider using HOST files to resolve domain names [as opposed to the Domain Name System (DNS) protocol].
- ✓ Consider using static route tables for more predictable packet delivery.
- ✓ Periodically audit static configurations to ensure they have not been changed.
- ✓ Do not allow unknown devices to communicate on an OT network without proper provisioning. (Approaches may vary, but could include software defined networking (SDN), native switch port security (e.g. 802.X), network and host-based firewalls, authentication, etc.)
- ✓ Take a deny-by-default approach to normal network operations (see below).
- ✓ If you must use dynamic network configurations, be aware of the security implications and provide additional logging and monitoring of network devices.

Learning the "Truth on the Wire"

To support a static approach to networking (see above) and a deny-by-default approach to allowing network traffic (see below), it is vital to understand what normal network communications are occurring on an OT network.

- ✓ Review as-designed and as-built OT network diagrams for expected normal communications.
- ✓ Review active network connections with tools like *netstat*.
- ✓ Use network tools like `tcpdump`, `tshark`, and *WireShark* to gather PCAP (packet capture).
- ✓ Review PCAP from hosts and OT networks to discover actual communications (e.g., "Who is talking to who, and what are they saying?".
- ✓ Review communications for misconfiguration (e.g., DHCP vs. static IP addresses, unreachable broadcast traffic, lack of encryption, and other misconfiguration problems).

Take a Deny-by-Default Approach

Begin by closing all ports. This approach is different from trying to decide what individual ports should be closed. Recall there are over 65,000 different possible destination ports. The best practice is to block everything, then explicitly open only the ports you need for the correct function of your network. After you have learned what normal communications look like on your OT network, use security policies and security controls to reject any network traffic that is not normal (e.g. abnormal or malicious).

A combination of host-based solutions and network-based solutions may be needed, depending on the capability of legacy devices within the OT network.

- ✓ Begin by identifying destination ports that should be in use. Follow vendor guidelines for OT devices and choose the most secure port available (e.g., SSH instead of TELNET).
- ✓ Beware of the "tyranny of the default setting" [9 10], which may prefer ease of setup at the expense of security.
- ✓ Block unknown network traffic as close to the source as possible (e.g. gateway).
- ✓ Use network-based firewalls to restrict known addresses to specific destination ports used in normal communications to reduce attack surfaces and prevent pivoting from a compromised network device.
- ✓ The last rule of any firewall rule set should be to drop any packet that does not a match a rule for normal communications.
- ✓ Provide diversity by using host-based security controls to cover network-based security controls [e.g., firewalls, end-point detection and response (EDR), etc.] if available.
- ✓ Be wary of stateful packet inspection or intrusion prevention security controls that could introduce delay or impact network availability leading to an adverse effect on safety systems that require timely delivery.
- ✓ Consider tripwire software that drops network traffic that originates from unknown source addresses or attempts to connect to unused destination ports.
- ✓ Periodically verify OT network configurations match existing documentation to ensure no new devices have been introduced, which could bypass existing security controls or add new attack surfaces.

For more information, please visit https://securecomms.ornl.gov.

The SPaRC (Secure Pathways for Resilient Communications) program is sponsored by the U.S. Department of Energy and executed through a multi-laboratory testbed to design, evaluate, and support next-generation secure grid communications.

The U.S. Department of Energy's SPaRC program is leading grid communications research and development through a multi-national lab virtual testbed, created to design, test, evaluate, and benchmark next-generation secure communications architectures and technologies. A secure communications system protects the end-to-end physical pathway that transports data from origin to destination. That pathway may involve different transmission methods, such as optical fiber, copper wire, and wireless technologies, and will transport a diversity of data, including grid state information and control messaging in a variety of analog and digital formats. Securing this end-to-end communications pathway, which is essential for reliable grid operations, involves preventing unauthorized access as well as monitoring traffic to identify anomalous activity without compromising the confidentiality, integrity, or availability of the data. Communications security methods complement the cybersecurity approaches used to protect data at the origin and destination. Key SPaRC activities include the grid communications test bed, next generation

[9] https://www.grc.com/sn/sn-710.htm

[10] https://www.grc.com/sn/sn-1036.htm