THE SECURITY TRIAD

An introduction to network security

by Mike Gates, Senior Sales Engineer, REDCOM

Abstract

Stories about security breaches of organizations like Equifax or the City of Atlanta are all too common in news media outlets. These stories highlight the need to identify and mitigate or eliminate network vulnerabilities. Infiltration into business communications can be just as damaging as a data network breach, so it is important to include these components in any assessment of a network's vulnerabilities.

Many sources equate secure communications to encryption. While encryption certainly plays a key role in a secure communications solution, it is not the only required element. The cybersecurity industry uses a model referred to as the security triad to define the various domains that need to be addressed when securing a network. The triad – sometimes also known as CIA – includes Confidentiality, Integrity, and Availability. This paper will review and define these domains for a better understanding of what is required to provide a complete secure communications solution.

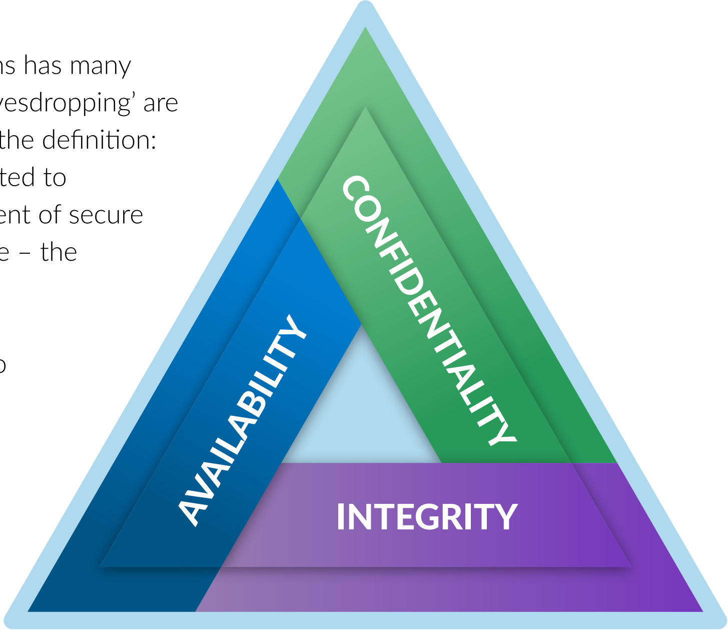
Introduction

Network security is receiving a tremendous amount of media focus recently and security breaches have become a common leading story in many media outlets. The risks associated with a security breach can lead to significant loss financially as well as have a significant negative impact on a company's reputation. As a result, many companies are taking a renewed look at network security to identify potential vulnerabilities and determining how to eliminate or mitigate the risks.

When conducting a network security assessment, it's easy to see how components like web servers or edge devices such as routers and firewalls should be scrutinized. One element that should not be overlooked, however, are the devices used to conduct an organization's communications. Business communications are just as vital to an organization's computer network and can be just as devastating if breached. How much damage could a malicious actor cause if they eavesdropped on a private conversation and learned proprietary or financial information? So, securing the business communications network is equally as important as securing the data network.

What is Secure Communications?

Depending on where you look, secure communications has many definitions. Terms like 'privacy' or 'protection from eavesdropping' are used, but one central theme is always at the heart of the definition: encryption. Too often secure communications is equated to encryption. It's true that encryption is a vital component of secure communications but it certainly isn't – nor should it be – the whole story.



The cybersecurity industry uses a standard concept to describe network security, referred to as the security triad – sometimes also known as CIA. The triad describes the three pillars that support the concept of security; namely confidentiality, integrity, and availability. To be a truly secure system, a solution must address the concerns in each of these three areas.

CONFIDENTIALITY

In the context of network security, the goal of confidentiality is to prevent unauthorized access to, or disclosure of, information and/or media. There are two primary methods used to achieve this goal: encryption and access controls.

Encryption

Encryption provides confidentiality by preventing unauthorized disclosure of data. Encryption is the act of using a cipher (algorithm) and key (variable data used with the cipher) to convert information into encoded data. Only those that know which cipher was used and possess the appropriate key to decipher the encoded data are able to unlock and retrieve the information. Even if a hacker is able to gain access to the encoded data, they will be unable to retrieve the information since they won't have the appropriate key.

There are two primary types of encryption, symmetric and asymmetric. Symmetric encryption uses the same cipher to both encrypt and decrypt the information. Some examples of symmetric encryption are the Triple Data Encryption Standard (3DES), Blowfish, and the Advanced Encryption Standard (AES). Asymmetric encryption uses a mathematically matched key pair – one to encrypt and the matched key to decrypt. These key pairs must be used together. In other words, the only key that can be used to decrypt data is the matched key for the one that encrypted it in the first place. Some examples of asymmetric encryption are Rivest, Shamir, Adleman (RSA) and elliptic curve cryptography (ECC).

There are a wide variety of protocols used to encrypt and transport information. These include IPSec, Transport Layer Security (TLS), Secure shell (SSH) and Hyper Text Transfer Protocol Secure (HTTPS).

Access Controls

Access controls are used to grant, or restrict, access to information. This will ensure that only the people who are authorized to have access to specific information can get to it. Access controls use a combination of identification, authentication, and authorization.

Identification is a claim of an identity. A user, for example, can claim an identity with a username during an attempt to access an account.

Authentication is used to prove the claim of an identity. Again, using the username example, a user may be required to enter a password to prove that they are indeed who they claim to be. The intent being that nobody other than the specific user will know the associated password.

Authorization is used to grant or restrict access within a system once a user's identification has been authenticated. This defines the level of access – or privileges – a user has.

INTEGRITY

Integrity provides assurance that data has not been modified, tampered with, or corrupted from its original form. The primary method to ensure that data has not lost integrity is through hashing.

Hashing

Hashing is the act of using an algorithm to generate a "fingerprint" for a piece of information. The algorithm will convert information of any size into a fixed size hash – sometimes also known as a digest or checksum. If the same hashing algorithm is used on the given piece of information, it will always result in the same hash value. In this way, hashing can be used to determine if the original information has been modified in any way. A hash value for a piece of information can be generated at two different times. If the hash values are the same then the data is the same. In other words, the data integrity has been maintained. There are several hashing algorithms in use today. These include Message Digest 5 (MD5), Hash-based Message Authentication Code (HMAC), and the Secure Hash Algorithm (SHA).

AVAILABILITY

Availability is an assurance that systems, services, and data are available when they are needed. The availability schedule will vary depending on the purpose and the organization that is using the system. Some applications may require that the system is available from 8 a.m. to 5 p.m. Monday through Friday while others may require the system be available 24/7. With availability, there are different components that need to be considered including hardware availability, software failover, and defending against attacks.

Hardware Availability

All systems and services operate from a hardware platform, either dedicated purpose-built hardware or a software application running on a generic server platform. The first line of defense for availability is to ensure that the hardware platform runs properly and continuously. This can be accomplished in two different ways, through reliable hardware design and hardware redundancy.

Hardware reliability is achieved through a design that ensures a long mean time between failures (MTBF). A robust design utilizing reliable components will result in an overall reliable system that is less prone to failure.

Hardware redundancy enhances the reliability of a hardware platform. Utilizing redundant processors, power supplies, disk drives, and the like can provide a hot standby system that will immediately take over operation in the event of a hardware failure on the primary component.

Software Failover

In addition to hardware redundancy, the software can also be configured in a redundant fashion. Using either the native application or a hypervisor, a system can be configured to provide both an active and hot standby solution. The active system will be online and performing the processing necessary to complete the applications functions. The hot standby will continuously monitor the state of the active system, but will otherwise remain inactive. In the event of a catastrophic failure of the active system, the hot standby can immediately take over the responsibilities of the active system.

Attack Defense

Another avenue that can be used to render a system unavailable is with a malicious denial of service (DoS) attack. Such attacks monopolize the processing power of the system to the point that is not available to perform its intended function. Attacks of this type are best dealt with using an appliance, such as a firewall, that sits on the edge of the network and shields the systems on a network from malicious attacks allowing them to carry on with normal operations.

Conclusion

Secure communications involves considerably more than just encryption. Encryption certainly plays a vital role, but there are many other building blocks needed for a complete secure communications solution. A complete secure communications solution must address all components within the security triad. Leaving even just one of these domains unaddressed will open a threat vector that is vulnerable to attack.

We at REDCOM realize that protecting your business communications is just as important to you as securing your data network infrastructure. As a result, we have taken a holistic approach to addressing all domains of security in our products. We have been trusted with providing secure communications solutions to some of the most secure locations in the world and are standing ready to assist you in securing your communications network.

Contact Information

REDCOM Laboratories, Inc.
One REDCOM Center
Victor, NY 14564
585-924-6500
sales@redcom.com
www.redcom.com

Talk to the experts at REDCOM

REDCOM specializes in the development of advanced communications solutions with a focus on security, reliability, and interoperability. REDCOM's customers include all branches of the military, government agencies, service providers, emergency responders, integrators, enterprises. Contact a REDCOM solution advisor today to learn more about our secure communications solutions.

REDCOM®