THREATS AND VULNERABILITIES FOR C^4I IN COMMERCIAL TELECOMMUNICATIONS: A PARADIGM FOR MITIGATION

Joan Fowler and Robert C. Seate III
Data Systems Analysts, Inc.
10400 Eaton Place, Suite 400
Fairfax, VA 22033
703/591-3704 (voice)
703/591-8418 (fax)
fowlerj@dsainc.com and seater@dsainc.com

Abstract

The current trend for the communication of Command, Control, Communications, Computers, and Intelligence (C^4I) information is a shift from point-to-point, closed, dedicated networks to the use of distributed, open, commercial networks. The threats and vulnerabilities that existed in the closed environment are different in scope and type from those that exist in the open environment. For this reason, mitigation techniques need to be refined and updated to reflect new risks to C^4I and sensitive information.

Introduction

The shift from the closed network to the open network for transmitting sensitive information is occurring largely because of the cost and lifecycle duration and risks of the traditional closed network. The closed network has traditionally taken longer to develop, cost more to both develop and maintain, held all of the programmatic risks of a development effort, and provided the lifecycle costs/risks inherent with a proprietary entity.

On the other hand, the open network and network technology currently exists. Therefore, the extension of the network for new “customers” should, and usually does, take a shorter time for connections which are usually sold to the Government on a fee-for-service basis. There is frequently little or no development effort involved. The maintenance of the open commercial network is spread across all of the users, not just the Government “owners” of the network. Finally, since the technology is not proprietary, the open network makes use of the state-of-the-art technology that can be developed using the economy of scale available because of the open environment.

All of these issues are outside of the direct security aspects of the closed/open choice. However, because of the advantages of the open environment, the decision is being made to go toward the open environment for both unclassified

as well as sensitive traffic. Therefore, the threats, vulnerabilities, and risks associated with the open commercial environment must be assessed and mitigated to provide an service that is as protected as possible.
safe

Threats and Vulnerabilities

The threats and vulnerabilities in the closed environment are predicated by the very nature of the networks: limited access points, historically customized applications, and known technologies. The threats and vulnerabilities in the new open environment are: increased access points to a portion of the network; global availability of access to the network; more sophistication of today's hackers; and new technologies for which the vulnerabilities have not been characterized. Because there are more points of presence, the number of unauthorized access points has increased. Furthermore, because of this maze of connectivity, the access technique and a clear path between origination and destination points become obscured.

Closed Environment

In the closed environment, limited legitimate access points are available to the intruder of the network. Due to this named accessibility, the corresponding limited threat provides a limited vulnerability for the network. Comparatively speaking, the closed environment can control access through protection of the limited resources through mitigation techniques that are non-technical, i.e., physical security of the environment and personnel security clearances. Figure 1 illustrates the simplified approach historically used for communications between facilities of C^4I and classified information.

Customized applications have historically been used in the closed environment to fulfill the specific requirements for the network/system. Therefore, the sponsoring organization can provide the kinds of control on the development effort that provide a level of confidence associated with the effort and the resulting product. Extensive testing of the product/system can be performed to ensure that not only the requirements have been met, but that anomalies have not been introduced into the network.

Finally, in the traditional closed environments used for C^4I information, known technologies (e.g., operating systems, platforms) have been used because of the procurement and development time for the customized system. By the time that the system or network is ready to be fielded, the technology that comprises the system has usually been tested and fielded in an operational environment. This operational experience with the technology provides a determination of the vulnerabilities inherent in the product and, usually, a mitigation of that vulnerability so that the risk of using the product is acceptable.

Figure 1. Closed Point-to-Point Environment

Open Environment

The threats and vulnerabilities in the new open environment are: increased access points to a portion of the network; global availability of access to the network; increased sophistication of today's hackers; and new technologies for which associated vulnerabilities have not been characterized. As can be seen in Figure 2, the complete globe today is in the cloud developed for world-wide communications. The benefit of this communication is that the world is accessible from almost everywhere. The challenge: protect the cloud against unauthorized intrusion and denial-of-service.

The networks that are being used to handle the communication of C^4I information today, and even more in the future, are restricted to limited access points as in the past. The number of points of presence, or points at which the user can gain access, has been increased to provide more availability to the network. This free flow of access enhances the availability and use of the open environment for authorized users. However, because there are more points of presence, the number of unauthorized access points has also increased. This increases the threat to the network by unauthorized users, and the vulnerability of the open environment to these unauthorized users.

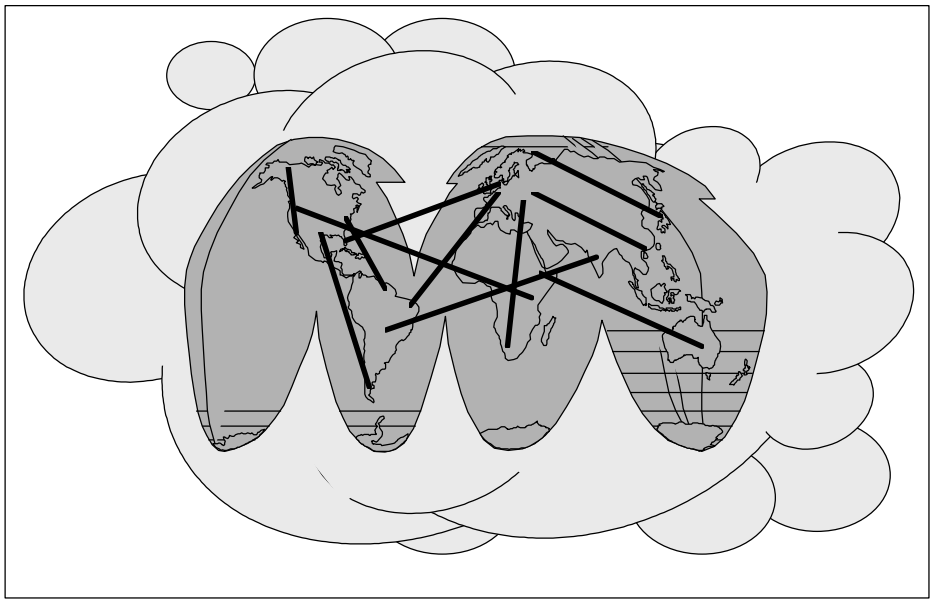

Figure 2. Open Global Environment

The open environment to be used for the communication of C^4I information is truly a global network. This global characteristic of the network translates into the availability of access to the network on the global level. Therefore, a user in Hong Kong is connected logically to the same global network that the users communicating, for instance, between Fort Bragg and Fort Hood are connected. This vulnerability of the cloud or global network invites those that desire to interrupt or intercept legitimate traffic, and not just C^4I information to disrupt that traffic. Frequently, the intruder/interrupter is so technically astute that the effort to disrupt is not a challenge to them at all.

Because of this maze of connectivity, the access technique and a clear path between origination and destination points becomes obscured. There are numerous techniques that can be applied to gain access to the open environment. That is a functional advantage of the environment. However, from a security perspective, it presents a vulnerability to the environment. Additionally, it is not possible for any user to determine prior to transmission the exact route that a packet of information will take to reach it's destination. Therefore, it is also not possible for the user sending a packet to be assured that the information will not be vulnerable to a particular threat at some instance along the way.

Today's hackers are far more sophisticated than those in the past. With the decrease in the cost of personal computers and software, and the availability of more powerful communications resources and additional shareware tools through the Internet, hackers have the tools available for them to wreak havoc on a global scale. Additionally, with the proliferation of technical skills to a wider variety of individuals, it is more common for any individual to have the needed

technical skills to intrude into a network. Therefore, current hackers have the technical ability to intrude in the legitimate traffic of the global open environment.

New technologies make the open, global communications environment possible. However, the vulnerabilities inherent in much of these new technologies have not been characterized through operational experience. When a new technology is inserted into the cloud, often times the vulnerabilities are not defined until the technology has been in operational use for awhile and the hackers have had a chance to attack it and find weaknesses with it for a period of time. This "trial under fire" for new technology leaves the open environment vulnerable for a time.

Paradigm for Mitigation

To reach an acceptable level of risk for the communication of C^4I and other sensitive information, there are a number of mitigations that can be applied to these threats and vulnerabilities. Some of the mitigations include: more robust standards for both communications and security technologies; the use of a layered security architecture to compartmentalize network availability; more sophisticated Commercial Off-The-Shelf security and general communication products; the availability and use of online tools to test for vulnerabilities and monitor/respond to incidences; greater availability of information on threats, vulnerabilities and potential mitigations; and heightened security awareness throughout the open environment.

Standards

As a result of the technology industry's response to the need for consistent baseline standards and defined processes, organizations such as the National Institute of Standards and Technology (NIST), International Standards Organization (ISO), and International Telegraph and Telephone Consultative Committee (CCITT) have researched, developed, and gained consensus for more robust standards associated with communications and security technologies. Examples of these standards include the Commercial Internet Protocol Security Option (CIPSO) and Internet Security Association Key Management Protocol (ISAKMP). These standards, as well as others of their type, enhance the security of the open environment. In addition, they increase interoperability of the total network from a security perspective.

Layered Security Architecture

The current trend in security architecture system design is to provide a multi-layered identification, authentication, and protection schema. In doing so, a security architecture design contributes a compartmentalized approach to network availability (i.e., each layer provides an independent level of protection

of which the aggregate results in a more robust security blueprint). Furthermore, by separating and using independent but interconnected layers, one or more of these layers could withstand being compromised without adversely affecting the aggregate countermeasure schema for denial-of-service, intrusion, and detection attacks.

Sophistication of Products

Today, security hardware and software products offer more sophisticated commercial off-the-shelf (COTS) features and functionalities. In addition, as communication technology advances, so do the inherent product access control features. Equally important are the increased functionality and stress testing processes associated with the research and development of these products. The technology industry has responded to the information security community requests by providing these important features as part of their regular product offerings.

Tools

The role of the Internet as a resource for information and software dissemination has grown beyond its original inception. The availability and use of online tools to test for vulnerabilities and provide network monitoring has also greatly increased. As new software products are developed, the role of the Internet community becomes a provider of global feedback for alpha and beta versions of these products. This role becomes cyclical as new releases of the software products emerge. As a result, the needs of both the user and the security software developer are very complimentary.

Information

The Internet also serves as an information superhighway. The security community has taken advantage of this near real-time method of information flow. As new vulnerabilities are discovered, an inflow of information occurs as information security data collection organizations accumulate and categorize this knowledge. Just as important is the organized outflow in information security data by these recognized institutions. Examples of these organizations include the Forum for Incident Response and Security Teams (FIRST), Computer Emergency Response Team (CERT), and Automated System Security Incident Support Team (ASSIST). Furthermore, tested mitigations for these categorized threats and vulnerabilities are also made available to the security community. Because of the global bridge that the Internet provides, efficient information distribution occurs.

Security Awareness

Security awareness of users, operators, and administrators of the open environment is an important mitigation of the threats and vulnerabilities defined above. Heightened security awareness throughout the open environment occurs in many cases because the types of threats that exist today continue to be assessed and inventoried rapidly. Additionally, the intrusion or disruption of the global network environment is frequently "front page news" and widely broadcast to both the technical and security community. The "importance" of information security in a C^4I environment not only is measured through "loss of life" indicators, but efficiency of operations and return on investment criterion. As a result, security awareness is quantified as essential to all support phases of mission critical programs.

Conclusion

The threats and vulnerabilities to the open environment are more varied and increased from those to the closed environment. However, techniques are available to mitigate these threats and vulnerabilities to an acceptable level of risk. Applying these mitigations to the open environment not only benefits emerging and sensitive traffic being carried on these networks, but also strengthens the communications infrastructure within this country.