SECTION 2. INFORMATION AND COMMUNICATION TECHNOLOGIES

DOI https://doi.org/10.30525/978-9934-26-459-7-11

RELIABILITY CRITERIA OF SOFTWARE TOOLS FOR REMOTE ADMINISTRATION

Andrii Osipov[1], Maiia Liuta[2], Mariia Zakharova[2]
[1]ISMA University of Applied Science, Latvia
[2]Cherkasy State Business-College, Ukraine
**Corresponding author's e-mail: andrey@visual-craft.com, maiialiuta@gmail.com, zmaria17mz@gmail.com*

Abstract

In the modern Internet, there are a vast number of risks associated with remote access to PCs, including traffic interception, personal data theft, and even file replacement with viruses. Therefore, it is crucial to pay attention to encryption methods and how traffic is transported over the Internet.

Key words: *efficiency, evaluation, software, remote administration, criteria, reliability.*

Introduction

Reliability of software is the ability of a software product to perform certain functions without failure under specified conditions for a specified period of time with a sufficiently high probability. The degree of reliability is characterized by the probability of the software product operating without failure for a certain period of time.

There are four main components of functional reliability of software systems:

- Fault tolerance: the property of a program to continue operating despite the presence of faults or errors.
- Performance: the property of a program to operate correctly (as expected by the user) throughout the specified period of use.
- Safety: the property of a program not to be dangerous to people and surrounding systems.

− Security: the property of a program to resist accidental or intentional intrusions.

In addition to the risks in the Internet space for remote access, a reliable physical connection to the global network is very important. When using remote access, the system administrator becomes highly dependent on the reliable operation of the power grid on the entire chain of network equipment, as well as on the reliable operation of the network equipment.

Based on this, the main risks for the user of remote access to a PC can be identified:

− The risk of remote rebooting of the PC, the system may not boot, as a result of which remote configuration of the PC will be impossible until local intervention.

− The risk of losing connection with the remote PC due to malfunction of the network equipment of the provider.

− The risk of losing connection with the remote PC due to the fault of the power supply of the intermediate equipment of the provider.

− The risk of losing connection with the remote PC due to the absence of power supply of the remote office and, as a result, the inability to remotely turn on and continue configuring the PC.

− The risk of losing connection with the remote PC due to the fault of the network equipment in the local network, the network equipment (switch, for example) may hang, as a result of which access to the PC will be impossible.

− There is a risk that part of the lightning discharge will get into the twisted pair, then all the network cards will burn out along the network distribution. In the case of a server, this is very critical. And in this case, the remote session will be irreversibly torn. In this case, access to the "network card" may help to see the affected areas.

− Risks associated with insufficient connection security. In remote access programs, there is the possibility of using a buffer exchange. There is a risk that during copying, a file may be replaced with a malicious one with the same name and size. As a result, there is a risk of getting a system infected with a Trojan in the best case, and in the worst case, getting a miner virus or a ransomware.

− When remotely connecting using remote access services from publicly available access points, especially WI-FI, there is a risk of intercepting login credentials and subsequently using them for malicious purposes.

− In the case of LiteManager, at first glance, it is a very convenient solution for remote administration. It consists of a server and client parts. Once installed on a remote PC, the server part can establish an unlimited

number of connections with the remote PC using a combination of ID and password. At first glance, everything is fine. However, the manufacturer company used a solution for processing connections similar to Torrent. Any interested person can install the NOIP Server on their PC and intercept all encrypted traffic passing through their server. This is a huge risk and a security hole for the program and the network in which it is installed.

In connection with the constant growth of attacks on local networks, new vulnerabilities are constantly being discovered in software and, as a result, a new type of attacks appears. Under these conditions, responsible systems for the security of remote access must be able to withstand various attacks, both external and internal, automated and coordinated. Sometimes an attack lasts a few seconds, sometimes probing vulnerable spots is slow and stretches over hours, so suspicious activity is practically invisible. The goal of attackers may be to violate all components of information security – availability, integrity, or confidentiality. The main threats to information security include:

- disclosure of confidential information;
- compromise of information;
- unauthorized use of resources of the local computing network;
- improper use of its resources;
- unauthorized exchange of information;
- denial of information;
- denial of service.

Means of implementing the threat of disclosure of confidential information may be unauthorized access to databases, eavesdropping on local computing network channels, etc. In each case, obtaining information that is the property of some person (or group) causes substantial harm to its owners.

Compromise of information is typically carried out by making unauthorized changes to databases, as a result of which the user is forced to either abandon it or spend additional efforts to detect changes and restore true information. In the case of using compromised information, the user may make incorrect decisions with all the consequences that follow.

Unauthorized use of local computing network resources, on the one hand, is a means of disclosing or compromising information, and on the other hand, has independent significance, since, even without touching user or system information, it can cause certain damage to subscribers or administration of the local computing network. The extent of damage can vary widely – from reducing the receipt of financial resources to the complete failure of the network.

Improperly sanctioned use of local computing network resources can also lead to the destruction, disclosure, or compromise of the specified resources.

This threat most often is a result of errors in the software of the local computing network.

Unauthorized exchange of information between subscribers of the local computing network can lead to one of them receiving information that is forbidden to access, which is equivalent in its consequences to the disclosure of information.

Refusal of information consists in the denial by the addressee or sender of this information of the fact of its receipt or sending. This, in particular, can serve as a reasoned reason for one of the parties to refuse a previously supported agreement (financial, trade, diplomatic, etc.) "technically", formally not refusing it, thus can cause significant damage to the other side.

Refusal of service is a very significant and quite common threat, the source of which is the local computer network itself. Such a refusal is especially dangerous in situations when a delay in providing network resources to the subscriber can lead to serious consequences for him. For example, the absence of data necessary for decision-making in the subscriber may be the cause of his irrational or non-optimal actions.

Conclusions

Reliability of software is crucial for the successful performance of its intended functions without failure. The main components of functional reliability of software systems are fault tolerance, performance, safety, and security. Remote access to a PC poses various risks, including remote rebooting, loss of connection, and insufficient connection security, which can result in unauthorized access, compromised information, and unauthorized use of resources. Responsible systems for remote access security must be able to withstand various attacks and protect against disclosure, compromise, and denial of information or service

References

1. Zharko E. F. Assessment of the quality of software for automated control systems: theoretical foundations, main trends and problems. *System identification and control tasks SICPRO* '15, vol. 1(32), 2015. Pp. 1129–1143.

2. Stallings, W., & Brown, L. Computer Security: Principles and Practice. Pearson, 2019.

3. Ross Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems," Wiley, 2020.