Trusted Systems, Data Access Control, and Trojan Horse Defense

Application in Modern Communication Systems

NAMITH K P
VML22CS127
Department of Computer Science
27-02-2026

Abstract

Modern communication systems rely on robust security frameworks to protect sensitive data and ensure reliable service. A Trusted System correctly enforces a defined security policy, guaranteeing confidentiality, integrity, and availability. This report examines the core concepts of trusted systems, data access control models, and Trojan horse threats with their defense mechanisms. A case study of a cloud communication platform demonstrates how these principles are applied in practice to achieve secure, controlled, and resilient communication environments.

1 Introduction

A Trusted System is defined as a system that correctly enforces a defined security policy. As digital infrastructure grows more complex, ensuring the trustworthiness of systems that handle sensitive data has become a foundational requirement in computer security. Trusted systems are deployed across modern communication environments including cloud messaging platforms, email services, and enterprise collaboration tools.

A trusted system ensures three core security properties:

- Confidentiality – Information is only accessible to authorised parties.
- Integrity – Data is not altered or corrupted by unauthorised actors.
- Availability – Systems and data remain accessible to authorised users when needed.

1.1 Core Components

The architecture of a trusted system rests on three fundamental components:

- Trusted Computing Base (TCB) – The combination of hardware and software responsible for enforcing the security policy. All other system components depend on the TCB's correctness.
- Security Kernel – The core mechanism within the TCB that implements access control policies, mediating all access to system resources.
- Reference Monitor – An abstract machine concept that intercepts and evaluates every access request, ensuring no operation bypasses the security policy.

2 Data Access Control

Data access control is the mechanism that regulates which subjects (users or processes) can perform which operations on which objects (files, databases, network resources). Standard operations include Read, Write, Execute, and Modify. Effective access control is a primary defence against data leakage, insider misuse, and unauthorised access.

2.1 Access Control Models

Model	Basis	Description
DAC	Owner discretion	The resource owner decides who may access the resource.
MAC	Security labels	Access decisions are made by the system based on classification labels.
RBAC	User roles	Permissions are assigned to roles; users are assigned roles.
ABAC	Attributes	Access is determined by user, resource, and environmental attributes.

2.2 Threats Prevented by Access Control

Properly implemented access control mechanisms address a range of threats:

- Unauthorised access is prevented by ensuring only credentialed users can reach protected resources.
- Data leakage is mitigated by limiting the scope of readable data per role or label.
- Insider misuse is curtailed through the principle of least privilege, granting users only the minimum permissions required for their function.

3 Trojan Horse Attacks and Defence Mechanisms

A Trojan horse is malicious software disguised as a legitimate and benign program. Unlike viruses, Trojans do not self-replicate, but they exploit user trust to gain execution. Once active, a Trojan can conduct a range of harmful activities under the privileges of the unsuspecting user.

3.1 Capabilities of Trojan Horse Malware

- Stealing sensitive data including credentials and personal files.
- Capturing passwords through keylogging or screen capture.
- Creating persistent backdoors for remote attacker access.
- Misusing user privileges to escalate access or modify system configurations.

3.2 Defence Mechanisms

A multi-layered defence strategy is essential to mitigate Trojan horse threats:

- Principle of Least Privilege – Users and processes are granted only the minimum permissions required, limiting the damage a Trojan can cause.
- Mandatory Access Control – System-enforced policies prevent a Trojan from accessing data beyond the user's cleared security level.
- Sandboxing – Applications are executed in isolated environments, preventing access to the broader system.

- Code Signing – Only cryptographically signed software from trusted publishers is permitted to execute.
- Continuous Monitoring and Auditing – Real-time analysis of system activity detects anomalous behaviour indicative of Trojan activity.

4 Case Study: Cloud Communication Platform

This case study examines the security architecture of a cloud-based communication platform, demonstrating how trusted system principles, access control models, and Trojan horse defences are applied in a production environment.

4.1 Authentication and Identity Verification

Users authenticate via Multi-Factor Authentication (MFA), combining a password with a one-time code delivered to a registered device. Upon successful credential submission, the platform's Identity and Access Management (IAM) system verifies the user's identity before any session is established.

4.2 Access Control and Data Encryption

Once authenticated, access to platform resources is governed by a hybrid RBAC/ABAC model. Role assignments determine base-level permissions (e.g., viewer, editor, administrator), while attribute-based policies apply contextual constraints such as device type, time of access, and geographic location. All data in transit is protected using TLS encryption.

4.3 Malware Mitigation

Third-party integrations and client applications are executed within sandboxed containers, preventing any compromised component from accessing other platform resources. Code signing ensures that only verified application builds are deployed.

4.4 Continuous Monitoring and Incident Response

The platform employs real-time behavioural monitoring. Anomalous activity — such as unusual login locations, rapid data exports, or repeated failed access attempts — triggers automated session termination and alerts the security operations team.

4.5 Outcomes

- Secure communication ensured through end-to-end encryption and MFA.
- Controlled data access via fine-grained RBAC/ABAC policies.
- Reduced malware impact through sandboxing, code signing, and least privilege enforcement.

5 Comparison of Security Mechanisms

Mechanism	Primary Goal	Example Application
Trusted Computing Base	System-wide security enforcement	Hardware security modules
MAC / RBAC / ABAC	Controlled data access	Cloud IAM policies

Mechanism	Primary Goal	Example Application
Sandboxing	Malware containment	Browser tabs, container runtimes
Code Signing	Software authenticity	App store verification
Continuous Monitoring	Threat detection and response	SIEM platforms

6 Conclusion

Trusted systems form the security backbone of modern communication infrastructure. Through the enforcement of defined security policies via the Trusted Computing Base, Security Kernel, and Reference Monitor, these systems guarantee confidentiality, integrity, and availability. Data access control models — particularly RBAC and ABAC — provide the granularity required to manage diverse user populations and complex resource hierarchies. Defence mechanisms against Trojan horse attacks, including least privilege, sandboxing, and continuous monitoring, further harden these environments against insider and external threats. As demonstrated in the cloud communication platform case study, the layered application of these principles yields a secure, resilient, and trustworthy communication system.

References

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
2. Stallings, W. (2022). Cryptography and Network Security: Principles and Practice. Pearson.
3. NIST Special Publication 800-53: Security and Privacy Controls for Information Systems.
4. 3GPP 5G Security Specifications (TS 33.501).
5. RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3.