






# A Zero Trust Model for Networked Self-Service Terminals

Boya Liu<sup>1</sup> , Haitao Ye<sup>1</sup> , Jizhou Chen<sup>2,3</sup>, Yong Xia<sup>2</sup>, and Jieren Cheng<sup>3</sup> 

<sup>1</sup> School of Information Technology and Electrical Engineering, Southern Cross University of Australia, Military Rd, East Lismore, NSW 2480, Australia

18975804657@163.com

<sup>2</sup> Guangdong Provincial Administration of Government Services and Data, Guangzhou 510030, Guangdong Province, China

<sup>3</sup> School of CyberSecurity and Crypt-Ology, Hainan University, Haikou 570228, Hainan Province, China

**Abstract.** Networked self-service terminals (NSST) are intelligent devices that are widely used in various fields. They can provide convenient services and interactions, but they also face various security threats. Traditional security protection models are often based on the division of trust boundaries, treating the internal of the terminal as a trusted area, and the external of the terminal as an untrusted area. However, in the application scenarios of self-service terminals, the concepts of internal and external have become blurred, and the security problems have gradually emerged. The traditional boundary security model can no longer meet their security needs. To solve this problem, a zero-trust model for NSST is proposed. This model is based on the security framework of the NIST zero-trust model, which no longer assumes that any area or component is trustworthy, but instead uses multi-level, multi-dimensional, and dynamic security policies to achieve comprehensive and real-time monitoring and protection of the terminal. On this basis, the characteristics and security requirements of NSST are analyzed, and the overall architecture and core components of the zero-trust model are designed, including identity authentication, access control, data encryption, behavior audit, permission management and other aspects. The protection of NSST is achieved by the collaboration of components.

**Keywords:** Zero trust model · Self-Service Terminal · Network Security · Security Protection

## 1 Introduction

### 1.1 Research Background and Motivation

With the continuous progress of internet technology and the popularization of intelligent hardware devices, more and more devices are connected to the internet, making the transmission of information more convenient and efficient. Connected devices are widely used in various fields due to their advantages of self-service, efficiency, and convenience. However, the openness, interconnectivity, and programmability of Networked

Self-Service Terminals (NSST) have also made them targets for hackers and malicious software intrusion, resulting in security risks for these interconnected devices.

In addition, with the rise of mobile internet and the IoT, the application scenarios of connected self-service devices are becoming increasingly widespread, such as in fields such as banking, hospitals, catering, retail, etc. Although their popularization and use have improved work efficiency and service quality, they have brought more security risks. For example, on a bank ATM, malicious software can steal user account information and passwords; On hospital self-service registration machines, hackers can cause serious consequences by tampering with the system. These security issues also pose increasingly serious security threats and challenges to these networked self-service terminals.

## 1.2 Research Purpose and Significance

This article aims to design a Zero Trust Model (ZTM) for NSST to improve their security and reliability. On the basis of the existing ZTM, combined with the characteristics and security requirements of NSST, a feasible and referential Zero trust security model is proposed to provide more comprehensive and rigorous technical support and guarantee for the security of self-service terminals. Through the relevant research in this article, new ideas can be provided to address the security threats and challenges faced by NSST, improve the security and reliability of self-service terminals, and ensure the privacy of users and the security of enterprise data.

Theoretically, the Zero trust security model is a technical means based on authentication, authorization, encryption, audit, etc., which transfers the basic point of network security from traditional border defense to fine-grained control of data flow, and realizes the comprehensive coverage of network security. Compared to traditional boundary defense models, ZTMs pay more attention to data security protection and can better adapt to the changes in security threats and attack methods in modern network environments [1]. In network terminals such as NSST, the ZTM can improve data security, reduce the occurrence of security vulnerabilities, and reduce security risks.

In a practical sense, the security issues of online self-service devices have attracted widespread attention and attention. With the popularization of the Internet and the development of technology, online self-service devices have become an indispensable part of people's lives, involving important fields such as finance, healthcare, and transportation, and their security is particularly important. The Zero trust security model can effectively solve the security problem of NSST, improve the security and reliability of devices, and protect users' privacy and asset security. Therefore, adopting the Zero trust security model can provide more comprehensive and rigorous security guarantee for NSST, protect user information and enterprise data from threats, and maintain social stability and security.

## 1.3 Research Status and Issues

With the continuous development of network security technology, Zero Trust Models (ZTMs) have gradually become one of the current research hotspots. Domestic and foreign scholars have achieved a series of achievements in the research of ZTMs.

Among them, the Beyond Corp model proposed by Google and the ZTM proposed by Forrester are representative ZTMs. Google's Beyond Corp model is a ZTM based on cloud computing and network security technology, aimed at protecting Google's internal network and cloud services through a borderless security architecture. This model achieves fine-grained control of the network by using a unified authentication and authorization mechanism to control user access rights and authenticate and authorize devices and applications [2]. Forrester's ZTM emphasizes fine-grained control over devices, users, applications, and data to improve network security. This model achieves security protection of data by using multiple authentication and access control techniques [3].

Domestic researchers of China have also been involved in the research of ZTMs, but compared to foreign countries, they are still in the early stages. At present, the domestic research mainly focuses on the theory, and has not formed a relatively mature Zero trust security model.

Although the ZTM has achieved certain results in network security, it still has significant results in only some areas. Firstly, most of the existing ZTMs are designed for centralized network environments such as data centers and cloud computing, without in-depth research in the field of NSST. Secondly, the existing ZTM lacks an effective defense mechanism against security issues in NSST, such as identifying and defending security vulnerabilities in old operating systems used by NSST. Therefore, these unsafe factors that may expose a large area of the internal network at any time are the starting point of this study. This study will provide new ideas for eliminating security threats in NSST through the basic theory of existing zero trust models.

## 2 Overview of the Zero Trust Model

### 2.1 The Origin and Evolution of the Zero Trust Model

At present, more and more organizations and enterprises have established their own information systems on the network, and these information systems often need to interact with external networks, which makes the network security problem more complex and serious. The traditional boundary security concept believes that there is a clear boundary between the internal network and the external network. By setting firewall, intrusion detection, access control and other security measures on this boundary, the security of the internal network can be effectively protected. However, with the rise of cloud computing, mobile office and other emerging technologies, the boundary between the internal network and the external network is gradually blurred, which makes the traditional boundary security concept more and more difficult to meet the challenges of network security. In order to address this challenge, ZTMs have emerged.

### 2.2 The Core Concept of the Zero Trust Model

ZTM is a network security architecture based on minimizing trust. Its core idea is not to trust any user, device, application or network traffic, but to require authentication and access control in every link [4]. The emergence of the ZTM indicates that traditional border security concepts are no longer able to meet the requirements of today's network security, and a more advanced and flexible security architecture is needed.

### 3 Analysis of Security Issues in NSST

#### 3.1 Application Scenarios and Characteristics of NSST

Networked self-service terminal is a terminal device that can provide various self-service services. It is connected to the backend server through the internet, and users can purchase goods, query information, and handle various services through these terminal devices. These terminal devices can be deployed in various public places or within enterprises, such as shopping malls, stations, airports, hospitals, banks, etc. At stations and airports, NSST can provide services such as flight and train schedules, ticket purchases, boarding, and pick-up. In hospitals, NSST can provide services such as registration, payment, drug collection, and medical reimbursement. In banks, NSST can provide services such as withdrawal, transfer, and account inquiry. It can be said that NSST have a wide range of application scenarios in various industries, providing users with a more convenient service experience. Under the widespread application of NSST, it also has some characteristics:

1. **Self-service:** NSST provide self-service, allowing users to freely choose the required service content without manual intervention, thereby reducing labor costs and waiting time.
2. **Intelligent:** The online self-service terminal is equipped with various sensing devices, scanners, speech recognizers, etc., which can identify user needs and provide corresponding services, achieving intelligent interaction.
3. **Efficiency:** NSST can operate 24 h a day without interruption, with a wide range of services and the ability to provide services to multiple users simultaneously, thereby improving service efficiency.
4. **Scalability:** NSST can access and control remote servers through network connections, and service content can be expanded and updated at any time.

However, the widespread application of NSST has also brought some security issues. Due to the connection between NSST and the internet, they may face the threat of being invaded by network attackers.

#### 3.2 Analysis of the Current Situation of Security Issues in NSST

In modern society, more and more self-service terminals use the Internet for data transmission and interaction to meet people's various needs. The widespread application of NSST has brought many security threats and attack methods, but the existing security defense measures are insufficient to resist these potential risks. Therefore, NSST are prone to posing threats to data and software in the following aspects [5]:

1. **Network Security:** The operating system and software versions are too old: Many NSST use operating systems and software versions that are too old and vulnerable to known vulnerabilities. Hackers can use these vulnerabilities to invade the system or obtain sensitive information. Unable to upgrade patches in a timely manner: Even with new vulnerability patches, many NSST cannot upgrade in a timely manner. This allows hackers to exploit vulnerabilities to attack systems, while terminal operators or enterprises fail to fix vulnerabilities in a timely manner and cannot respond quickly

to attack events. Improper device management: Many NSST have improper device management, such as using weak passwords, not changing default passwords, and not configuring firewalls correctly, which can easily allow hackers to invade the system.

2. **Software Security:** Security issues with third-party software: Many NSST require the installation of third-party software or applications, which may have inherent vulnerabilities or security risks. Hackers can exploit these vulnerabilities for attacks.

Security issues with their own software: The software used by NSST may also have vulnerabilities or security risks, such as lack of good code specifications, lack of security testing, and other issues. Lack of timely software updates: Software suppliers may not update their software in a timely manner, resulting in known vulnerabilities not being repaired in a timely manner, leading to opportunities for hackers to exploit.

3. **Management Security:** Data management: NSST usually require users to provide personal sensitive information, such as account number, password, ID number, etc. If the user information management of NSST is not in place or there are insufficient security measures to protect users' sensitive information, there is a risk of information leakage. In terms of device management: The management of NSST is also prone to problems, such as untimely maintenance, inadequate security measures, and administrators' excessive trust in the system. These management problems may lead to a decline in system security, which may lead to Data breach or other security problems.

### 3.3 Security Threats and Attack Methods of NSST

With the increase in the number of NSST, the security threats and attack methods they face are becoming increasingly diverse and complex. By analyzing the security threats and attack methods faced by NSST, it can provide a basis for the subsequent design of ZTMs.

#### 1. Network Security:

DDoS attack: Hackers may exhaust the network bandwidth of self-service devices by sending a large amount of malicious traffic to the network where the devices are located, resulting in the devices being unable to function properly.

Malicious software attack: Hackers may inject malicious software (such as viruses, trojans, etc.) into self-service devices, causing them to be controlled or stealing internal data. Port scanning attack: Hackers may scan the open ports of self-service devices to identify vulnerabilities and exploit them for attacks.

Man-in-the-middle attack: hackers may obtain or tamper with the communication content by cheating the communication between self-service devices and servers to steal data or control the devices. Identity authentication attack: Hackers may obtain the login password of self-service devices through violent cracking or social engineering attacks, thereby gaining control of the device.

#### 2. Software Security:

Buffer overflow attack: hackers may send data exceeding the buffer capacity to the device, crash the device program and run malicious code to control the device.

SQL injection attack: hackers may attack the database of the device and steal or tamper with data by injecting malicious SQL statements.

XSS attack: Hackers may inject malicious script code into the device to attack the device's web application, achieving the goal of controlling the device or stealing user data.

Reverse engineering attack: hackers may find vulnerabilities or weaknesses in equipment through Reverse engineering of equipment programs, and use these vulnerabilities or weaknesses to attack.

Encryption algorithm attack: Hackers may attack the data security of devices by analyzing the encryption algorithm or key used, such as stealing encrypted data or tampering with encrypted data.

### 3. Manage Security:

Unauthorized access attack: Hackers may obtain unauthorized access to self-service devices by deceiving or attacking administrator credentials, in order to obtain sensitive data or control the device.

Remote attack: Hackers may control devices or steal sensitive information by remotely accessing administrator accounts or management interfaces.

## 4 Design of a ZTM for NSST

### 4.1 Analysis of Security Requirements for NSST

Network and information security refer to a three-dimensional system structure that involves multiple aspects of content, based on the structural characteristics of the network, taking different measures from different network levels and system applications to improve and defend [6]. Therefore, it is necessary to analyze the security requirements of NSST and provide ideas for future security solutions based on the ZTM. For the security needs of NSST, the following aspects can be considered:

1. **Authentication and Authorization:** NSST require authentication and authorization of users, and only users who have passed the authentication and authorization can perform corresponding operations. Therefore, it is necessary to deploy effective identity authentication and authorization mechanisms on devices, such as the use of multi factor identity authentication (MFA) and other technologies to ensure the legitimacy and credibility of user identities.
2. **Data Protection:** NSST typically involve the collection and processing of user sensitive information, so a series of technical measures need to be taken to protect the security and privacy of these data. For example, technologies such as encrypted transmission, data classification and labeling, data backup and recovery are used to ensure the security of data during transmission and storage.
3. **Malicious Behavior Detection and Prevention:** NSST need to have the ability to detect and prevent malicious behavior, such as intrusion detection, threat intelligence analysis, antivirus software, and other technologies. These technologies can effectively prevent hacker attacks, malicious software, and other threats.

4. **Operational Audit and Risk Assessment:** NSST need to have the ability to conduct operational audit and risk assessment, track users' operational behavior, and conduct risk assessment and threat analysis on devices. These technologies can detect abnormal operations and risk events in a timely manner and take timely measures to handle them.
5. **Management and Operation:** NSST need to have effective management and operation measures, such as device configuration management, vulnerability management, software updates, backup and recovery measures. These measures can ensure the stability and safety of equipment operation, and promptly handle equipment failures and safety incidents.

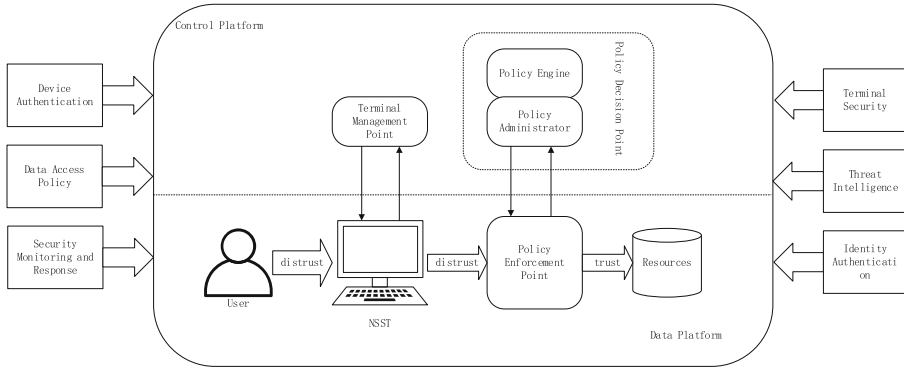
#### 4.2 Design of a Security Solution for NSST Based on ZTM

The core idea of the ZTM based on the NIST framework is "never trust, always verify", which means that no device, user, or request should be trusted by default, but each access request should be fully authenticated, authorized, and encrypted to protect resources and data [7]. At the same time, based on the characteristics of self-service, intelligence, efficiency, and scalability of NSST, as well as the analysis of the security requirements of networked autonomous terminals, a specific security solution based on the ZTM will be designed from the following aspects.

1. **Develop access strategies:** sort and classify NSST and related resources, identify all sensitive and non sensitive data and applications in the system, and establish corresponding asset lists. Develop access policies based on asset inventory, including authentication, access authorization, and access restrictions for different users and devices.
2. **Implement network segmentation:** By isolating NSST from other devices, network segmentation is implemented to prevent horizontal movement attacks.
3. **Strengthen identity authentication:** Use multi factor identity authentication to verify the user's identity, and protect the user's identity information through hardware, software, and other technical means.
4. **Implement permission management:** implement the Principle of least privilege based on the roles and responsibilities of users to ensure that users can only access the resources they need.
5. **Monitoring and response:** Detect and respond to security events by implementing real-time monitoring and response mechanisms to prevent hacker intrusion and Data breach.
6. **Implement data encryption:** Encrypt sensitive data to ensure its security during transmission and storage.

#### 4.3 Security Framework and Process for NSST

Based on the above security scheme design, in order to address the security issues of NSST, this study designed a security framework based on the ZTM to adapt to the scenarios of NSST. Firstly, in this model framework, users, terminals, and data are considered untrustworthy. The security framework is shown in Fig. 1 and consists of the following components:



**Fig. 1.** Safety framework based on NIST ZTM

1. Core components:

- A. Data: All data involved in the scenario of NSST.
- B. User: A person who uses an online NSST.
- C. Device: The NSST device used by the user.
- D. Resources: Network resources that need to be accessed by NSST.
- E. Self-service terminal: A NSST device provided to users.
- F. Policy Engine: A system that evaluates and authorizes access requests from users, devices, and NSST based on predefined rules and conditions.
- G. Policy administrator: The person or system responsible for defining and updating access policies.

2. Logic components:

- A. Policy Execution Point (PEP): A system or software module that executes access control between users, devices, or NSST and resources.
- B. Policy Decision Point (PDP): A system or software module that allows or denies access requests based on the output of the policy engine.
- C. Policy Management Point (PMP): A system or software module responsible for distributing access policies defined by policy administrators to various PEPs and PDPs.
- D. Policy Information Point (PIP): Refers to a system or software module that provides relevant information required by the policy engine.
- E. Terminal Management Point (TMP): Refers to the system or software module responsible for managing the configuration, updates, monitoring, and maintenance of NSST.

3. Functional components:

- A. Identity authentication: The process of verifying the identity of users, devices, and NSST, such as using multi factor authentication technology.
- B. Device authentication: The process of verifying whether devices and NSST meet security requirements.
- C. Data access strategy: The process of protecting data from leakage or tampering during transmission and storage, such as using encryption, signature, hash, and other technologies.



- D. Security monitoring and response: refers to the process of monitoring Réseau Sentinelles activities, detecting and responding to potential security threats, such as using log analysis, intrusion detection, alarm notification and other technologies.
- E. Terminal security: The process of protecting the hardware and software of NSST from attacks and damage, such as using physical locks, cameras, firewalls, and other technologies.
- F. Threat intelligence: Collect, process, and analyze data to understand the motives, targets, and attack behaviors of threat actors, helping us make faster, wiser, and more data-supported security decisions.

Compared to the NIST, the main difference of this security architecture is the addition of self-service terminal components and the addition of terminal management points for centralized management of NSST, as well as terminal security functions to protect the security of NSST in real-time.

The process of this security framework in the scenario of NSST is as follows:

1. Users use devices to connect to NSST and initiate requests to access resources.
2. PEP intercepts requests and sends access requests and related information to PDP, such as the identity, attributes, status, etc. of users, devices, and NSST.
3. PDP evaluates and authorizes access requests based on the output of the policy engine, and returns the decision to allow or deny to PEP.
4. The policy engine evaluates and authorizes access requests based on the access policies defined by the policy administrator and relevant information obtained from PIP, such as threat intelligence, SIEM system analysis results, etc.
5. PEP executes PDP's decisions, and if access is allowed, forwards the request to the resource; If access is denied, an error message is returned to the user.
6. Data access policies protect data from leakage or tampering during transmission and storage, such as using encryption, signature, hashing, and other technologies.
7. Terminal security protects the hardware and software of NSST from attacks and damage, such as using physical locks, cameras, firewalls, and other technologies.
8. TMP manages the configuration, update, monitoring, and maintenance of NSST to ensure their normal operation.

## 5 Discussion and Outlook

### 5.1 Discussion on the Advantages and Disadvantages of a ZTM for NSST

The traditional network boundary-based security protection model determines the security level of the object to be protected based on the sensitivity of business and information, and divides it into security zones. Then, relevant technologies are used for security isolation to achieve protection for each security zone [8]. However, due to the inability of traditional security models to adapt to higher intensity attack scenarios targeting NSST, this paper proposes a ZTM for NSST, which emphasizes the verification and authorization of all devices and users, and even within the internal network, all traffic needs to be audited and restricted, thereby improving the security and reliability of the system. Here are the advantages and disadvantages of the ZTM:

### 1. Advantages:

**More secure:** The ZTM can better protect the security of the system and reduce the risk of malicious attacks by verifying and authorizing devices and users.

**More reliable:** The ZTM can better ensure the reliability of the system and reduce the risk of system failure by auditing and limiting all traffic.

**More flexible:** The ZTM does not rely on specific network structures or devices, can adapt to different network environments and device requirements, and has more flexible deployment methods.

**More controllable:** The ZTM audits and restricts all access requests, enabling better management of user and device access permissions and enhancing system controllability.

### 2. Disadvantages:

**Single point risk:** Zero trust is a strong control architecture, and the control of resources is concentrated on the gateway. Therefore, once a Single point of failure occurs, the whole business will be interrupted.

**Risk of centralized permissions:** The zero trust architecture converges and concentrates many risks, reducing management costs. However, if centralized management is out of control, it will also bring greater risks;

**Complexity risk:** The ZTM requires auditing and limiting all traffic, requiring the deployment of a large number of security devices and technologies, which increases the complexity of the system.

**High cost risk:** The ZTM requires verification and authorization on all devices and users, requiring a significant investment of cost and effort.

## 5.2 Future Development Prospects of ZTM for NSST

The ZTM for NSST is the future development direction in the field of security for NSST. On the one hand, in terms of technology, the future ZTM will rely more on the support of advanced technologies such as security chips, artificial intelligence, and blockchain to improve security and credibility. The development of these technologies will provide more possibilities and support for the application of ZTMs. On the other hand, in terms of application, future ZTMs will pay more attention to the expansion and adaptability of application scenarios. ZTMs for NSST can be applied to more fields, such as smart homes, industrial control, and so on.

Overall, the ZTM for NSST is the development direction in the future security field of NSST, and will become an important means of ensuring the security of NSST.

## 6 Conclusions

This article proposes a ZTM for NSST based on the NIST zero trust architecture. Through the collaboration of core components, multiple logical components, and rich functional components, it achieves continuous identity verification and authorization of terminals,

encryption of data, minimization and differentiation of access, and restriction and audit of operation and maintenance operations. The ZTM proposed by the relevant research institute in this article can provide more efficient and secure security solutions for NSST, providing useful reference and guidance for practical applications in related fields.

## References

1. Assunção, P.: A zero trust approach to network security; proceedings of the. 2010 In: Proceedings of the Digital Privacy and Security Conference, F, (2019)
2. Ward, R., Beyer, B.: Beyondcorp: A new approach to enterprise security (2014)
3. Kindervag, J.: Build security into your network's dna: The zero trust network architecture. Forrester Res. Inc. 27 (2010)
4. Feng, J.Y., Yu, T.T, Wang, Z.Y., et al.: Edge ZTM for Resisting the Threat of Lost Terminals in Power IoT Scenarios. *Comput. Res. Dev.* (2022)
5. Shao, L., Niu, W.N., Zhang, X.S.: Self-service terminal network security threat assessment and response in IoT application scenarios. *J. Sichuan Univ. Nat. Sci. Ed.* **60**(1), 11 (2023)
6. Hu, Z.: *Network and Information Security*. Tsinghua University (2006)
7. NIST has released the second draft of SP 1800–35: Implementing a Zero Trust Architecture. *Inf. Technol. Standard.* (1): 1 (2023)
8. Wang, S.L., Feng, X., Cai, Y.B., et al.: Analysis and application of Zero trust security model. *Inf. Secur. Res.* **6**(11) (2020)