Research on Active and Passive Terminal Discovery Technology for Power Marketing Site

Chen Wei *, Xianzhou Gao and Ruxia Yang

Global Energy Interconnection Research Institute, State Grid Key Laboratory of Information & Network Security, Nanjing, China

*Corresponding author e-mail: chenwei@geiri.sgcc.com.cn

Abstract. Aiming at the possible access security impacts of various terminals caused by the openness of the power marketing site, it is necessary to solve the problem of monitoring the access to the marketing site network terminal, discovering the access terminal information in time, and the diversity of the access terminal types. According to the agent monitoring, there is a need for a terminal that does not perform terminal hardware and software transformation and does not affect the network architecture for terminal discovery. The active and passive terminal-based power marketing field terminal discovery technology proposed in this paper does not need to modify the equipment or network, and is deployed by means of bypass, using the agentless mode, and the terminal device can be automatically discovered.

1. Introduction

The power industry has carried out a lot of research and practice work on the safety access of various terminals, and has achieved certain results. However, the existing research results still have large limitations, which are mainly reflected in the following aspects: First, most of the current research results rely on customized terminals, which require hardware and software transformation of the terminal, and the authentication strength of security access. Basically, it matches the depth of the terminal customization. It is completely unsuitable for a large number of terminals that have been deployed in the field and cannot be customized by software and hardware. Second, most of the current access gateway architectures are used, and access authentication gateway devices are connected in series in the communication network. In the middle, all communication traffic needs to be represented by the gateway. The real-time security analysis of the data stream easily causes the performance problem of the service system, and objectively introduces the fault point of the network transmission, increases the communication delay, and involves the network structure in the implementation process. The transformation made it difficult to implement.

In summary, the security access work of various types of power service terminals has high dependence on the software and hardware of the service terminals, and the security access products are single, which cannot meet the business needs of the marketing site terminal without client pure bypass deployment, and the marketing scene is not solved. The problem of illegal terminal and counterfeit terminal discovery in time, this paper is to automatically discover the power marketing field terminal by studying the active and passive discovery technology suitable for the marketing scene.

2. Marketing terminal equipment discovery status

2.1. Marketing site terminal equipment status

The terminals currently deployed at the power marketing site include power self-service payment terminals, power wireless payment terminals, power wired POS terminals, queuing machines, marketing video surveillance terminals, office computer terminals, printers, fax machines, and the like. The operating system of the office computer terminal is a Windows or Linux system, and the terminal has hardware features such as a network card, a CPU, a hard disk, and various installation software features. The power self-service payment terminal uses a power security chip for the power customization terminal and has certain security protection capabilities. While dumb devices such as printers and monitoring terminals are connected to the network of the marketing site, the discovery and protection of such dumb devices are missing. The dumb devices are easily replaced and tampered with, and are not easily found.

2.2. Marketing site terminal management status

For the computer terminal management of the marketing site, the computer terminal is controlled and controlled by the desktop terminal management system deployed by the company. The desktop terminal management system is mainly processed by two parts: a client (client) software installed on each computer device and a console (Server) software installed on the management server. The client program automatically collects the main hardware information such as the host CPU, memory, hard disk, MAC card MAC address, motherboard chip, and board on the motherboard, and automatically reports it to the server. The management platform can query the specific information of all intranet terminal computers, and can also learn about hardware changes through hardware change queries, and can alarm for changes, and can find the access of counterfeit and forged devices. The monitoring software installed on the computer implements unified centralized supervision of computer terminal software installation, vulnerability patch installation, and anti-virus software installation by the desktop management system. The unified desktop management system realizes the control of intranet resources and the control of accessing the external network, restricts the access of the illegal computer to the network; and realizes the supervision of the behavior of the computer terminal.

For the power wireless payment terminal, since the power wireless payment terminal is a power customization terminal, the technical route based on the customized modification of the terminal hardware is adopted, and the hardware chip is used to realize the terminal security access, and the wireless payment terminal at the power marketing site adopts the security connection. Into the platform access solution to achieve monitoring and management of the access process.

For dumb devices such as printers and video surveillance devices, it is impossible to install a desktop management system for management and control. On the other hand, they are generic types of devices and are not suitable for customization. Therefore, such dumb devices lack security management during access. And there are difficulties in monitoring later. The marketing site is faced with the problem of not only discovering and controlling access to all types of terminals, but also not modifying the network architecture.

3. Agentless terminal automatic discovery technology

3.1. Terminal agentless discovery mode

The computer terminal utilizes the desktop management system to implement monitoring of the terminal device, and the power dedicated device realizes the discovery and access of the dedicated device through the customized software and hardware and the secure access platform. For third-party general-purpose equipment, dumb equipment, etc., equipment that is not customizable and modified, cannot be modified in the above manner for equipment discovery. In order to realize the discovery of such devices, it is necessary to discover and identify them in an agentless manner. The agentless terminal discovery method does not need to modify the terminal or install related software, but realizes the discovery and

identification of the device through active and passive discovery technologies. The agent-free terminal discovery technology can overcome the difficulty that the terminal cannot be customized or modified, and can easily identify and identify various types of devices, and is easy to deploy and adapt to various scenarios. The agentless mode generally uses bypass to the target network to monitor traffic in the network without modifying the network architecture or modifying the terminal. The discovery technology adopted by the specific agentless terminal discovery method is divided into active discovery and passive discovery technologies. This section will focus on proactive discovery techniques and passive discovery techniques.

3.2. Terminal Active Discovery Technology

Active host discovery technology refers to the analysis of the target host by sending a specific or forged data packet to the target host, and then according to the response information of the target host, such as returning the network characteristic value of the data packet or determining whether the target returns a data packet or the like. Feature information and identify the host's technology[1]. Terminal active discovery technology has been widely used on the Internet. Common technologies include IP address scanning, TCP/UDP port scanning, and ARP active detection. These technologies can be used to discover multiple key features for terminal discovery and identification.

3.2.1 IP Address Scanning

IP address scanning is the most common way to scan active hosts and discover the IP of the terminal. The basic principle of IP address scanning is to use ICMP's response request and response messages, and use PING to detect the target address[2]. The target system responds to this or not, and can be used as the identifier of the active host. This method is simple and convenient to implement. Calling the PING program to ping the target address can be achieved, but the problem is also very obvious. Many computers now have the ping response function turned off, or the firewall installed in the middle will invalidate the ping.

3.2.2 Tcp active discovery

(1)TCP connect scan

TCP connect scanning is the most basic TCP scan. The connect() system call provided by the operating system is used to connect to the port of each interested target host. If the port is listening, connect() will succeed; otherwise, the port is closed, ie no service is provided[3].

This method is relatively easy to implement, and it is determined whether the host is active or not by the activity of the port. The difficulty lies in choosing the right port, and using multiple ports will waste system resources and increase the scanning time.

(2) TCP SYN Scan

A TCP SYN scan is generally considered a "semi-open" scan because the scanner does not have to open a full TCP connection. The scanner sends a SYN packet, a TCP-based three-way handshake to establish a TCP connection. The return information of a SYN | ACK indicates that the port is in the listening state. If a SYN | ACK is received, the scanner must send another RST signal to close the connection.

This method is not fully established when the TCP three-way handshake is established, so the scanned host will not be recorded for this scanning process, and some connection-based protection systems (such as the IDS system) can be bypassed, which is somewhat concealed. This method is fast and effective, and can more accurately and effectively detect whether the host port in the LAN is open.

(3)TCP FIN scanning

Sometimes SYN scans are not enough to cover, or secret enough. Some firewalls and packet filters monitor some of the specified ports, and some programs can detect them. Instead, FIN packets may pass through firewalls and packet filters without any hindrance. The idea of this scanning method is that the closed port will reply to the FIN packet with the appropriate RST.

This method is more difficult to implement, but more is used to secretly scan the active host, and this method has a certain relationship with the scanning system. This scanning method is useful for distinguishing between UNIX and Windows NT

3.2.3 UDP/ICMP cannot reach the scan

UDP/ICMP port non-reachable scanning differs from the above methods in that it uses the UDP protocol. Since this protocol is simple, scanning becomes relatively difficult. This is because the open port does not send an acknowledgment to the scan probe, and the closed port does not need to send an erroneous packet. Fortunately, many hosts return an ICMP_PORT_UNREACH error when sending a packet to an unopened UDP port, so that the port is closed.

3.2.4 Active detection of ARP technology

The ARP protocol is used to actively detect hosts in the network. This technology has the advantage of fast network topology discovery and can actively collect network topology information[4]. The ARP detection technology mainly sends the ARP protocol through the target host on the Ethernet, and detects whether the target host returns the MAC address to the target host. The ARP detection has a strong penetration capability in the network segment. The occupied bandwidth is very small. However, the disadvantages of this method are also obvious. ARP detection can only detect active hosts in the network.

The specific process of ARP remote detection technology detection is as follows: first send the ARP broadcast packet to the target host, and thereby obtain the address name of the remote network host physical network, and then the probe host constructs the ARP broadcast data packet, and the network transmits the data packet physical frame. The first part will set the physical MAC to the physical MAC address of the probe, the target host will be set to the broadcast address, the source IP address will be set to the probe IP, and the protocol type will be set to ARP, forming a full-network broadcast forgery. ARP packet. At this time, other hosts in the network will respond positively to the ARP request sent by the probe host. After running this mode, the host terminal that survives in the network can be quickly discovered.

3.3. Terminal passive discovery technology

The passive host feature recognition technology is based on the network monitoring, and obtains the data of the target host and the network communication device by sniffing, analyzes the communication information of the remote host, and obtains the feature information of the target host. The so-called "passive" means not actively sending out data packets, but acquiring information through long-term interception and analyzing it[5]. Therefore, identification is a long-term, dynamic process. The main advantages of passive identification technology are: it has less impact on network performance, can be dynamically updated with network conditions, can adapt to multiple network environments, does not change the network architecture, and does not increase network load. The terminal passive discovery technology first captures the terminal traffic in the network, and then uses the message protocol to parse, and obtains the message key segments of different levels and positions, and further analyzes the terminal characteristic information. Common analysis contents include terminal clock offset rate, terminal network flow characteristics, and terminal protocol characteristics.

3.3.1 Clock Offset Rate

Calculate the relative clock offset rate between the two hosts by obtaining the host timestamp information contained in the host data packet, and extract the host fingerprint information according to the host clock offset rate to construct the host fingerprint database[6].

3.3.2 Network flow characteristics

Terminal network flow feature detection mainly focuses on the following characteristics: WS, TTL, DF, ToS, TL. These four characteristic information can be obtained through passive sniffing, and they are combined to form network flow characteristic information[7].

WS (Window Size): The window value in the TCP packet header. Windows will change this value in the session, while Unix remains unchanged.TTL (Time To Live): The lifetime of a data packet during network transmission.DF (Dont Fragment): No fragmentation flag, which is set by default for most operating systems.ToS (Type of Service): The type of various services.TL (Total Length): The total length, which refers to the packet length including the IP header.

By relying on these feature combinations and comparing with the data in the tag database, the operating system type and version information of the remote host can be determined to complete the location tracking of the target host in the network.

3.3.3 Fingerprint characteristics

The host fingerprint mainly includes four categories: hardware (MAC address, clock, etc.), software (operating system, browser type version, etc.), service (host name, system service, port, etc.) and user (online behavior, habits, traffic, etc.)[6].

The type and version of the operating system installed on the target host are identified and determined by the difference in the feature information existing between the TCP/IP protocol stacks of different operating systems. According to the TCP/IP Layer 4 protocol architecture protocol stack, including TCP, IP, UDP, ICMP, ARP, and data link layer protocols, the process implements an application layer protocol. The protocol stack parses the TCP/IP data of each layer protocol according to all the corresponding settings in the fingerprint database, and then decides to discard, continue to operate, re-establish the connection, and generate a response. The host feature information is identified and determined according to differences in characteristics in the TCP/IP protocol stack of different hosts.

3.3.4 Difference between the two methods

The process of obtaining the terminal feature information by the passive discovery technology is transparent, and does not need to be authorized access by the target host, and the terminal feature extraction is completed without the target host knowing, and the method has little influence on the network performance, and It is not affected by fluctuations in the network environment, has high stability, and can adapt to a variety of network application scenarios.

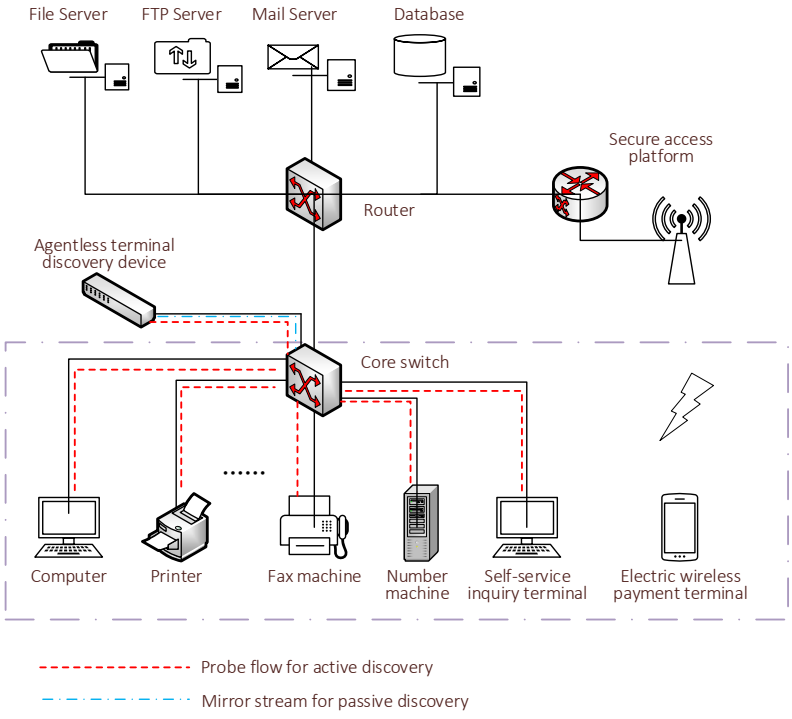

Figure 1. Schematic diagram of the terminal discovery mechanism for power marketing field

The active discovery technology constructs corresponding detection messages according to the characteristics of the protocol, and can obtain more detailed terminal information content and feature information.

4. Terminal discovery mechanism for power marketing site

The agent-free terminal discovery technology is applied to the application architecture of the site as shown in figure 1. The agentless terminal finds that the device bypass is next to the core switch, and does not need to modify the hardware and software of the terminal device, and does not affect the existing network structure.

The terminal discovers that the device discovers the device by detecting it in an active and passive manner. When the proactive mode is used for the probing, the non-proxy terminal discovery device sends various types of probe packets, including protocol packets such as ICMP and ARP, to obtain the required terminal information. When the passive mode is used for the detection, the agentless terminal finds that the uplink traffic packets captured by the mirroring at the switching level are parsed to obtain different levels of feature information of different terminals.

5. Conclusion

The computer equipment on the power marketing site can discover the terminal access situation in time through the desktop management system. The power marketing wireless payment device uses the power security chip to realize the terminal discovery and secure access by using the secure access platform, while other types of devices are especially dumb devices. Access cannot be discovered in time, and such devices are easily controlled and tampered, which becomes a security risk when the terminal is accessed. How to accurately and quickly discover the access of various terminals is a problem that needs to be solved at the power marketing site. The agentless terminal discovery technology based on active mode and passive mode studied in this paper has no client-side pure bypass deployment. It does not require software terminal hardware and software transformation, does not affect network service transmission performance, and can realize timely discovery of multiple device access. In particular, it includes a dumb terminal device, which quickly grasps the key feature information of the access device, and can be used to discover the access of the illegal terminal and the counterfeit terminal at the marketing site.

Acknowledgments

This work was financially supported by the science and technology project of State Grid Corporation of China: "Research on Key Technologies of Marketing Site Terminal Security Access" (Grand No. SGGR0000XTJS1800079).

References

[1] L. Polčák, J. Jirásek, and P. Matoušek. "Comment on “Remote Physical Device Fingerprinting”." IEEE Transactions on Dependable & Secure Computing 11.5(2014):494-496.
[2] Fu Xin. "Research and Implementation of Passive Recognition of Host Feature Information." Science and Technology and Engineering 13.3(2013): 652-658.
[3] Niu Rui. Research on the characteristics and identification of host network behavior patterns——Snort-based instant messaging and web session restoration. Diss. Beijing University of Chemical Technology, 2008.
[4] Zhao Jianjun. Research on the identification technology of cyberspace terminal equipment. Diss. 2016.
[5] Cao Laicheng, et al. "Network Space Terminal Equipment Identification Framework." Computer System Application 25.9(2016): 60-66.
[6] Liu Ying, Xue Xue, and Wang Yujun. "Remote operating system identification based on TCP protocol options." Information Security and Communication Security 11 (2007): 71-72.
[7] Huang Liyun. Design and Implementation of Network Traffic Identification Control System. Diss. Beijing University of Posts and Telecommunications, 2012.