Report1

This report aims to identify and analyze some of the Network security threats to sensor networks and to propose preventive measures. To analyze the potential risks. I use the following methods: (1) System characteristics (2) Identifying potential hazards (3) Testing potential vulnerabilities (4) Outlining preventive measures (5) Strengths and weaknesses analysis.

1. CHARACTERISTICS OF THE SYSTEM

A university will deploy 1000 sensors in the building, which are connected to a BACnet controller using the KNX protocol and to a management system in the main building via the IP network.

2. POTENTIAL THREATS

Firstly, BACnet's Peer to Peer system allows any device to write at the highest priority to writable objects in other devices.

Secondly in KNX, it is possible to set a so-called bus coupling unit (BCU) key. which was designed to prevent unwanted changes to the devices.

Hackers can gain access to the sensor system via the IP network. Once root access has been gained, the device can be uninstalled or the key reset using the BCU Key in the KNX protocol. This prevents the original administrator from restarting the service because the key has been changed.

3. TESTING POTENTIAL VULNERABILITIES

To test these vulnerabilities, it is recommended that the following penetration tests.

(1) Use Wireshark to capture packets on the target IP network and analyze the privilege information in the messages to try to crack the system password.

(2) Use Reaver to try to brute force the router password

(3) If (1) or (2) is successful, try to take over the controller's control privileges.

(4) modify the BCU key and run the shutdown command on the device.

An example - (October 2021: A German company was attacked and the BCU key in KNX was modified. The automation control devices in hundreds of buildings no longer work, Peter Panholzer)

4. PREVENTIVE MEASURES

(1) Change the default SSID

(2) Hide SSID and MAC filtering

(3) Add a firewall

(4) Consider 802.1x wireless protocol

5. STRENGTHS AND WEAKNESSES ANALYSIS

This report considers a potential risk to the KNX protocol and BACnet controller in this university sensor network. The advantages of an attack on it are: it is easy to cause moderate damage, device damage, and tampering with data. However, these attacks are not as simple and common as DDoS attacks. It can be easily avoided by only allowing communication between the KNX IP network and other networks via a suitable firewall.

Report2

The purpose of this report is to identify and analyze some of the Web-application security threats to web servers and to suggest preventive measures. To analyze the potential risks. I use the following methods: (1) System characteristics (2) Identifying potential hazards (3) Testing potential vulnerabilities (4) Outlining preventive measures (5) Strengths and weaknesses analysis.

1. CHARACTERISTICS OF THE SYSTEM

A university has deployed a web server that is deployed as a virtual machine in Azure, which is managed by the university. Only computers within the university's local network are allowed to access this server. The server is based on Ubuntu with an Apache2 server and runs a Mysql database managed by PHP scripts.

2. POTENTIAL THREATS

Analysis of this webserver shows that it can be attacked through vulnerabilities in Ubuntu, infiltrated through vulnerabilities in Apache2, or through PHP scripting vulnerabilities to modify data in MySQL. I have chosen to analyze only the PHP vulnerabilities.

For scripting, PHP sets up Session and Cookies to facilitate user input of accounts and passwords. PHP treats input data as global variables to be processed. Therefore, hackers can obtain the user's SessionID through various attacks, and then use the attacked user's identity to log in, to use the user's rights to tamper with or destroy the data.

3. TESTING POTENTIAL VULNERABILITIES

(1) The target user first successfully logs into the site, at which point the user is given the sessionID provided by the site.

(2) Using brute force, prediction, network sniffing, or XSS attacks to obtain the SessionID.

(3) If (2) is successful, then the legitimate session of the target user can be obtained and the sensor data can be tampered with or corrupted. (In 2014, A company came under attack. Random people requested and successfully cashed remittances of $3,000-30,000 each in the company's local and foreign departments., Helen Martin).

4. PREVENTIVE MEASURES

(1) Change the session name

(2) Set HttpOnly

(3) Turn off transparent SessionID

(4) Close all phpinfo dump request information pages

5. STRENGTHS AND WEAKNESSES ANALYSIS

Session attacks are one of the common attacks used by hackers, with low attack costs and low technical requirements. However, due to the uncertainty of brute force cracking and other methods lead to the process of obtaining SessionID is still unstable. At the same time, with the upgrade of the PHP version, these vulnerabilities have been gradually reduced.