Vulnerabilities Analysis and Solution of VxWorks

Zhigang Zhang [1,2,a], Zhuo Lv [1,b], Jiansong Mo [1,2,c], Shuangxia Niu[1,d]

[1]HAEPC ELECTRIC POWER RESEARCH INSTITUTE,CHINA

[2]Henan EPRI GAOKE Group Co. Ltd, Zhengzhou, China

[a]15838150770@126.com, [b]zhuanzhuan2325@sina.com.cn, [c]jiansong_mo@yahoo.com.cn, [d]sxniu_wang@163.com

***Abstract*—The paper provides a brief introduction about VxWorks, analyzestheimportanceofOSsecurity, discusses the current revealed vulnerabilities, describes the risks、the attack paths、and the affected systems about them, and gives the solutions on this foundation.**

Keywords- VxWorks; vulnerability; solution

I. BACKGROUND

A. Summarize on VxWorks

With the rapidly development of the computer, Internet and EPC system network，the computer devices becomes more and more popular, users can access and control the information at any time. The Embedded system is a special computer system, centered on the application and based on the computer technology. It hasthe flexible interface insoftware and hardware, also thedemandingrequirementson function, reliability, cost, size,andpower consumption.In the application of embedded system, the computers are combined with other devices other to achieve the real-time monitoring and control operations of the other equipment status, which can greatly improve the production efficiency. Compared with the conventional computer system, the embedded system has limited resources and relatively simple task. In addition, there is a certain time limit and accuracy requirements, ensuring the need of the proper implementation in the stipulated time in most embedded systems applications. In such conditions,the operating system is often referred as embedded real-time operating system (RTOS).

VxWorks, an embedded operating system, with the good real-time performance, the flexible developed interface and the user-friendly develop environment, is widely used in the high sophisticated technology and real-time required fields like communication、military、aviation and space flight and so on. Vxworks has the multi-task mechanism using the preemptive priority scheduling and the round-robin scheduling，providing the reliable real-time performance and relatively flexible user-developed ability. In the high-end fields of hard real-time embedded applications, the VxWorks of American Wind River is absolutely dominated. VxWorks is used in the United States the F-16, FA-18 fighter, the B-2 stealth bombers and the Patriot missiles, even in the detector landing on the surface of Mars in April 1997[1].

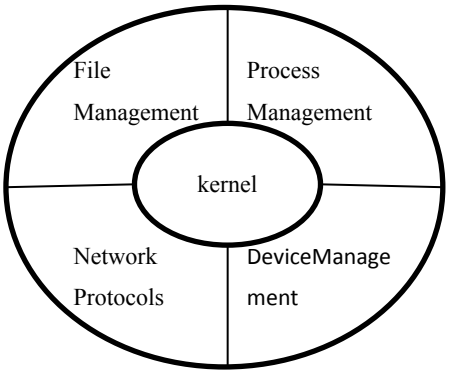

Figure1.1VxWorksarchitecture

VxWorks is a powerful and complex operating system, the kernel includes a few parts of process management, device management, file management, network protocols, applicationsand so on. Occupyingverylittle storage space and highly flexible interface, VxWorks can ensure the higher efficiency ofsystem. VxWorks real-time operating system is composed of nearly 500 independent, short and refined target modules, the users can select the appropriate modules to configure the system as needed. In 1984 Wind River launched its first version - VxWorks 1.0.1, introduced a new version of VxWorks 5.4 in 1999. From 1995, Wind River introduced a real-time operating system development environment-Tornado. In 2009, Wind River introduced significantly enhancedVxWorks6.7, allowing device manufacturers the ability to make full advantage of the latest multi-core processors to solve key question in their businesses[2].

B. VxWorks OS security

VxWorks has a standard development suite called as Wind River Workbench which is a JAVA Eclipse platform. This Integrated Development Environment (IDE) is used as development suite for code compiling, analysis, editing, and debugging. First, VxWorks can be optimized to run as a closed system having a protection between processes running in kernel and user mode with effective error management. Second, VxWorks OS can be optimized to run as a networking platform having similar functionalities of a network OS such as firewalls and security protocols. Third, VxWorks can be implemented as a safety critical system or hard real-time system that meets the highest levels of safety and security requirements..

Vxworks（the core can be smallest up to 8KB）has excellent portability，which can be used in the systems without MMU (Memory Management Unit)[3]. In VxWorks,anew concept is introduced which is called protection domains.The function of protection domains is

to separate software components from others. The protection domain inherits individual MMU and private address spaces. The function of MMU is checkingthe addresses of the process in protection domains. For design engineers, VxWorks is very flexible. They can define execution boundaries during the runtime to specify the usage of different objects in the software components. This states are simple enough for the developerswhich is equipped enough to create OEP (Object Entry Point) in the kernel domain according to the requirements. In general, this design is not robust from the security point of view[4].

Because of the base software that supports different applications, OS security is very critical. In the operating systems, the running applications can be dramatic impacted by vulnerabilities. If the OS level vulnerabilitiescompromisea system, by such as in kernel level, the system can be completely taken over by an attacker, installing malicious programs or backdoors. Then OS can be used for nefarious purposes such as stealing sensitive data from the machines and executing remote commands. Attacker can also exploit the system access rights and cause the applications to execute maliciously. A trend of embedded system is a combination of embedded devices and networks, Once therearesomeproblemsin embedded system security, the consequences will not only interfere with people's daily lives seriously, infringeof citizens' privacy, but also cause huge economic losses, even a threat to national security.

But like other RTOS, Vxworks has many vulnerabilities, leading to random restart、dead halt or changing the random city. Thus, analysis of OS security vulnerabilitycan providea better insight about the robustness of the operating system. It can also help us to understand the serious repercussions of persistent vulnerabilities.

II. VXWORKSVULNERABILITY ANALYSIS AND SOLUTIONS

Vulnerabilities of VxWorkscan be divided into four categories, named input validation vulnerabilities, permissions and access control vulnerabilities, trust management vulnerabilities, encryption vulnerabilities.

A. Input validation vulnerabilities

The function of input Validation is to test the correct of any input which is supplied by something else.Users' input is always needed for applications to achieve some purpose. The source of users' input isvarious, an end-user, an application, a malicious user, or any number of other sources. The attackerwill not announce that he/she is an attackerwhen he/sheis ready to attack your software. That meansall input should be checked and validated, because you can notknow exactly the source of the input. All the applications and software should check the input entered by others to ensure if it's trusted, but this is not the only time that input should be checked. Although an end user is very unlikely to input specific SOAP requests to a web service, a malicious user could. Maybe you are getting input from a database. Where did that input come from? Was it your application, was it another application, is it some shared database table that another application is storing data in that you would never expect?

We shouldtest all of the input in order to protect against a future potiential security hole and vulnerability in the software application.Problems resulting from incorrect input validation could lead to all sorts of problems and vulnerabilities. Here is a listing of some of vulnerabilities that could be solved just by validating input.

1) SSH server denial of service vulnerability 1

Description: In Wind River VxWorks 6.5 through 6.9 IPSSH (SSH server) has vulnerabilities of input validation. IPSSH (SSH service) is reliable,speciallyin providing security protocol for remote login sessionand other network services.SSH protocol can effectively prevent information leakage problem in remote management process.The vulnerability could make SSH server denial of service.

Thevulnerabilities' major hazards affect in four areas:

a) Remote attackers can use the vulnerability to cause a denial of service (daemon outage) via a crafted authentication request.

b) Remote authenticated users canuse the vulnerabilityto cause a denial of service (daemon outage) via a crafted packet.

c) Remote authenticated users canuse the vulnerabilitytocause a denial of service (daemon outage) via a crafted pty request.

d)Remote attackers canuse the vulnerabilitytoexecute arbitrary code or cause a denial of service (daemon hang) via a crafted public-key authentication request.

Solution: The developers have released a related patch for the vulnerabilities, you can download the patch to solve these vulnerabilities.

2) WebCLIcomponent denial of service vulnerability

Description: WebCLI component in Wind River VxWorks 6.5 through 6.9 has Input validation vulnerabilities. The vulnerabilities can make WebCLI component denial of service.

Thevulnerabilities' major hazards: The vulnerabilities allow remote authenticated users to cause a denial of service (CLI session crash) via a crafted command string.

Solution: The developers have released a related patch for the vulnerabilities, you can download the patch to solve these vulnerabilities.

3) Web Server remotedenial of service vulnerability

Description: The web server in Wind River VxWorks 5.5 through 6.9 has Input validation vulnerabilities. The vulnerabilities can make the web server denial of service.

Thevulnerabilities' major hazards:Remote attackers can cause a denial of service (daemon crash) via a crafted URI.

Solution: The developers have released a related patch for the vulnerabilities, you can download the patch to solve these vulnerabilities.

B. Permissions and access control vulnerabilities

Permissions and access control is a security process that controls usage of specific resources within the predefined criteria and is a part of the AAA (Authorization, Authentication, Accounting) security model. All modern systems use certain permissions and access control models to manage their security. Permissions and access control models can be grouped in three main classes: Mandatory Permissions and access control (MAC), Discretionary

Permissions and access control (DAC), and Role Based Permissions and access control (RBAC)

Permissions and access control involves the use of several protection mechanisms such as authentication (proving the identity of an actor) authorization (ensuring that a given actor can access a resource), and accountability (tracking of activities that were performed). When any mechanism is not applied or otherwise fails, attackers can compromise the security of the software by gaining privileges, reading sensitive information, executing commands, evading detection, etc.

1) WDB target agent debug services permissions and access control vulnerabilities

Description: In Wind River VxWorks 6.x, 5.x, the WDB target agent debug service which is used on the Rockwell Automation 1756-ENBT series A with firmware 3.2.6 and 3.6.1 and other products has vulnerabilities of permissions and access control.So as tosupport embedded software development, the VxWorksdevelopersconfigure a target agent components. In order to comply with WDB (Wind River DeBug) protocol, the target agent which allows remote users to debug the programs inthe target machine[5].a remote attacker can use the vulnerability to exploitthe storage unit, functions, administrative tasks.

Thevulnerabilities' major hazards: The vulnerabilities allow remote attackers to read or modify arbitrary memory locations, perform function calls, or manage tasks via requests to UDP port 17185.

Solution: The WEB target agent, debugging components(INCLUDE_WDB and INCLUDE_DEBUG) and other operating system components which do not support the client applications can be removed.

2) FTPdaemon permissions and access control vulnerabilities

Description: The FTP daemon in Wind River VxWorks has vulnerabilities of permissions and access control.

Thevulnerabilities' major hazards: After a number of failed login attempts, the TCP connection can not be closed by the FTP daemon, which makes it easier for remote attackers to obtain access via a brute-force attack.

Solution: You can disable the FTP service if it's not required.

C. Trust management vulnerabilities

The concept of trust management has been introduced by Blaze[1] to aid the automated verification of actions against security policies. In this concept, actions are allowed if they demonstrate sufficient credentials, irrespective of their actual identity, separating symbolic representation of trust from the actual person.

Trust management is an abstract system that processes symbolic representations of social trust, usually to aid automated decision-making process. Such representations, e.g. in a form of cryptographic credentials, can link the abstract system of trust management with results of trust assessment. Trust management is popular in implementing information security, specifically access control policies.

Trust management can be best illustrated through the everyday experience of tickets. One can buy a ticket that entitles him e.g. to enter the stadium. The ticket acts as a symbol of trust, stating that the bearer of the ticket has paid for his seat and is entitled to enter. However, once bought, the ticket can be transferred to someone else, thus transferring such trust in a symbolic way. At the gate, only the ticket will be checked, not the identity of a bearer.

1) 2.3.1 INCLUDE_SECURITYfunction trust management

Description: The INCLUDE_SECURITY functionality in Wind River VxWorks 6.x, 5.x, and earlier has Trust management vulnerabilities.

Thevulnerabilities' major hazards: The INCLUDE_SECURITY functionality uses the Login_USER_NAME and Login_USER_PASSWORD (aka Login_PASSWORD) parameters to create hardcoded credentials, which makes it easier for remote attackers to obtain access via three ways:

a) Telnet protocol: Telnet protocol is one of TCP / IP protocols, which is the main way of Internet standard protocols and remote access services. It provides users with the ability to complete the work of the remote host on the local computers. . Users can use the Telnet program on the end user's computer and use it to connect to the server. End users can enter commands in Telnet programs and the commands will run on the server, as same as input directly on the server console so that you can be able to control the server locally. Telnet is a common method ofremote web server control[6].

b) rlogin(Remotelogin): Remotelogin (rlogin)allows the authorized users access the other machines on the network as same as the user uses the machine locally.Once access the host, the user can operate anything allowed by the host, such as: reading the file, editing the file, or deleteing files.

c) FTP session.

Solution:Avoid the hardcoding of account credentials and set the 'LOGIN_USER_NAME' and 'LOGIN_USER_PASSWORD' parameters to empty strings.

D. Encryption vulnerabilities

If you lock your door with a deadbolt instead of a chain, you make it more difficult for a burglar to get inside your home. Similarly, there are differences in the level of security that encryption software provides. Most of the well-known encryption algorithms that are considered "good" are mathematically complex enough to be difficult to break; otherwise, they wouldn't be so widely used. But even good algorithms are vulnerable to being broken if someone is persistent enough. In this section, we discuss the general vulnerabilities in encryption software, and offer tips that you can use to combat them. If you'd like more information on the vulnerabilities of a particular algorithm or software program, search the Web for reviews on its effectiveness.

1) Wind River VxWorks loginDefaultEncrypt algorithm encryption vulnerabilities

Description: The algorithm "loginDefaultEncrypt"in loginLib in Wind River VxWorks before 6.9 has algorithm encryption vulnerabilities.

Thevulnerabilities' major hazards: The loginDefaultEncrypt algorithm in loginLibcan not support a large set of distinct possible passwordsproperly.Remote attackers can easily use itto obtain access via three ways below:

(1)Telnet protocol.

(2)rlogin(Remotelogin).

(3)FTP session.

Solution:Use trusted verification API to instead of the standard API (loginDefaultEncrypt ()) default HASH algorithm by installing loginEncryptInstall () loginLib hook.

III. CONCLUSION

The paper mainly introduces the VxWorks operating system, explains the significance of the OS security vulnerability, analyzesthe 4 kind of security vulnerability: Input validation、Permissions and access control、Trust management、Encryption，and gives their solutions. It provides the useful foundation for maintenance and development of the operating system.

REFERENCES

[1]Chen Xing, Hu Xiao, Zhang Jianjun. Focus on International Information Security Standard Development Trend Report on the Working Group Meeting of ISO/IEC JTC1/SC27[J]. Information Technology standardization, 2006, (07);

[2]New Edition Introduction to VxWorks Real-time Operating System [J],Microcontrollers Embedded Systems,2009(4):69;

[3]Sun Luyi, The Comparison & Research of Four Popular RTOS—VxWorks, QNX, linux, RTEMS[J]. Computer Applications and Software,2007(24): 196-197;

[4]Tian Li, Yuan Jiabin, Research on Security Mechanism of Embedded RTOS VxWorks[J], Microcontrollers Embedded Systems,2009(4):69;

[2]Wang JInhun. Theory and Realization of VxWorks OS[J]. Radio Engineering, 2007(01):62-64;

[6]Zhu Kai, Xie Min. On The Embedded Real-time System[A].Proceeding of the 2004 Guangxi Computer Conference[C].Guangxi Computer Federation, 2004:4;

[7]Wind River Systems, High-Availability Compact PCI Systems: Introduction to Foundation HA, COTS Journal, September 2003:47-53.