Global Journal of Researches in Engineering: J
General Engineering
Volume 15 Issue 3 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 Print ISSN:0975-5861

Security in Untrusted Updated Environments

By Jahnavi Terva, Jaya Krishna K & K. Kondaiah
K L University, India

Abstract- At present days, technology growth was rapid and its use is very often. So the attacks were concentrated on the user systems mainly by using the network applications. Bugs in the application of a network can ruin the applications in a system that are running. When the user is in the use of internet or e-commerce sites, etc.., the applications will be considered that they are in an unsafe environment. Providing security to the network applications like web servers, mails, etc... Is very difficult because they are usually very big applications to make them free from bugs.

Now this paper describes how to provide security to the network applications which are in unsafe environment. This idea describes that all the applications were wrapped together for the security purpose and there will be no use to rewrite the network applications.

Keywords: internet security, network applications, secure environment [2], sandbox technique.

GJRE-J Classification : FOR Code: 090799

Strictly as per the compliance and regulations of :

Security in Untrusted Updated Environments

Jahnavi Terva [α], Jaya Krishna [σ] K & K. Kondaiah [ρ]

Abstract- At present days, technology growth was rapid and its use is very often. So the attacks were concentrated on the user systems mainly by using the network applications. Bugs in the application of a network can ruin the applications in a system that are running. When the user is in the use of internet or e-commerce sites, etc.., the applications will be considered that they are in an unsafe environment. Providing security to the network applications like web servers, mails, etc... Is very difficult because they are usually very big applications to make them free from bugs.

Now this paper describes how to provide security to the network applications which are in unsafe environment. This idea describes that all the applications were wrapped together for the security purpose and there will be no use to rewrite the network applications.

Keywords: internet security, network applications, secure environment [2], sandbox technique.

I. Introduction

Because of the easy access of the Internet throughout the globe, many various applications can be runned on the hardware platforms, which gives any opportunities in the commercial field. Developing an application is also an issue for providing the security from the internal attacks of users system. With a correct Securitas guard, the attacks can be detected. Different security solutions should be provided to the different attacks from the network. Many applications which are developed cannot provide a guarantee that can give total security. To develop a bug free application is very complex for the network applications which can result in a security issue.

In this paper, CMW which mean Common Mode Workstation Operating system with a B1-level grade is used to secure the applications from the unsafe helper environments. In this rewriting will not be done for an existing application as the applications will be wrapped and can be upgraded safely and securely.

II. Background

There are many protocols for the network security like SHTTP, SHHP, TLS, BITCOIN Protocol, etc… to give some protection where the communication is done at the two Ends of a receiver and sender. Unwanted connections can be kept out by using the Firewall [3]. If the bugs which are hidden in the server side is connected with the data of a user that may lead to the leakage of data from user system. Because of the bugs that are present in the network applications, either internal attacks can be done to sensitive data or leakage of data will be done. Providing security to a network application is almost impossible. While providing security, rewriting of the application will be done which also leads to a security issue. Mainly while providing security to the social networking sites is a complex issue.

While opening these networking sites the data transfer should not be done from receiver to the sender. All the applications should be developed keeping the security issue in the mind.

III. Existing Techniques

The traditional technique used is called sandboxing which can prevent the vulnerable applications running in a confined environment. Protecting the data from hackers and unwanted network applications from the break ins. There are many possibilities to the hacker to develop many privileged applications to break the security policies. Let us consider an example TIS96 which depends on the physically distinguish hardware which gives us information separation. Another example GWT96 which depends on operating systems. There is a user and security check at the user level. There is still the possibilities that the hacker can make use of compromised privileged applications to alter the security policies and further his attacks.

IV. Our Approach for Security

HP-UX[1] CMW can be used to combine all the untrusted network applications. In this approach we are going to design an Operating systems [5] that facilitates a group of fine grained administrative security assigns and operations to handle these assigns. Security checks should be done at each level to the Operating System in which process are running simultaneously so that it can guarantee maximum protection. Because of these features, it will be able to distinguish the network application format from security format, to provide a general platform for combining the existing untrusted dumb applications for security. For explaining how to use CMW in sandbox for untrusted applications, for serving as case studies we took two typical examples. One of those examples is the HP's Presidium Virtual Vault, which prevents the unauthorized access unauthorized modification of the data in the server by wrapping the Web server. Other example is Trusted Send mail Proxy which was developed in HP Labs[4],

Author α σ ρ: Dept. of Electronics and Computer Engineering, K L University, Guntur. e-mails: jahnaviterva@gmail.com, smile.jayakrishna@gmail.com, kondaya.kuppala@kluniversity.in

Bristol and this prevents highly privileged but vulnerable send mail that are running on the system without causing any fatal damages to the users system.

The objective of the work is to provide the network application services safely by combining untrusted applications and to have a view on the advantages of introducing CMW to solve the security issues in the commercial field.

V. Flow Chart for the Approach

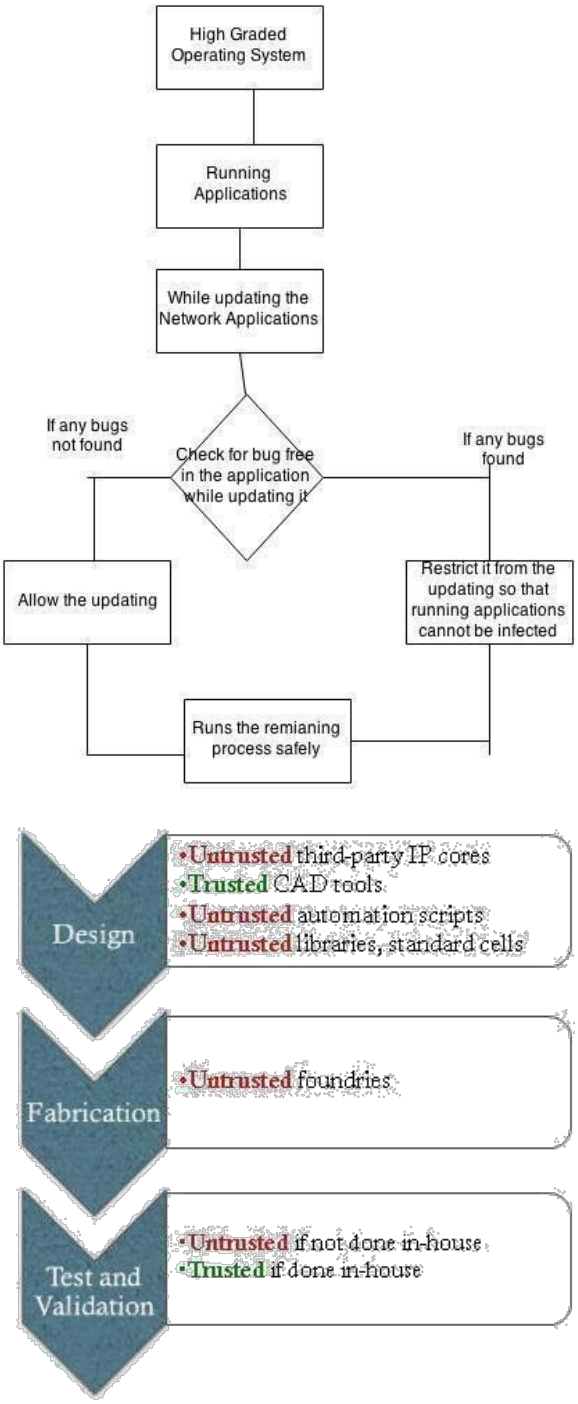

Fig. 1 : Example of tokens to be generated for security purpose to the network application

VI. Working of the Idea to Provide Security to Application

a) Finding an restricted process

The parent and child privileges are given to the applications which are to be updated so that safe transfer of the information can be done. Let us consider an example in which a child process cannot get access to the privileges of a parent process by inheriting, it can be restricted as inheritance is an automatic process. If it can get access from the parent process it can be given an token that it is an trusted application. So by this way we can find which process is to be restricted and which process is to be continued with security. If the child process which cannot gain access is allowed to continue further it leads to a serious issue for the internal attacks of the users system.

b) How CMWis used to combine the Untrusted Applications

As our objective is to prevent an third party gaining the access of user's system and to protect oneself from the untrusted vulnerable network applications. We use two typical network applications to wrap the application data i.e. by using the web server and send mail illustrating what is done to apply the methods to give security. A trusted mail is sent at the ending by illustrating what is done in the process.

VII. Security Analysis of the Network Application

Even if the data is broken by the bugs then the damage will be confined to only the compartment which is considered as system inside. It doesn't harm much because the data in the system inside of the operating systems cannot get access to the connections of the data which is provided from outside network.

VIII. Conclusion and Future Work

An operating system with highly grained administrative security management helps to meet many security policies while using the network applications and can protect us from an intruder accessing the gain root access of the data in a system of user. Security dumb applications can be easily found and can be issued an unsafe token to prevent access and is restricted. Depending on the various commercial applications security infrastructures should be modified according to that and should have possibility to extend the CMW for the application platform of that network.

References Références Referencias

1. Hewlett-Packard, "HP-UX Compartmented Mode Workstation key security concepts", 1996.
2. Ian Goldberg, David Wagner, Randi. Thomas and Eric A. Brewer, "A secure Environment for Untrusted Helper Applications --- Confining the Wily Hacker".

3. W.R. Cheswick, S. M. Bellovin, “Firewalls and Internet Security - Repellimg the Wily Hacker”, Addison-Wesley, 1994.
4. Andrew Berman, Virgil Bourassa, and Erik Selberg. TRON: Process-speci_c _le protection for the UNIX operating system. In Proc. 1995USENIX Winter Technical Conference, pages 165{175. USENIX Assoc 1995.}
5. Robert Wahbe, Steven Lucco, Thomas E. Anderson, and Susan L. Graham. Efficient software-based fault isolation. In Proc. of the Symp. On Operating System Principles, 1993.