

Semi-network OS and New Mode of Application Software Sharing

Yin Sheng Zhang

PhD Candidate of Electrical and Computer Engineering,
University of British Columbia, Vancouver Canada

Correspondence:

807-8171 Saba Rd Richmond B.C V6Y 4B3 Canada

E-mail: cxo888@hotmail.com

walterz862@hotmail.com

Abstract- Once semi-network operating system architecture becomes a reality in near future, the deployment of application software will be transformed into a unified and oriented network sharing mode, and this new network sharing mode contains four core contents: 1. OSPU (operating system processing unit) becomes the orientation guide and command center for download or upload of application software, and the application software cannot determine the download destination then it cannot be downloaded from server to local platform without OSPU; 2. There is a special and unified database on server side for application software without having to set up a local database; 3. There is no permanent installation site and database for application software on local platform and application software can only run temporarily on local platform; 4. Application software uses its own security code together with OSPU's hardware identity code to receive system and network verification in software download or upload process, both codes are indispensable.

Keywords- *Application software sharing; semi-network operating system; OSPU regulatory mode; sharing process of device driver.*

I. INTRODUCTION

Once semi-network operating system architecture becomes a reality in near future, the deployment of application software will be transformed into a unified and oriented network sharing mode, and this new network sharing mode contains four core contents: 1. OSPU (operating system processing unit) becomes the orientation guide and command center for download or upload of application software, and the application software cannot determine the download destination then it cannot be downloaded from server to local platform without OSPU; 2. There is a special and unified database on server side for application software without having to set up a local database; 3. There is no permanent installation site and database for application software on local platform and application software can only run temporarily on local platform; 4. Application software uses its own security code together with OSPU's hardware identity code to receive system and network verification in software

download or upload process, both codes are indispensable.

A. The problem faced by old mode.

In the past, people mainly rely on material and energy to survive, but now information technology gradually penetrates into every corner of society and occupies a decisive position, information has become another major resource in people's lives.

The semi-network OS architecture is a new exploration of information technology that will also inevitably generate series of configuration innovations, such as the changes of system software architecture, hardware structure of client device, and application software deployment mode, all these changes are mutually interdependent.

The reason that computing devices and network technologies can penetrate into every corner of people's lives and work is mainly due to the development of system and application software, however, some inherent defects in old software deployment mode also have greatly affected the security and functioning of computing devices and their network activities, such as:

a) The over-stacking of normal application software: for example, much application software is often only used for temporary needs, but always occupies the resources of device. In addition, the old architecture of localized operating system has to repeatedly increase or update application software to maintain interaction with network, accumulating over time, which also forms the over-stacking of normal application software on local platform.

b) The stacking of malware: malware is also in the scope of application software, and there is even no absolute standard for identifying "good" and "malignant" application software, as long as local platform allows application software to be freely installed, then it is impossible to exclude free installation and stacking of malware.

c) The stacking of junk software: many discarded application software that are not timely or periodically cleared from client device, and various junk software that automatically downloaded from network, will remain on local platform permanently, and their stacking speed often exceeds the speed of normal application software installation.

Such a phenomenon stems from the inherent defects of old architecture of computing devices and operating

systems, as a result, solution for removing these inherent defects cannot be obtained under old architecture.

Now, the semi-network operating system architecture requires application software to be stored on server and downloaded to local platform to run as needed, which will of course bring about an opportunity to thorough rebuild of old application software deployment mode.

B. The key of solution.

Compared with the existing architecture of operating system on local platform, the most obvious feature of semi-network operating system architecture is its flexibility, which is mainly determined by expanded portion of semi-network OS (server-OS).

a) Flexible file package.

Semi-network OS on local platform is not a file package with stable and unchanging content but is adjustable (refers to the expanded portion of semi-network OS) according to operation needs, which should also benefit application software to be flexibly downloaded and temporarily run on local platform as a network shared resource.

b) Flexible platform.

Semi-network OS will not establish bundled relationship with a specific local platform, and it follows OSPU to move and run on different types of local platform, which should also benefit application software as a network shared resource to run on different local platform following OSPU.

c) Flexible network connection.

Semi-network OS not only operating under network condition, but also operating under non-network condition, which provides basic function for computing device to ensure basic operation, which should also benefit some basic application software (such as device drivers) to be permanently stored in OSPU after downloading and will no longer be constrained by network connectivity.

II. SEMI-NETWORK OPERATING SYSTEM ARCHITECTURE

A. The architecture.

The semi-network operating system architecture consists of two portions of system files, that are expanded portion and base portions, the system files of expanded portions are from database of network server, and the system files of base portions are permanently stored in a mobile chip component of local platform, so, its architecture comprises the following main component:

a) Base portion of semi-network OS, which is installed in OSPU (operating system processing unit) of local platform, so it is also referred to OSPU-OS.

b) OSPU, which is a component of client device.

OSPU is the abbreviation of "operating system processing unit", which guide the expanded portion of semi-network OS (server-OS) downloading and act as the storage place of the base portion of semi-network OS (OSPU-OS), and OSPU will support system files of two portions of semi-network OS to be combined together and operating together in Random Access Memory of local platform.

OSPU configure optional activating process, which allows users to set up their own user name and password for OSPU, then OSPU with user name and password to startup OSPU function of system file download, but the record of user name and password is saved on server, and its verification process is completed on server. Because this process is optional, so users can choose to give up.

OSPU is not only for processing semi-network OS, but also for integrating the feature of network connection, integrating the system files of base portion of semi-network OS (OSPU-OS), integrating the programs of anti-virus, anti-hack, anti-phishing, etc.

c) Expanded portion of semi-network OS, which is downloaded from OS server to local platform, so it is also referred to server-OS.

OSPU is the core hardware component on local platform that not only acts as channel of exchanging data between network server and local platform, but also protects security of data transmission in network, more importantly, OSPU is a settle place of OSPU-OS and a regulatory center of entire semi-network OS, so it can be said that without the OSPU there will be no semi-network OS.

OSPU-OS and server-OS will be working together to form a complete semi-network operating system on local platform, and which will be the only functioning operating system in computing device.

Semi-network OS needs to be run on the basis of some innovative components, which includes software and hardware:

B. Dedicated startup process.

Semi-network OS replace current graphical interface OS in computing device, which is bound to change the startup steps of computing device.

In detail, step 1, computing device startup OSPU on local platform, and through OSPU network connector to connect network server; step 2, system files of expanded portion of semi-network OS (server-OS) are downloaded by OSPU from database of network server to local Random Access Memory and it will be downloaded in accordance with actual operation demand of local platform.

Here, server IP has been permanently embedded in OSPU chipset, so OSPU can only connect specified network server, and from there to get system files of server-OS and related application data.

The startup process of semi-network OS is divided into three cases:

a) There is only one OSPU on local platform, and there is no other graphical interface OS on local platform.

In this case, OSPU will first deploy base hardware supporting files of semi-network OS to Random Access Memory of local platform, then OSPU actively connect network server to request for downloading system files of server-OS to Random Access Memory of local platform.

b) Local platform is already installed other graphical interface OS in hard drive, but user want to use OSPU.

In this case, after computing device is turned on, system will prompt user to select from which system carried component to start up, if user selects OSPU, OSPU will first deploy local hardware supporting files of semi-network OS to local Random Access Memory, then OSPU actively connect network server to request for downloading system files of server-OS to Random Access Memory of local platform.

In addition, once user selects OSPU, the original permanent graphical interface OS of local platform will no longer work, because it lost hardware and system support.

After OSPU (external plug-in component) is removed, computing device will be restored to original operating system based on old hard drive.

c) There is multiple OSPUs to be used on one local platform and no other graphical interface OS on local platform.

In this case, system will prompt user to select from which OSPU to start up, and start-up menu will present all the OSPU serial number, so user is easy to make choice.

III. NEW MODE OF APPLICATION SOFTWARE SHARING

One of the characteristics of old mode is that designated application software should be permanently installed on designated local platform.

In concept of architecture of semi-network operating system, most of the system files (expanded portion) of operating system of client device will be stored on network server as shared resources, and then downloaded directly from database of network server to RAM of client device, but which not being permanently stored in client device, besides, some other system files of operating system of client device will act as the base files (base portion) to be installed in a removable component OSPU (operating system processing unit) in an enclosed state, and third party software is strictly forbidden to be installed freely to OSPU, wherein the OSPU is an abbreviation of operating system processing unit, which is the core and dedicated hardware component in the semi-network operating system architecture, and on its chip will be embedded with a variety of application software to implement network connection, data encryption and decryption and so on.

Since the architecture design of semi-network operating system is going to subvert old system architecture, the application software deployment mode that based on old system architecture will be also forced to be completely rebuilt.

A. In the architecture of a semi-network OS, the hard disk of local platform will not serve as a right place for application software free installation, so the application software have to find some other resting-place to permanently settle down, and in architecture of semi-network operating system, the permanent resting-place of application software is the database of network server.

In this case, the ordinary application software can only be downloaded from database of network server to RAM of client computing device to operate and to be temporarily stored in this component until shut down of said computing device, but there are exceptions, the device drivers (a special type of application software) will be permanently stored in OSPU after they are downloaded from database of network server, which are not affected by power disruption.

B. Sharing process of ordinary application software is carried out together by network server and OSPU, both of server and OSPU will check, guide and control the whole process, so as to change the "unilateral process" model that specifically designed for client device, or for network server in existing and old architecture, and which require the computing devices that at both ends of network to work together in the whole process from an application software is uploaded, authenticated, entered the database of network server, downloaded from database of network server, and to be normally and safely operating on client computing device.

OSPU plays a crucial role in this sharing process of application software, so the sharing process can also be viewed as "OSPU regulatory process", and the role of OSPU in this regard can be briefly summarized in following:

a) In the common sharing process of ordinary application software, the storage platform of a dedicated application software is on network server, but its operating place is on local platform, in this case, server selectively provide application software for local platform, and local platform according to the actual need to selectively download and operate application, such a mechanism is mainly executed and regulated by OSPU.

OSPU go through inspection of anti-virus, anti-hacker, anti-phishing before application software are uploaded to network server, and OSPU will identify the security code of application software when after application software is downloaded to local platform, wherein the security code of application software is granted by network server.

b) In the sharing process of device driver, the device driver of local platform is downloaded from database of network server via OSPU, then to be permanently stored in OSPU chipset.

IV. ORDINARY APPLICATION SOFTWARE

A. Network sharing and security process.

Under existing technology, ordinary application software is usually installed on external storage device of local platform together with operating system, and a large number of application files are directly integrated in system software.

The development of computing device functions depends on development of application software, therefore, popular operating systems always adopt open attitude to installation of application software on local platform.

It brings trouble that virus and hacker also belong application software, to open installation platform, which is equal to open door to virus and hacker.

In addition, a large number of ordinary application software are integrated into operating system, resulting in the system files to be increasingly complex and expanding, which form a large number of depletion of resources of local platform, and become a reason of system running slow down.

In network terminal or cloud technology, user data is centralized processed and generated on server, therefore, application software is bound to be installed on server, which resulting an new problem that for anti-virus and anti-hacker, server usually take stringent measures to prohibit foreign application software to be uploaded, or allow only a limited number of protocol software of developer's application software to be uploaded, and it makes the overall functionality of computing device to be falling instead of rising.

Because there is no effective application software sharing process, the network terminal and cloud technology also have to face with the major obstacles for promoting in wider range.

Academia has been some ideas related to the issues of specified security code of application software, but most of those ideas are based on the case of that "application software is installed and operated on local platform", and focused on design of anti-hazard measure of local platform.

However, faced with software free installation mode of local platform, the ideas of application software security code is destined to be rarely effective, in fact, so far there has been no widespread acceptance and great popularity in reality, that is because the effect of application software security code is not only depend on software design, but also depends on the feature of computing device, depends on functional characteristics of external storage device.

Therefore one of creativity of "new mode of application software sharing" under the architecture of semi-network operating system is that it combines application software security code and network anti-hazard process into one, and combine anti-hazard, convenience and efficiency of application software into one.

Of which:

a) The ordinary application software security code no longer takes local platform as foothold, because its foothold will be moved to server. It no longer takes anti-hazard of local platform as focus, because application software will only temporarily runs on local platform, and its security code will focus more on preventing virus and hack program to threat server.

b) The security code combines network anti-hazard process to prevent virus and hacker that fake name of ordinary software of client computing device to invade server.

c) The ordinary application software storage platform and operating platform are divided in two different locations, so as to reduce the opportunity for virus to

launch attack, or increase difficulty for virus to launch attack.

Ordinary application software is stored on server, and its safety is inspected by server, and its security code is specified by server, but application software do not run directly on server and it run on local platform.

The running place of ordinary application software is Random Access Memory of local platform, once computing device shut down, application data will automatically disappear, and therefore, this new mode of application software sharing will not only reduces accumulation of additional data in client computing device, but also will help to improve the safety of local platform and server.

B. Implementation.

Here should particularly explain that the security authorization code of application software in the architecture of semi-network operating system belongs to a link of whole process rather than an isolated authorization. In addition, that of definition of "ordinary application software to be installed in computing device that equipped with semi-network operating system" contains two meanings, namely: a). Ordinary application software to be put into network server's database; b) ordinary application software to be downloaded through OSPU to local platform, then temporarily run in the RAM of local platform.

The new mode of ordinary application software sharing is based on the architecture of semi-network operating system, and is added a key element: OSPU, therefore, it would inevitably lead to a chain reaction and produce a series of sub-processes, and these sub-processes get together to form a complete sharing process of application software.

a) The general process.

In this case, the ordinary application software must be downloaded from database of network server to local platform via OSPU because local platform is no longer permanently installed with any ordinary application software, then the local platform can only get the ordinary application software from server-side database; in addition, an search engine of "application software" will be set in user's personal network account, and those application software selected by user is stored in user's account, and their relevant files will be set on personal operator interface of user's account in the form of shortcut.

b) The user-supplied application software process.

In this case, user-supplied application software first has to accept the hazard inspection by OSPU, and then it will be uploaded to network server, or suspicious application software will be blocked to upload by OSPU.

c) The application software security process.

In this case, the network server will be divided and set a dedicated area for isolating application software and testing application software, and after safety of application software is confirmed, and it is confirmed that there are no duplicate of same application software in server database, network server will grant a security code to said application software, and transmit said application software into its database.

d) The application software security code confirmation process.

In this case, application software must be confirmed by OSPU on security code before temporarily running on local platform's Random Access Memory.

e) "Random Access Memory" only process on local platform.

In this case, ordinary application software are not storage in OSPU chipset, but even if network connection interrupted, as long as Random Access Memory continues to work, application software that downloaded in Random Access Memory will still continue to run.

V. SOFTWARE OF DEVICE DRIVER

A. Network sharing and security process.

The device driver as a special type of application software, its installation and operation process is no different from ordinary application software in old mode, however, in architecture of semi-network operating system, although the hard disk of local platform is no longer a free installation place for application software, so the device driver can only be forced to become a network shared resource for local platform to download, but unlike the ordinary application software, the device driver is allowed to be permanently stored in OSPU (operating system processing unit) after downloading without having to be downloaded repeatedly. In this case, the network sharing and security process of device driver includes the following features:

a) Users are not allowed to install device drivers on local platform (including OSPU) by themselves, the device drivers that required by local platform must be downloaded from database of network server.

b) Network server set up a device driver database, and device drivers that required by local platform must be downloaded from this database.

c) Device drivers are downloaded from database of network server to the OSPU of client computing device, and to be permanently stored in OSPU chipset, as long as said computing device is not replaced, or new hardware component is not used, these device drivers do not need repeatedly downloaded.

d) User-supplied device driver is to be uploaded to network server after hazard inspection of OSPU, then it will accept hazard inspection once again by network server, and then to be put into the database of network server, and then to be downloaded from database of network server to OSPU of client computing device for permanent storage.

e) The files of device driver that stored in OSPU are in closed state, they do not accept user modification, but it accepts update by network server.

f) After a new device driver is downloaded, the old device driver that stored in OSPU will be automatically removed from the stored data of OSPU.

B. Implementation.

In the old mode, every mainstream architecture of operating system have their own matching computing device models with their special device drivers installed permanently on local platform, so they do not require to design additional special sharing process for device driver.

However, switch to architecture of network-source operating systems, such as network terminal, there is no software of operating system to be permanently installed on local platform, and the host server does not provide extra device drivers to its terminal, so it is the reasons that why the terminal technology cannot be freely chosen by local platform, and why the server cannot cross specified platform to implement in a wider range.

If network- source operating system software wants itself to be successfully running on different models of computing device, it must first make the operating process of its device driver to be able to adapt to different models of computing device, and also this process must meet at least three conditions:

a) Server has device driver database that with rich resource, because device drivers of local platform can only be downloaded from server.

b) Local platform is equipped with an intelligent selection mechanism that can accurately select appropriate device drivers from server database.

c) Local platform is assigned a specific room for storing device drives that downloaded from server.

These conditions above just constitute the component of the sharing process of device driver in the architecture of semi-network operating system, and which also constitute the creativity of new mode of device driver sharing under architecture of semi-network operating system that this sharing process can make the architecture of semi-network operating system to be applied to a variety of type of computing device, and it can broaden application area of network-source operating system, make device drivers to be installed easily and to be running smoothly, and guarantee the security of device driver in client computing device.

In architecture of semi-network operating system, there is no hard drive in local platform for permanent installation of operating system software, then device driver can only be stored in OSPU chipset, and OSPU is a sealed package, and it rejects out-system or none-system data to be stored in it except those predetermined and pre-installed data.

In addition, user-supplied device driver must first be uploaded to server, then go through hazard inspection, and then enter network server database, and then to be downloaded to OSPU for storage, after first download, device drivers will be permanently stored in OSPU, as long as the model of computing device do not change, said device driver will no need to be repeated downloaded to OSPU, so as to speed up computing device startup.

REFERENCES

[1] Jianli Pan, Raj Jain, Subharthi Paul, and Chakchai So-In. Milsa: A new evolutionary architecture for scalability, mobility, and multihoming in the future internet. Selected Areas in Communications, IEEE Journal.

<https://www.cse.wustl.edu/~jain/papers/ftp/milsajsc.pdf>.

[2] Subharthi Paul, Raj Jain, Jianli Pan, and Mic Bowman. A vision of the next generation internet: A policy oriented perspective. In BCS Int. Acad. Conf. https://www.bcs.org/upload/pdf/ewic_vs08_s1paper1.pdf.

[3] Subharthi Paul, Jianli Pan, and Raj Jain. A future internet architecture based on deconflated identities. In Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. <https://www.cse.wustl.edu/~jain/papers/ftp/deconf.pdf>.