## Contact Information

Publications@ipcg.com

ipCapital Group, Inc.
400 Cornerstone Drive, Suite 325
Williston, VT 05495
United States of America
(802) 872-3200

## TITLE

Kernel Based User Authentication

## ABSTRACT

A Security Sector is included in the kernel of the operating system. The Security Sector prevents the execution of system commands unless the user can be authenticated by the Security Sector. Implementing the security system in the kernel prevents malicious parties from circumventing the security system.

## 1. BACKGROUND

### *Problem or Opportunity*

Security threats to computing machines exist in the opportunity to execute dangerous and destructive commands. These commands are necessary for operation of the machine but must be carefully regulated to avoid accidental or intentional misuse. Security restrictions implemented in the operating system such as administrator or "super-user" accounts still leave the opportunity for malicious users or code to directly access the kernel and execute dangerous commands. A more secure system is necessary to prevent the malicious execution of commands by circumventing existing security.

### *Background Publications*

Previous publications have attempted to address security issues from within the kernel. However, these publications do not address security concerns related to the execution of dangerous commands by users or applications on a computing machine.

US Patent Number 7398389 describes a "Kernel-based network security infrastructure." In this invention a code set within the kernel protects from malicious attempts to insert code into the rest of the kernel. This invention does not protect against the execution of dangerous system calls by unauthorized parties.

US Patent Number 7246233 describes "Policy-driven kernel-based security implementation." In this invention, network security is implemented in the kernel such that it provides transparency to applications. This invention does not relate to the security of system commands on a computing machine.

US Patent Application Number 20090089579 describes a system for validating software applications. In this invention a key checking module is implemented within the kernel that verifies the authenticity of software from a vendor. This invention does not relate to the security of system commands on a computing machine.

US Patent Application Number 20090007233 describes a system for securing information from a root user on a computing system. In this invention, sensitive data is protected from access by unauthorized root level users by adding an additional level of authentication to access the sensitive data. This invention does not provide additional security against the malicious use of root level commands.

Trusted Computing Platform Alliance (TCPA) chips, such as HP's ProtectTools Embedded Security[1] is another recent development in computing security. In these systems, a TCPA chip embedded in a system's hardware, manages security functions such as network authentication, data encryption, and privacy measures. TCPA Embedded Security does not involve a portion of the operating system kernel that is dedicated to securely authenticating users for access to root user privileges.

## 2. SUMMARY OF INVENTION

### *Invention Summary*

Current Linux operating systems restrict the abilities of normal users. Only the root user or super-user is able to modify OS preferences, install or modify applications, access OS system files, or perform other system commands.

In the present invention, super-user or root privileges are authenticated at the kernel level of the operating system. An additional set of code, the Security Sector, is added to the OS kernel. The Security Sector of the kernel prevents the execution of super-user or system commands unless the user can be authenticated. By implementing the Security Sector within the kernel, the opportunities for spoofing and malicious attacks are greatly reduced.

The OS kernel is in direct communication with the hardware of a computing machine. This includes processors, storage drives, and I/O devices. As such, the kernel is in a unique position because there is no opportunity for malicious individuals to come between the kernel and the system hardware. In order to authenticate a user for root or super-user privileges, the Security Sector takes advantage of this position by requiring that user authentication come directly from the hardware.

[1] http://h71019.www7.hp.com/enterprise/downloads/HP_ProtectTools_Embedded_Security.pdf

Hardware authentication may be established in a variety of forms. At the most basic level, a password that originates directly from the keyboard could be used to authenticate a user. More secure implementations could involve the use of smart cards, or biometric identifiers to authenticate a user for root privileges. By ensuring that authentication identifiers come directly from a system's hardware, the ability for malicious individuals to gain root access through network connections is eliminated.

***Unique Concepts***

The unique concept of the present invention is the requirement of kernel level authentication in order to execute system or root level commands.

## 3. DESCRIPTION OF THE INVENTION

Figure 1 depicts the system for Kernel Embedded Security Authentication.

The User Machine is a computing device such as a desktop computer, laptop, server, or mobile device.

The Applications are a collection of software applications installed on the User Machine.

The OS is an operating system, such as Linux, running on the User Machine. The OS manages interactions between users, software, and hardware.

The Kernel is the code foundation for the OS. The Kernel communicates directly with the Microprocessor, I/O Devices, and other hardware components.

The Security Sector is a portion of the Kernel that is dedicated to managing security. The Security Sector prevents the execution of system commands by unauthorized parties, and manages the authentication of root users through direct communication with I/O Devices.

The Microprocessor is an integrated circuit that handles the processing necessary for the operation of the User Machine.

The I/O Devices are a collection of input and/or output devices such as keyboards, display devices, removable storage drives, and security hardware devices.

The Memory is all the physical memory residing within the User Machine.

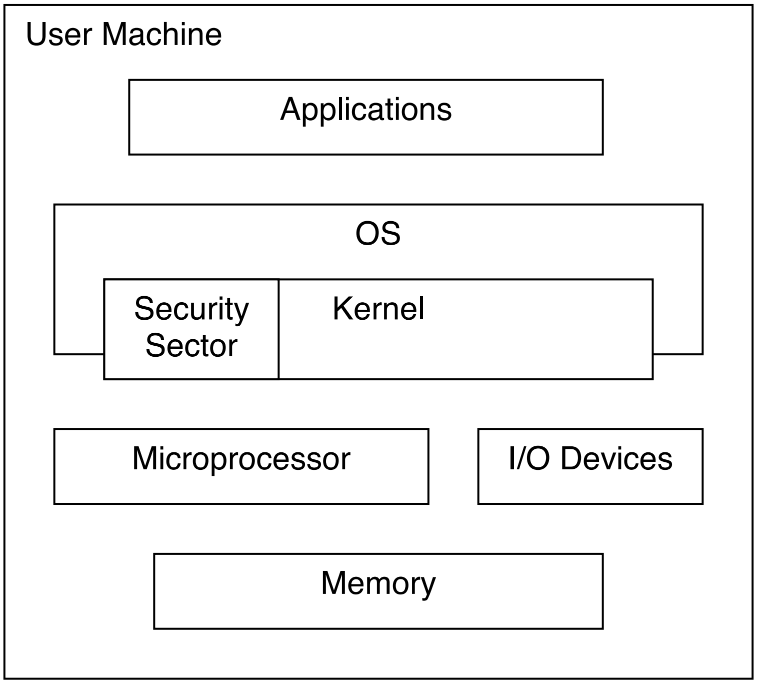

**Figure 1. System for Kernel Embedded Security Authentication.**

Figure 2 depicts the method of Kernel Embedded Security Authentication.

In step 1, a User or Application issues a system command. A system command could be a request to modify system settings, to install an application, or to access secure memory.

In step 2, the Kernel receives the system command and the Security Sector prompts the user, via an I/O Device such as a display, for a security identifier. The security identifier could be a password, hardware identifier, or other security implementation.

In step 3, the user inputs the security identifier via an I/O Device.

In step 4, the Security Sector of the Kernel receives the security identifier from the I/O Device. Security Identifiers originating from an unauthorized source such as a network connection or software application are rejected. The Security Sector attempts to authenticate the security identifier by comparing it to the approved identifier(s) stored in a restricted portion of the Memory. If the Kernel authenticates the security identifier, proceed to step 5. If the Kernel cannot authenticate the security identifier, the method proceeds to step 6.

In step 5, the Kernel executes the system command as issued.

In step 6, the Kernel denies the system command and notification is sent to the OS.

In optional step 7, after the execution of the desired command, the Security Sector revokes root level privileges to prevent exploitation by malicious individuals.

The method ends.

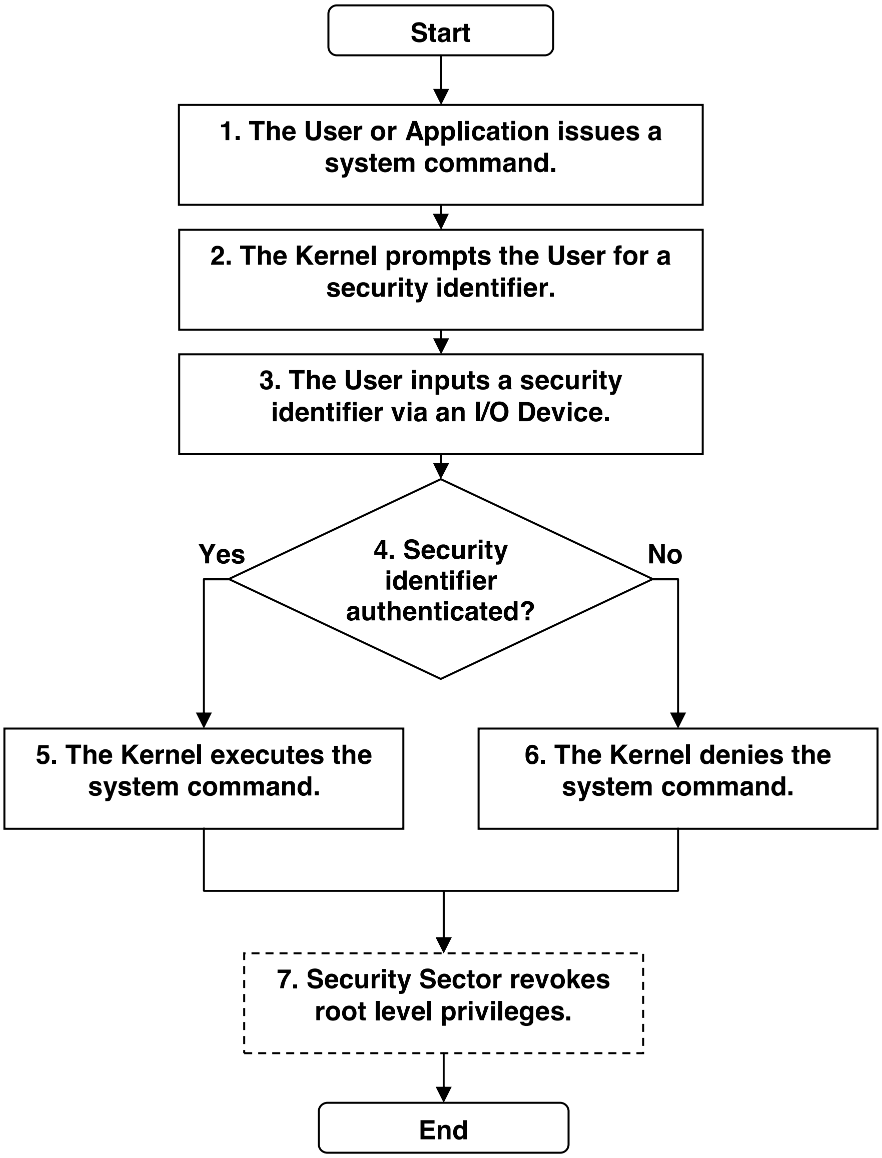
Start
1. The User or Application issues a system command.
2. The Kernel prompts the User for a security identifier.
3. The User inputs a security identifier via an I/O Device.
4. Security identifier authenticated?
Yes
No
5. The Kernel executes the system command.
6. The Kernel denies the system command.
7. Security Sector revokes root level privileges.
End

**Figure 2. Method of Kernel Embedded Security Authentication.**