Technical Disclosure Commons

Defensive Publications Series

March 28, 2019

MANAGEABLE ELECTRICAL LOCK FOR SERVER CHASSIS

Yang Sun

Zomin Gan

Bruce Chen

Jayaprakash Balachandran

MANAGEABLE ELECTRICAL LOCK FOR SERVER CHASSIS

AUTHORS:
Yang Sun
Zomin Gan
Bruce Chen
Jayaprakash Balachandran

ABSTRACT

Techniques are described herein for a central manageable solution to servers to protect the data and components inside the chassis. The electronic locks or latches may be centrally controlled and monitored by a central software manager. This lock may prevent theft or unintentional access of the internal components to protect the internal data.

DETAILED DESCRIPTION

Data is now the most valuable resource in the world. The importance of securing confidential data is well-known. Sometimes preventing the leakage of data is vital to a business. Normally data is stored in hard drives. Dual In-line Memory Modules (DIMMs) are traditionally volatile, which means data would be lost when the DIMM loses its power. But with increasing usage of non-volatile memories, there is a growing need for data security not only to protect the drives but also the DIMMs.

Data is largely stored in a data center. There are two main mechanisms by which a data leak can occur: online and on the ground. Firewalls or sophisticated programs can be used to prevent online data leakage, and doors can be used to secure the servers from theft on the ground. Some servers also have mechanical locks with keys, but key management is difficult.

A traditional data center usually uses door access control to grant access only to certified people to access the servers. But in reality, there are multiple groups of people who can access the equipment (e.g., air conditioner engineer, electricity engineer, cleaner, etc.). Furthermore, even the data center equipment engineers have several groups such as network groups, server groups, or storage groups. It is possible that many unrelated personnel could access the physical presence of the server components. This could allow them to steal server components such as disks or memory, which contains sensitive data. It is also possible to steal data via interfaces on the front panel (e.g., plug in a USB

(Universal Serial Bus) key with a virus to steal or destroy data). Cameras may be installed to monitor the data center, but that may only be helpful after the security issues have already occurred. As such, a method is needed to help to prevent an unauthorized person from accessing components or data of servers in a data center.

Some servers have some mechanical locks with keys in order to improve security in data centers. However, is nearly impossible to manage hundreds or thousands of keys each corresponding to a respective server implemented in a data center. On the other hand, if thousands of servers share one common key it is also impracticable to replace the thousands of locks if the key is lost.

Accordingly, described herein are techniques that use a remote central control capability to prevent unauthorized personnel from physically accessing a server component. An electrically-controlled lock may be used to lock the server. The lock may latch a cover in front of the server chassis, or fix some components to the server chassis.

A validating operator may use different methods to unlock a lock (e.g., password, Radio Frequency Identification (RFID) card, fingerprint, remote command, etc.). The system also includes a remote communication unit responsible for receiving a remote management command or monitoring the lock status of all the servers.

The locks on the chassis may lock one or several chassis covers or directly lock one or several chassis components, such as dedicated blade or memory modules. Multiple levels of access control may be centrally managed. The lock may also help to provide a “locate” function to locate the equipment the operator wants to access. The locks may be electrically-controlled, and may use RFID, password, fingerprint, local/remote software management, or any other suitable mechanism for obtaining access rights to release the lock(s) for the servers. Software/hardware may be used to centrally control and monitor the lock status of many servers. An outside power source may be used to power the electrical lock unit to operate/override even when the chassis has no power supplied. Each slot may be locked independently, and the unit(s) may support multiple sets of passwords/keys.

Data are typically stored in the chassis in hard drives or memory. If the memory is volatile then the inner data may be lost when no power is applied. But as memory technology evolves, new types of non-volatile memory is being increasingly used. The user

may also need to secure the data in all aspects, including online data transfer and ground theft.

As illustrated in Figure 1 below, the chassis has several vertical hard drive slots. The drives in these slots may be plugged out.

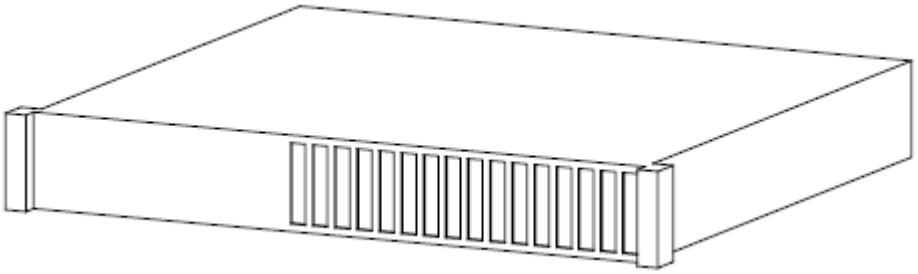

Figure 1

As illustrated in Figure 2 below, a cover may protect the whole chassis. If the cover is in a closed lock state, there is no way to plug the drive out.

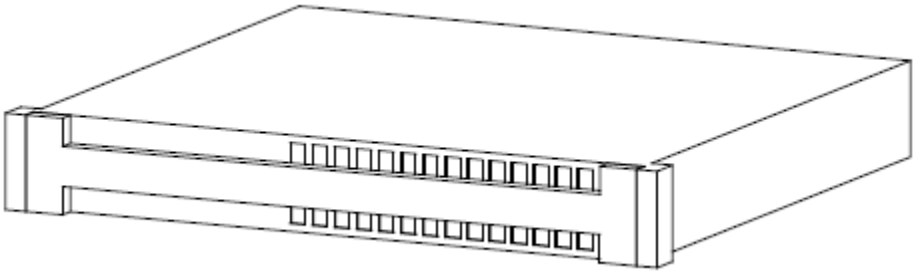

Figure 2

As illustrated in Figure 3 below, a similar mechanism may be implemented on blade servers. If there is a cover on the blade server system with a lock, then no blade can be plugged out without first unlocking the lock.

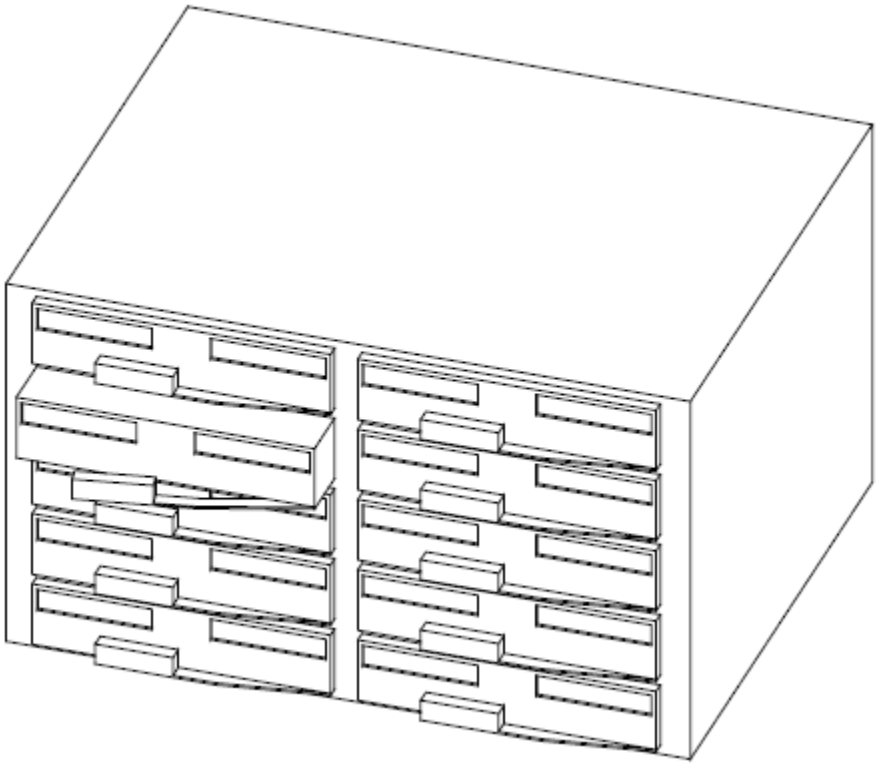

Figure 3

Figure 4 below illustrates functional components included in an example lock.

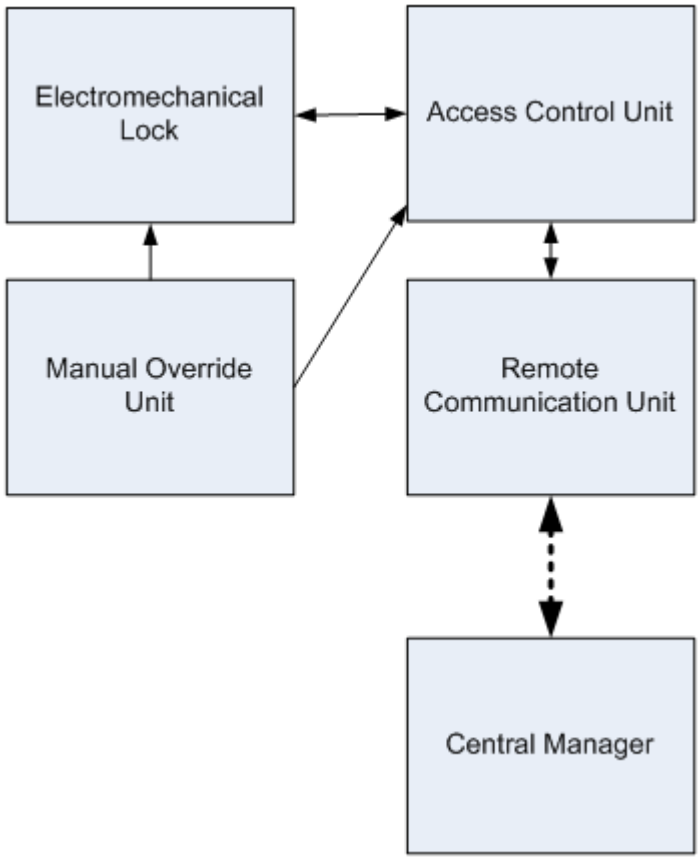

Figure 4

The Electromechanical Lock may provide a lock/unlock function for the chassis via latching, magnetic attachment, or any other suitable method. The Electromechanical Lock receives lock/unlock commands from the Access Control Unit, and also provides lock state monitoring for the Access Control Unit. It is also possible to override the lock states via the Manual Override Unit.

The Access Control Unit controls the lock/unlock state of the lock by identifying the correct user through password monitoring, fingerprint detection, facial recognition, remote control, etc. It may receive lock/unlock commands from the Remote Communication Unit. A user may input the commands or passwords via a keyboard/screen. The Access Control Unit also monitors the lock states and Manual Override Unit states. It transmits this information to the Remote Communication Unit and receives control command / key settings from the Remote Communication Unit. It may also provide an

indication of some information via a Light Emitting Diode (LED), screen, or sound to help the operator quickly locate a particular machine among thousands of identical machines.

The Remote Communication Unit provides communication functionality to a remote management site. It may receive a lock/unlock command from the remote site and send the monitored information to the remote site. The communication path may proceed from the lock, to the server internal communication module, and then to the central management point via one or more networks. Alternatively, this unit may have its own wired or wireless communication path.

The Manual Override Unit provides a failsafe mechanism to override the lock when there is loss of power, communication, or a key. It may override the Access Control Unit to unlock the lock. It may also transmit its override state/alarm to the Access Control Unit. In certain examples, the Manual Override Unit may merge with the Access Control Unit.

The Central Manager may be local or remote. It may manage one or more servers and provide lock/unlock controls or state monitoring. The Central Manager may generate an alarm when the lock is unexpectedly opened. It may also provide an identity function wherein only the dedicated server lock may be opened among many servers. The Central Manager may cooperate with other management units to provide automation. For example, if the management software discovers some issue on one of the servers that requires manual intervention, it may automatically locate that server and unlock the lock.

Figure 5 below illustrates an example lock module. The lock integrates an RFID sensor, a latch, a USB type-C backup power connector, and a communication cable.

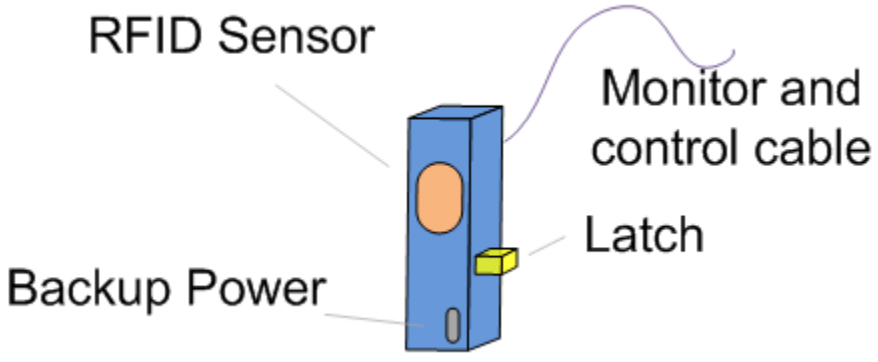

Figure 5

Figure 6 below illustrates the independently locking functionality of the locks among one or more of the modules to provide increased flexibility. Each blade front panel incorporates a digital electronic smart door lock (lock module). Each lock module includes a latch to latch to the chassis wall. The wall is mounted to the chassis such that if the lock operates in a latch state the operator cannot remove the blade from the chassis.

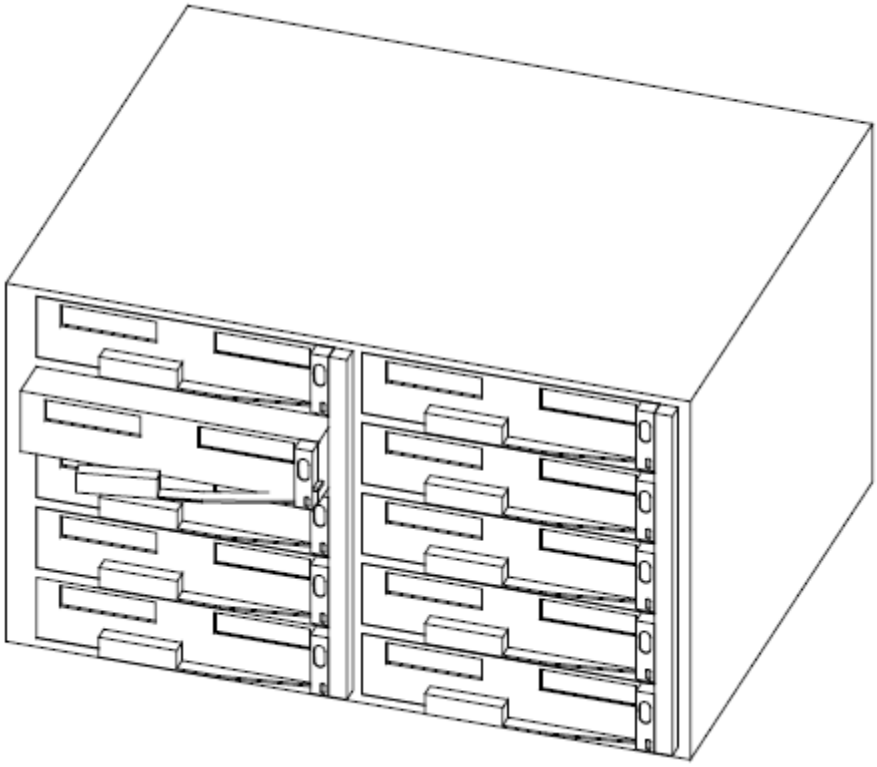

Figure 6

As illustrated in Figure 7 below, there is one Inter-Integrated Circuit (I2C) bus. Other signals communicate between the blade Baseboard Management Controller (BMC) chip and the lock module. The Electromechanical Lock and Manual Override Unit are inside the lock module. The Access Control Unit and Remote Communication Unit are located on the blade. The Access Control Unit's sensor input is located on the lock module.

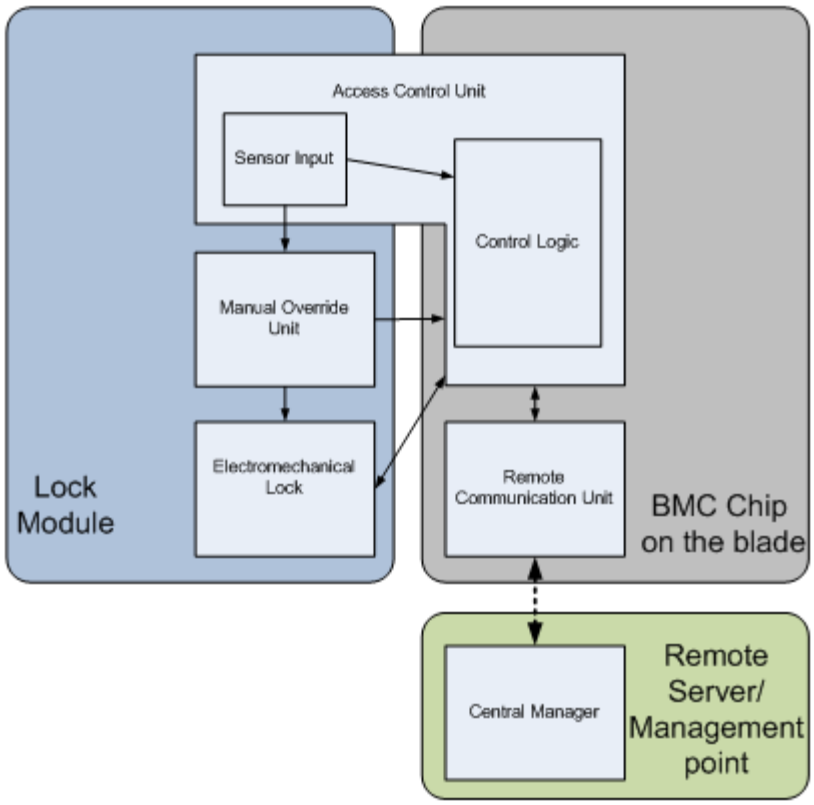

Figure 7

Figure 8 below illustrates an example in which the Central Manager is located at a remote management point.

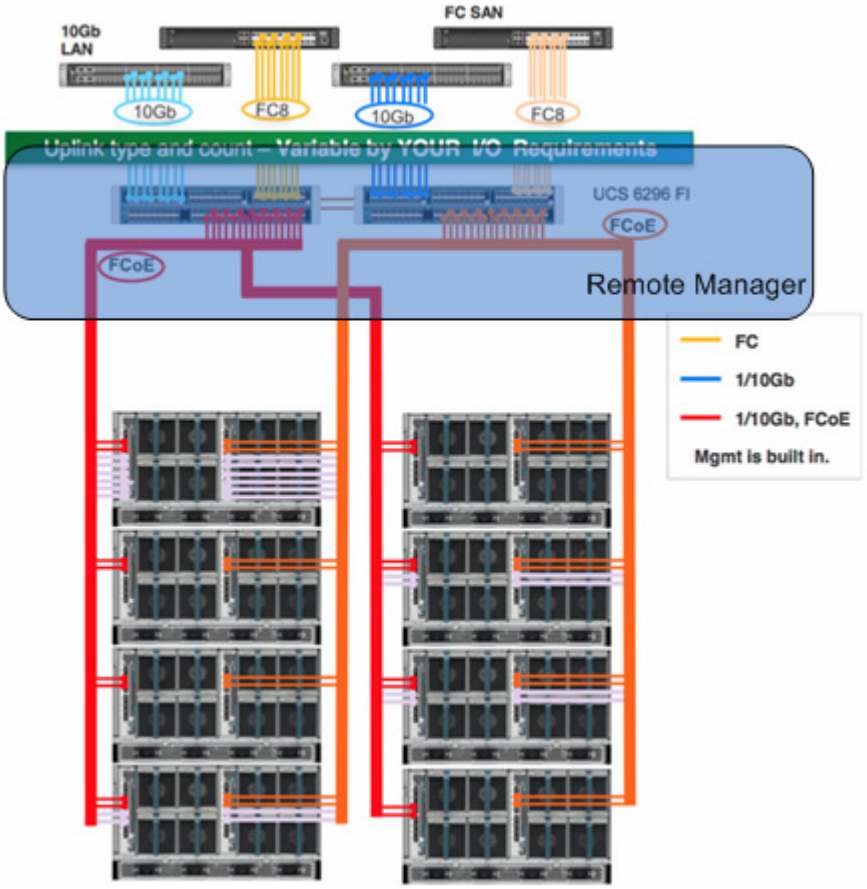

Figure 8

If an operator wants to remove a blade when a chassis is online working inside a data center, the operator needs to log in, configure the Central Manager to power down the specific blade, set the "prepare to unlock" status. The Central Manager communicates with the blade Access Control Unit (here, the BMC chip on the blade) and sets the operator's RFID card as the correct key to unlock the blade. There may optionally be an expired time setting. The operator finds the specific blade and puts the RFID card close to the lock module RFID sensor window. The sensor input passes the RFID data to the Control Logic and Manual Override Unit to verify the key. If the key matches the Access Control Unit, it may grant access and communicate with the lock module accordingly. The module releases the latch and passes the "latch release" status to the Access Control Unit, which passes a "successful unlock" message to the remote Central Manager. The operator can thereby

remove the blade. However, is the only blade the operator can remove in the data center. This eliminates the possibility of a false removal of an operational blade.

In another example, an operator wants to remove a blade when the chassis has no power. Here, the Manual Override Unit already programmed and stored a master RFID key. The operator may connect a power source via the USB type-C cable to the lock module. This will power the lock module and make it functional. The operator places the RFID card close to the lock module RFID sensor window. The sensor input passes the RFID data to the Control Logic and Manual Override Unit to verify the key. If the key matches the Manual Override Unit, it grants access and releases the latch without a response from the Access Control Unit. The operator may then remove the blade.

All the servers' keys and access rights may be configured by the Central Manager when the blade is online. There may be several master keys. When any key is lost it may be removed from the access list.

As described above, each slot may be separately locked rather than using the entire enclosure locker. This also assists in providing an "identify" functionality to prevent the operator from unplugging the wrong working blade. Since the unlocked blade is the only unlocked blade, the operator may remove the blade from among thousands of server chassis. Thus, the central manageable lock server system provides the capability for per-slot/chassis component security.

In summary, techniques are described herein for a central manageable solution to servers to protect the data and components inside the chassis. The electronic locks or latches may be centrally controlled and monitored by a central software manager. This lock may prevent theft or unintentional access of the internal components to protect the internal data.