CRU

Protecting Your Digital Assets™

A New Approach to Cyber Defense

An Elegant Hardware Malware Endpoint Defense System

by Randal Barber

Introduction

The CRU® SCILock® Secure Drive is a game-changing hardware solution to address the never-ending battle to maintain the highest levels of organizational cyber security. The SCILock Secure Drive prevents unauthorized changes to a computer's system environment and in doing so, prevents malware from taking hold and becoming persistent. SCILock also can restore a system to its last known good configuration in a matter of seconds, with a simple reboot. In a marketplace filled with myriad software solutions, firewalls, and other applications, SCILock hardware elegantly simplifies and enhances computer security.

CYBER INSANITY

A week does not go by without news of a new attack or exposure of confidential information. Those are the ones that are made public—what about those attacks that are intentionally kept quiet or have not yet been made public? And consider those unknown attacks that are still in process–the ones that have not been discovered. What a disaster!

A quick sampling of computer technology publications, online articles and blogs clearly shows the IT industry is hard at work creating defenses against these attacks. Corporations and government agencies alike are looking for solutions to protect their systems and data. Yet the attacks continue and seem more ubiquitous than ever.

One of the major, and arguably first, lines of defense is to PATCH and PRAY: PATCH your systems with the latest release from operating system and application vendors and PRAY you don't get attacked. Yet even the patches are sometimes problems in themselves and can cause issues with system stability. And they just seem to set up the next challenge for hackers.

Can we call this what it is? Insanity? Wasn't it Albert Einstein who quipped that insanity is doing the same thing over and over and expecting a different outcome? Continuing to throw more software at threats, no matter how current or adaptive that software might be, is more like a path to the asylum than it is to success.

THE NEW SCILOCK APPROACH: A HARDWARE-BASED SECURE DRIVE

Malware can effectively compromise a computer system because of its ability to make unauthorized changes to that system. Unauthorized system changes can be nefarious, well-meaning, or just accidental. No matter how a change occurs, it can become a mess for the IT professional to clean up. A cleanup can take days, weeks, or sometimes months. Even a quick recovery is rarely all that quick.

And after the effort is completed, there remain nagging thoughts about whether all of the unauthorized changes were found and addressed.

It is time to consider a new approach, one that is hardware-based and cannot be disabled or altered by any software running on the system. One that addresses the core of the problem and protects the system whether the operating system is running, the latest software patches are installed, or the IT administrator forgot to follow a step in some process. This new approach is the SCILock (pronounced "sky-lock") Secure Drive.

HOW MALWARE WANTS TO CHANGE YOUR COMPUTING SYSTEM

For malware to thrive, it needs access to a computer system and rights to the targeted data–either for exfiltration or to control the data in some other way (e.g. ransomware). Remove either of these attributes and the malware is rendered impotent.

ACCESS:

To gain access to a system, malware attacks follow a few basic approaches. This is true whether an attack is launched externally or internally. While details of attacks change and mutate over time, the basics remain the same.

For example, a very common approach is called phishing–the use of online communications to trick someone within an organization to launch the malware or launch code that opens a back door that then allows malware to be downloaded in small portions and build into an attack over time.

An attack might also be initiated by an insider launching similar code, either knowingly or unknowingly, via thumb drive (for example). The insider could be an employee using the computer network or a contractor who is servicing a system within the facility–even a system not directly related to the computer network itself. This code also opens a back door that allows the attack to be downloaded and built over time.

In either case, to initiate the damaging malware, i.e., downloading the payload, requires a change to be made to

the system–a change that needs to survive a reboot the of the host system. Stop this access and the attack will not proceed.

PRIVILEGES:

Along with access, malware normally needs to escalate its rights or privileges before completing its task. Malware often positions itself to work around current operating system or third-party software defenses at the next boot cycle.

No matter the method of access, or the method of privilege escalation, the component most targeted by malware, in any system, is the system drive. Protect the system drive and you have drastically reduced your attack profile and increased the stability and uptime of your network.

THE SCILOCK SECURE DRIVE

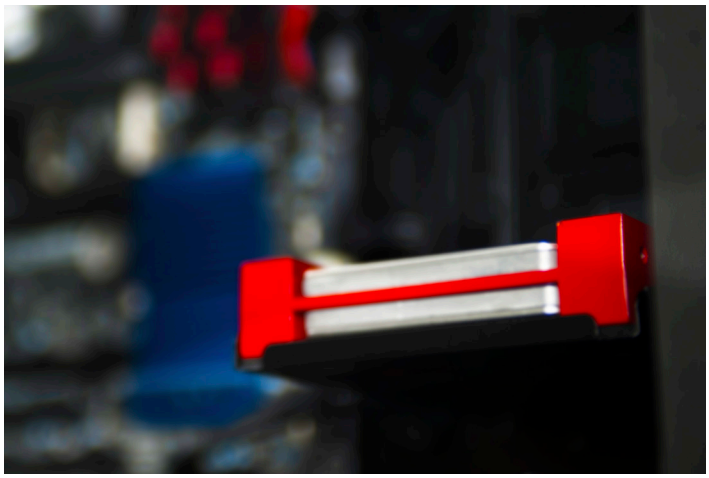
SCILock is a unique, patent-pending secure drive that takes the place of a computer's hard drive. SCILock provides an environment that shields the operating system, applications, and any other data you wish to protect from unauthorized changes. In operation, SCILock is undetectable–SCILock appears to the system and user as a standard drive. It requires no special drivers and leaves no signature that could be exploited. SCILock uses no CPU or RAM resources from the host system and does not rely on signature files or other databases for operation–no updates are required.

The difference between SCILock and a standard system drive is that SCILock prevents unwanted changes to operating system and application resources. Thus, to the extent that malware relies on changes to those resources–that is to say, most strains of malware–your system is protected. For instance, malware that requires a system restart in order to run or to escalate privileges–many strains of malware fall into this category–will be disabled upon reboot, as any corrupted files and registry settings are returned to their trusted states. Indeed, any malware that requires changes to operating system resources will be disabled upon reboot.

SCILock provides the ultimate "restore to last known good configuration". Literally, the 1,000th boot of a SCILock protected system will be exactly the same as the 1st boot. Guaranteed!

SCILock not only improves the stability and usability of your computer, it also provides you peace of mind that your network has not changed outside of your control and knowledge. Endpoint security is widely known as an effective method to secure a network: allow no changes to an endpoint (a computer, in other words) and malware cannot propagate into the network.

That's the power of SCILock: hardware technology that protects your system resources from threats known and unknown. It's an elegant security tool in an industry where complexity has become its own enemy. SCILock has achieved what software never could: physical protection of your system.



SECURITY WITH CONVENIENCE INCLUDED, NO CHARGE

For convenience and the utmost in security assurance, SCILock provides two modes of operation: Secure Mode and Admin Mode. When in Secure Mode (the default mode), changes are not allowed on the system and application files that you have chosen to protect. When you want to update the system, you boot the computer into SCILock Admin Mode. While in Admin Mode, changes to the system drive are allowed. Once these changes are

complete, the system is rebooted to Secure Mode and those authorized changes are protected.

Changing the mode of SCILock requires a secure, hardware authorization key (dongle). The authorization path is independent of the data path used by SCILock to connect to the system. This creates an impenetrable system drive–there is nothing the system can do, no command it can send, that will alter the mode of SCILock. Without the authorization key, the system will remain the same, day in, and day out.

SCILock eliminates the ability of malware, and other unauthorized changes, to become persistent within the system drive. This gives you control over when changes are made to your system.

WHAT ABOUT THE NEW OR UNKNOWN?

We are often asked, "but what about new malware strains we do not know about? Or those types of malware that attack other components within a system? How does the SCILock Secure Drive help there?"

New malware is being released routinely. As long as malware needs to live or become persistent within the system drive, SCILock protects the system. Whether the malware is a well-known strain or a new zero day attack, SCILock protects the system drive from unauthorized changes.

No one can claim 100% success defeating all malware types. However, a drastic reduction in the attack profile of your systems, blocking of 99-plus percent of malware currently harming networks, allows your other cyber defenses to focus on malware that targets components other than your system drive.

KEEP CALM AND REBOOT

SCILock does not replace the software security you currently use. Proper system and network configuration, along with monitoring memory processes, protecting the network perimeter, and policing network traffic, will remain vital. SCILock does protect your security programs from being altered or disabled by malware and assures the software defenses will properly launch during the next boot cycle.

When some type of cyber event occurs within your organization, how much time and manpower will you save if you can simply reboot a computer or the network and be back to your last known good computing environment? Think about that–in just a few minutes you can reboot to recovery every system on your network. Compare this to the days, weeks or months of time the typical network recovery takes.

SCILOCK: THE CORNERSTONE OF SECURITY AND CYBER SAFETY

SCILock is a unique, hardware-based solution to your cyber defense. By eliminating the possibility of malware making persistent and unauthorized changes to computers on your network, and giving you a way to quickly reboot to your golden image, SCILock will become the cornerstone on which you build your cyber-safe computing environment.

For more information,
visit the CRU web site.

www.cru-inc.com
scilock@cru-inc.com