Seagate

SECUDE
IT SECURITY PRODUCTS & SOLUTIONS

A higher level of IT-Security

No Back Doors. No Open Windows.

Pre-Boot Authentication White Paper

Abstract: **F**ull **D**isk **E**ncryption (FDE) has been hailed as the final word in **D**ata-**a**t-**R**est (DAR) security by many in the industry, but some fail to recognize that encryption is only as secure as the authentication used to access it. Encryption without strong authentication is like locking your door and then leaving the key in the lock while you walk away. Leaving authentication to your operating system is one step better, but only gives you the security of hiding the key under your doormat.

Table of Contents

1 Introduction: To Boot or to Pre-Boot?

Full **D**isk **E**ncryption (FDE) has been hailed as the final word in **D**ata-**a**t-**R**est (DAR) security by many in the industry, but some fail to recognize that encryption is only as secure as the authentication used to access it. Encryption without strong authentication is like locking your door and then leaving the key in the lock while you walk away. Leaving authentication to your operating system is one step better, but only gives you the security of hiding the key under your doormat.

Operating systems are great and wonderful things, but they are so complicated that even the mouse interface can be a potential attack vector. The sheer amount of code that must interface flawlessly without giving up so much as a single buffer overflow is so vast that Microsoft employs thousands of full time programmers and years of effort to develop and maintain its assorted Operating Systems and it doesn't take more than a Google search to come up with an overwhelming list of known and potential vulnerabilities.

A **P**re-**B**oot **A**uthentication (PBA) environment serves as an extension of the BIOS or boot firmware and guarantees a secure, tamper-proof environment external to the operating system as a trusted authentication layer. The PBA prevents Windows or any other operating system from loading until the user has confirmed he/she has the correct password to unlock the door. That trusted layer eliminates the possibility that 1 of the millions of lines of OS code can compromise the privacy of personal or company data.

2 Why bother with PBA?

PBA is about security and security is about managing risks; the risks of theft, non-compliance with government regulations, fraud, loss of data, and more.

Sound complicated? It can be and many enterprises are finding they do not have the right skill set or budget to implement tight security. Secude and Seagate believe that good security should never be unnecessarily complicated. The goal of PBA is to eliminate the complexity associated with security. But first let's review the reasons why security is complicated today.

2.1 Technical: *Complexity breeds insecurity.*

The four eyes principle is a well known and well verified principle to enhance security which simply states that two pairs of eyes should be involved in every important transaction. This reduces incidents of fraud as well as errors which one person might make, but two people are unlikely to miss. However, there is a point of diminishing returns where adding more eyes will not make the system more secure.

Security guards are a classic example of this situation. One guard can only patrol one given area at a time, leading to holes in the security system. A pair of guards can look in different directions for threats and watch each other's backs, so security is increased dramatically.

However, adding one hundred guards can be self defeating if you have to give each of the guards a set of keys to perform their patrol. Instead of making the area more secure, you've just added 100 more potential targets for a burglar or pickpocket. Instead, it's better to hire two really good guards and make sure they're doing their job.

2.2 Social: *If I can't use it easily, I won't use it.*

To eliminate the risks of user behaviour, ease of use is an important consideration for security software. Without an easy to use system, users will leave their passwords unattended, leave their laptops unattended with the encryption unlocked, and simply turn the system off if it is too cumbersome. What good is the six foot safe to protect your laptop?

In addition, ease of use offers increased productivity as users are not burdened with frequent authentication requests or forced to make frequent help desk calls which cost enterprises considerable amounts of time and money. Research from the Burton Group

indicates that each call to the IT help desk may cost $58 USD.[1] Eliminating even one password that a user has to remember means one less help desk call and a clear ROI.

As every CSO knows, users simply will not tolerate security that interferes with their day to day operations and will easily avoid using it. The prevalence of Full Disk Encryption products on the market attests to the inability of file and folder encryption to sufficiently protect documents. Users consistently manage to save critical files in unencrypted folders, chose easy to guess passwords, or worse yet, save their passwords in an unencrypted text file on the desktop. Full Disk Encryption avoids these obstacles by ensuring that the user does not notice any impact on their productivity and is unable to turn off or avoid the encryption at any point.

[1] RSA Security (2004), *Are Passwords Really Free?,* CLHC WP 0804

3 Keeping it Simple

3.1 The Requirements

A Pre-Boot Environment protects against these risks by keeping a simple shell and only providing enough functionality to authenticate the user and pass on credentials. Any additional unused functionality should be eliminated as each function represents an additional door to lock and guard. The fewer doors and windows, the more security.

An ideal Pre-Boot Environment must be secure and adaptive.

- **Secure**
  - *Must have a significant developer talent pool and level of interest*
  - *Should be well written and provide a reasonable internal security model*
  - *With the aid of hardware it should be difficult to alter or spoof the Pre-Boot Environment*
- **Adaptive**
  - *Must have widely available extensible driver support for authentication devices such as smartcards or biometric readers*
  - *Should be portable to common computer hardware platforms*
  - *Must be adaptable to a standards based model*

3.2 Why Linux?

Linux is an ideal environment for Pre-Boot Authentication. Many software vendors attempt to create their own environment because they've become infected with NIH (Not Invented Here) syndrome. The temptation to believe you can do it better than anyone else may often be true, but the idea that you can do it better than *every*one else is clearly flawed. Teamwork produces results and open source solutions provide a framework where a tremendous amount of brainpower from all over the world can be applied to any given problem.

Here's a step by step approach to the qualifications listed above:

3.2.1 A Secure Environment

- *Must have a significant developer talent pool and level of interest*

More guards don't necessarily mean more security, but more testers definitely do. Windows doesn't have more security holes than other operating systems because it has bad programmers; Windows is just a bigger target. With so many people looking to exploit security holes, more security holes will be found. If that same level of interest can be applied to a Pre-Boot Environment in a positive fashion, security holes can be found and patched effectively.

Linux does this with tens of thousands of developers constantly testing, programming, and actively searching for ways to break the system. Some of the same people that find the bugs in Windows are the same people finding bugs in Linux, but the difference is that when a bug is discovered in Linux it will be patched immediately. That same bug fix will be inspected by hundreds of other programmers all contributing to that section of the code and double checking each other's work.

Proprietary operating systems which must be patched by a limited number of developers working on the clock often lack this level of oversight. An open environment with higher visibility means more security.

- *Should be well written and provide a reasonable internal security model*

While this seems straightforward, it is remarkably easy to get wrong. The security model and philosophy must be adaptive to be able to work with a variety of hardware platforms and easily update to newer technologies.

Linux uses a well-known and proven Unix-based security model. The enormous pool of developer talent is linked to this subject as a large number of individuals with different desires for an environment are pushing and pulling for the most extensible environment possible. This has made Linux remarkably flexible with the ability to configure a Linux kernel to easily suit individual needs. This was a key reason that the NSA used Linux as the basis for creating a secure operating system.[2]

[2] http://www.nsa.gov/selinux

- *With the aid of hardware it should be difficult to alter or spoof the Pre-Boot Environment*

The Pre-Boot Environment must have verifiable data integrity. An attacker must not able to modify the Pre-Boot and add an extra set of keys or any sort of spy ware to the system.

Spy ware attacks are unlikely as they involve an extremely sophisticated hacker with intimate knowledge of the Pre-Boot code able to modify or spoof the data integrity checks (hashing). But even such an attacker would also have to steal the laptop in question without the user's knowledge, modify the Pre-Boot in an undetectable way, return it to the user, wait for the user to type in their password, and then steal the laptop a second time. A scenario even James Bond might find daunting.

Software based FDE such as SECUDE secure notebook uses such data integrity checks to eliminate the possibility that the Pre-Boot can be modified without inadvertently destroying the functionality of the program or the integrity of the key. So even the above mentioned super spy wouldn't be able to use this as a potential attack vector.

Hardware based FDE such as that provided by SECUDE's Finally Secure Pre-Boot Authentication and Seagate Momentus FDE.2 drives offer an additional level of protection in that when the drive is in a locked state, the Pre-Boot partition is read only. In order to modify the environment at all, the user must authenticate, which is exactly what the attacker is unable to do in the first place.

3.2.2 An Adaptive Technology

- *Must have widely available extensible driver support for authentication devices such as smartcards or biometric readers*

As an open source solution, there are a great variety of developers seeking to use Linux for a variety of purposes, and that means a large amount of driver development often available for free. Smartcard or biometric vendors can have their devices ported to Linux at no cost to themselves.[3] That means greater compatibility and flexibility for future development. In addition, Linux is well known for playing nice with installed OSes and BIOS, as well as being widely accepted worldwide by both large and small entities.

- *Should be portable to common computer hardware platforms*

There are at least five common CPU architectures and Linux runs on all of them. Proprietary OSes have advantages, but are limited to those architectures they are actually designed for. By virtue of the fact that its developers have wide ranging interests and use cases, Linux has been developed to be completely portable to any widely distributed CPU architecture.

- *Must be adaptable to a standards based model*

Proprietary systems are intrinsically not standards based because one company wants maintain secrecy over key elements and use that secrecy to control the entire system and dominate the market. This produces potential conflicts and security holes as various extensions to the Pre-Boot Environment will vie to interact with each other and the Pre-Boot to access credentials, activate hibernation or sleep mode, or even simply shut down effectively.

The number of potential conflicts from various security vendors providing their own proprietary operating systems and methodology which can interfere with each other and the main Operating System mean a chaotic mess of race conditions, BIOS incompatibilities, and boot strap failures. Translation: It just won't work.

[3] http://www.kroah.com/log/2007/01/29/

4 Conclusion: End to End Security

This paper has discussed some of the reasons why a Pre-Boot Authentication system is a must have for security conscious users and why a Linux based Pre-Boot offers distinct advantages in this regards. In addition, as an adaptive technology, Linux offers flexibility which proprietary OSes can not match.

Enterprises must embrace a holistic view of security to create an authentication chain beginning prior to the start of the operating system at the Pre-Boot level and leading all the way to business applications within the corporate network. A Pre-Boot Authentication environment is the first link in the authentication chain, providing an Adaptive Technology with Risk Management and Productivity gains for end to end security. By securing this link, users can be assured that they've taken the first step to a complete solution.

Secude secure notebook and FinallySecure provide this authentication functionality to operate with best of class technologies such as Seagate Momentus FDE.2 drives for total Data-at-Rest protection. Allowing your business to survive, adapt, and grow in a heterogeneous IT environment.

About SECUDE

SECUDE International AG is a market leader in the areas of authentication & authorization, encryption, data integrity and the management of digital identities, delivering a higher level of IT Security to organizations around the world. The company offers solutions in single sign-on, role-based access control, and the security of documents, applications and transactions.

SECUDE is a member of IT SEC SWISS AG and was founded in 1996 out of a partnership between SAP AG and the Fraunhofer Institute in Darmstadt, Germany. This partnership resulted in the Secure Network Communication (SNC) module for SAP AG. The company is headquartered in Zurich, Switzerland, with a worldwide customer base and offices in the USA, Germany, Netherlands, Spain and United Arab Emirates.

For further information, please consult www.secude.com

About Seagate

Seagate is the worldwide leader in the design, manufacture and marketing of hard disc drives, providing products for a wide-range of applications, including Enterprise, Desktop, Mobile Computing, Consumer Electronics and Branded Solutions. Seagate's business model leverages technology leadership and world-class manufacturing to deliver industry-leading innovation and quality to its global customers, and to be the low cost producer in all markets in which it participates. The company is committed to providing award-winning products, customer support and reliability to meet the world's growing demand for information storage.

Seagate can be found around the globe and at www.seagate.com

SECUDE IT Security GmbH

D-64293 Darmstadt - Germany

CH-8048 Zürich - Switzerland

Sales: info@secude.com

Technical support: support@secude.com

www.secude.com