Western Digital.

WHITE PAPER

SEPTEMBER 2020

ArmorLock™ Security Platform

Table of Contents

Introduction

Western Digital's ArmorLock Security Platform is the next stage of evolution in secure storage. We designed the platform from scratch, developing it over several years with the objective of pushing the boundaries of state-of-the-art security techniques while maintaining ease-of-use that feels virtually seamless. Western Digital began the design process by choosing existing, proven security concepts, improving them whenever possible, and creating innovative solutions where they were needed. We then wove these concepts together, to create a next-generation architecture that provides security over many technology layers. Our first product that uses this platform is the G-Technology encrypted ArmorLock NVMe™ SSD, which we will refer to as the ArmorLock drive in this document.

Innovative security made simple

As we designed the ArmorLock Security Platform, we looked for inspiration in our daily lives. People have become accustomed to using mobile phones throughout the day, as many of us now keep our phone with us at all times. We pair our phones with external devices such as headphones, and log in with biometrics such as fingerprint or facial recognition.

Using these same sorts of actions seemed like the ideal way to add security features in a way that feels very natural and intuitive. But because we believed the existing Bluetooth™ security standard could be improved upon, we rebuilt parts of it to make it simpler to use, while adding additional layers of security.

We utilize the dedicated, hardware-backed key storage available on the Apple iPhone and MacBook devices to improve our authentication process. Rather than asking you to create and remember yet another username and password to unlock your drive, we use two factors of authentication available within your phone. That could be something you know, such as a passcode used to unlock your phone, or something you are such as the biometric, plus the presence of the hardware-backed key as something you have. This helps provide a secure method of establishing trust while also eliminating a traditional point of friction and weakness within the verification process.

The ArmorLock Security Platform is also designed with features to help protect your data if your drive is lost or stolen. With our Armor-Lock drive, you can make a locked device cryptographically indistinguishable from an erased device by using the default settings.

Principle of least privilege in action

While mobile devices give us a great way to add innovative security features, it's also important to avoid common pitfalls that can come with using such highly-connected devices. The way most of us use our mobile devices is like a computer that's always in our pocket. This sort of interaction tends to involve a lot of internet activity, not all of which is well secured. To exist in this sort of environment safely, it was critical for us to leverage boundaries existing within modern mobile operating systems. It was critical to enable only as much functionality as is absolutely necessary to do what you intend to do.

Your first point of interaction with an ArmorLock drive is with the ArmorLock app. This software is available for download initially through the Apple iOS App Store and Mac App store. In order to be offered on these stores, an app must first go through their screening process. To accomplish this, the software must include sandboxing which limits the privileges of an app to its intended functionality.

When you open the ArmorLock app, you'll notice that it requires minimal permissions on the device. What you may not notice is that it also prevents its data or functionality from being accessed by any other apps on the device by leveraging the hardware-backed key store.

This focus on limiting privileges does not stop with the app itself. Wherever possible, we choose peer-to-peer (P2P) functionality instead of communicating with a centralized cloud. This enables you to use the product in environments where the internet is not available. We also wanted to give you the option to decide where to strike a balance between eliminating security issues with cloud usage and allowing cloud-based features that you find useful.

You don't need to have a Western Digital account or subscription in order to use the ArmorLock drive. Your own authorized device provides the chain of trust, rather than an external entity.

After you download the ArmorLock app, any further cloud communications are optional. If Last Known Location is enabled, the app will retrieve map data. And if you need to authorize someone remotely, then you can do so over the communications and messaging service of your choice.

Administering the ArmorLock drive

You may need to share your drive with others, and we help you do that safely too. The ArmorLock app allows you to share permission to unlock your drive with others when they're within close proximity to it.

Because a phone can be used as a key to unlock your drive, it's important to make sure that device is being handled securely. You have the option within the app to mandate that the people who have permission to share your drive must input the passcode or biometric authentication method they used to set up their mobile device, before they can unlock the drive.

External validation

We don't expect you to simply take our word for the quality of our security functionality. Through every step of the development process, we've sought transparency and external validation. We developed software using formal verification techniques and participated in third-party audits. We've also made our core algorithms available as open-source software, making it available for public review.

Future-proofing

We also understand that we can't foresee all possible future issues, so we've made our platform updatable so that we can address issues as they occur.

Western Digital advantage

As we manufacture our own components from flash silicon and hard disks all the way to system-level products, we are able to create drives that are specially built for their particular purpose. We are able to architect and tune our components for optimal system performance, and to add key features as needed. We can change parameters to suit specific product needs. Because we manufacture our own flash silicon and SSDs, you can be confident that our products will have consistent performance and reliability.

Systems Security

Overview

ArmorLock has been designed with privacy and security in mind from day one. At every step of the process, from the day we manufacture the product, to the day you take ownership of your new drive, to any further firmware updates, we have built-in multiple layers of protection for your data.

The computers we use for manufacturing ArmorLock drives have a variety of systems in place to protect your drive as it's being built. Firmware is verified at multiple stages, and updates are designed to be invisible and protected. We created our own implementation of the elliptic curve cryptography that helps protect your data against a variety of attacks, and we released its source code and a full third-party audit report to provide transparency in our technology. Even our choice of programming languages was made with an eye on protecting the integrity of the device.

Root-of-Trust

The ArmorLock chain of trust begins with a production root private key which is secured offline by Western Digital to defend against key theft attacks. This private key was generated in an offline environment using entropy input from multiple sources, including manually entered entropy from multiple individuals. This root private key is stored in a FIPS 140–2 validated hardware security module (HSM), as are all signing keys used in establishing the ArmorLock chain-of-trust.

Manufacturing security

ArmorLock security begins on the manufacturing line, where computers test the hardware for functionality and performance. Our custom-built manufacturing systems maintain a root-of-trust that begins with Western Digital's root public key and extends a cryptographic chain-of-trust into each drive following a vetted, documented process. Each drive generates its own unique private key, then the corresponding public key is signed by the manufacturing server using an integrated FIPS 140–2 validated module.

These appliances operate in kiosk mode so that the operator only has access to the manufacturing application, and no access to the command line or desktop shell. Additionally, the manufacturing systems are fully containerized, helping to ensure the integrity and reproducibility of this trusted system. These computers are not connected to the internet, which further limits the attack surface of our manufacturing line.

Firmware verification

Software updates are an important part of the security process, but they can also cause friction as you're using the device. Notices about updates might interrupt your workflow. You may have concerns about the potential for new software to damage data or brick the device. ArmorLock incorporates a multi-stage firmware update methodology to mitigate these concerns.

We store a backup image of your existing firmware bundle so it can be used to avoid bricking the device during the update process. If the firmware update process is interrupted – for example by the user unplugging the USB cable during the update – then the new copy might be corrupted. If this happens, the backup copy will be used to restore the drive to a functional version of the firmware.

To address workflow concerns, ArmorLock devices first download the new firmware bundle to a staging area. This download is performed using reduced bandwidth to help avoid affecting the performance of the drive. When the download is complete, we'll notify you that a new copy of the firmware is ready.

If you choose to update, the drive will reset, and it will begin executing the new firmware. If you decide that now is not a good time, then the bundle remains in the staging area until the next time you reset the drive on your own schedule. At that point, the final steps of the firmware update process are completed.

ArmorLock validates its firmware using two main processes: Secure Firmware Boot and Secure Firmware Update. Secure Firmware Boot validates the cryptographic integrity of the firmware image each time the device powers on. Secure Firmware Update validates the digital signature of a newly downloaded firmware update each time you update. This verification also ensures that you can't roll back to an earlier version of the firmware, protecting you from being forced to use an older and potentially less secure version by an attacker.

Production-ready ArmorLock firmware images are signed using a FIPS 140–2 validated cryptographic module, and signing takes place in an air-gapped environment. Once a firmware image passes our extensive automated testing suite and is approved for release, a member of the release team follows a documented process to convey the firmware to a signing computer which has never been connected to the Internet and which boots from a read-only storage device, signs the firmware using a FIPS 140–2 token, then transfers the resulting signed image back to the Western Digital intranet.

Sweet B

The advanced ArmorLock key management functionality is built on asymmetric cryptography, specifically elliptic curve cryptography (ECC) using the NIST P-256 curve. These asymmetric algorithms are used to validate the firmware of the device, each connection between the device and the smartphone or desktop applications, and they are ultimately used to derive the keys used to encrypt and decrypt data on the disk.

We created our own software implementation of ECC called "Sweet B" which uses Digital Signal Processing (DSP) instructions to accelerate core cryptographic computations. Sweet B is designed to defend against multiple classes of attacks on ECC, including timing attacks, per-message secret reuse, and invalid curve attacks. In order to ensure its correctness, we equipped the library with a full set of unit tests and evaluated it using multiple open source tools that detect undefined or unspecified behavior in software. It was then provided to the security research firm Trail of Bits for a third party audit.

Trust is built on transparency. To build trust in Sweet B, we have released the library as open source on GitHub, and the repository history begins with the version that was audited. The current version includes both the full, unredacted audit report from Trail of Bits along with documentation for each mitigation that was carried out following the report.

Memory and type safety

Memory unsafety and related problems in C or C++-based software are a frequent cause of exploitable vulnerabilities in software, a problem that stretches back decades to the Internet-breaking Morris worm of 1988. Statistics from one of the largest multinational technology companies indicate that 70% of the vulnerabilities patched every year in their software are caused by memory unsafety.

In order to comprehensively mitigate these vulnerabilities in the ArmorLock firmware, we chose to implement our software in the Java language using the open source OpenJDK class libraries and a custom virtual machine optimized for embedded environments. Utilizing a virtual machine also provides software fault isolation as another defensive measure in the event of an error in the firmware.

This approach to memory safety extends to all aspects of the ArmorLock Security Platform. The client software applications for smartphones and desktop computers are implemented using Swift, Java, and Kotlin, and our manufacturing line systems are also implemented in Java and Kotlin. The use of modern languages provides comprehensive mitigation for the vulnerabilities often found in C or C++-based embedded firmware.

Hardware Security

Overview

Encryption is important to both the confidentiality of your data and the drive where your data resides. ArmorLock drives utilize strong, hardware-based encryption to help increase security without impacting speed. Products are also cryptographically verified so you can be confident that the ArmorLock products you're using are authentic.

Whole disk encryption

ArmorLock drives feature 256-bit Advanced Encryption Standard (AES) hardware-based encryption utilizing the XTS block cipher mode. This hardware encryption engine is tied to the ArmorLock key management system, which helps protect the privacy of your data in case the drive is lost or stolen.

Hardware encryption

The ArmorLock drive is designed with always-on hardware encryption and decryption built into the data path while mitigating its impact on performance. On the ArmorLock NVMe SSD product the encryption engine is built into our own custom-designed drive controller silicon, so you can access your data at up to 1000MB per second over a SuperSpeed USB 10Gbps connection.*

The ArmorLock key management scheme is implemented on a separate security element that communicates with the ArmorLock app over Bluetooth or USB. This separate coprocessor isn't responsible for data path processing, which helps mitigate any impact on the speed of access to your drive.

Hardware-based encryption is also more secure than encryption done in software. In software-based encryption, the host computer has access to the encryption key for the disk, which means that malware on the host can steal that key. Once stolen, access to that key can never be revoked. In hardware-based encryption, the key used to encrypt data on the drive stays isolated within the drive itself, and if malware is discovered on a computer, that computer's access to the drive can be safely revoked.

Authorized product verification

You can be sure that your ArmorLock drive and app are authentic products. Each ArmorLock drive contains certificate data signed by the ArmorLock manufacturing systems to validate the authenticity of the device, firmware, and related files. The certificate data is stored in a tamper-resistant form in the product hardware.

Each drive has its own unique hardware identity key and certificate, which is validated by the ArmorLock client applications when connecting to the drive. This certificate is also tied to a unique key in the QR code on the back of the drive, helping to ensure that the application is connecting to the correct drive. This helps prevent an attacker from using a compromised ArmorLock drive to attempt to intercept messages from your phone or computer.

Application Security

Overview

Since your ArmorLock drive uses your phone or computer as a key, it's important that the ArmorLock application be as secure as the drive. To help protect the application from attacks, we've sandboxed the application and limited its access to other files and programs.

App store-approved software

The ArmorLock app is available for download through platform-native software distribution methods such as the Apple App Store. In order to ensure our software is available through this method, we had to design the hardware and our software applications together so that they did not rely on kernel-level drivers or other features not available in App Store apps. By ensuring that our software is available this way, you can easily find the official client application and keep it up to date along with the rest of your apps.

Sandboxed applications

One of the security measures that must be met by apps listed on official app stores is application sandboxing. Sandboxing supports built-in operating system checks to limit an app's use of system resources to only those features that the app developer intends. This helps prevent inserted malicious code or faulty code from being used to access additional system resources.

For instance, a sandboxed application cannot corrupt other applications' files, or spoof operating system level security dialogs. By contrast, an app which contains a kernel-level driver has full control over your operating system as well as all applications and files on your computer. Any security bug in this driver might allow malware to take over your entire computer.

Sandboxed applications include an entitlement list that enumerates the set of system resources that the app requires. This list is checked by the operator of the app store (such as Apple) to ensure that it matches the features of the application. If the application attempts to access a resource that it does not have permission to use, such as a microphone, then the operating system's sandbox will prevent the application from continuing.

This keeps an app from being used to access resources and data on your device which it should not have. We keep the entitlement list for our application as small as possible, to further limit risk. When permissions are required, such as access to location or the camera, the ArmorLock app will ask for permission only when it is needed and explain why that access is needed.

Communications Security

Overview

ArmorLock provides a simple "point and pair" wireless experience that improves security when compared to existing Bluetooth products. To enable this experience, we've created and verified the ArmorLock Secure Transport protocol that helps protect both your wired and wireless communications when using the ArmorLock app.

Communication protocols

ArmorLock gives you two methods to unlock your drive and authorize other users: wirelessly over Bluetooth and using a wired method over USB. No matter which method you choose, the same technologies are used to help secure your connection to the device.

We customized our Bluetooth implementation for improved security as well as usability. Traditionally, the Bluetooth pairing process requires a pairing code to be entered on both devices. Some devices use a default code which undermines the security of the pairing process. We've designed our own layer of Bluetooth security which provides a "point and pair" connection process. This layer makes it easier to pair and also provides improved security by verifying the authenticity of the drive when you connect to it.

Each ArmorLock drive contains a label with a unique key that is used to locate the drive and secure the connection. When connecting over Bluetooth, you simply scan the QR code on the label, then your phone finds and connects to the drive using the key embedded in the code. When connecting over USB, a separate, shorter code is used, which is printed next to the QR code. This code serves as validation you're connecting to the right drive, and also helps prevent malicious applications from connecting to it.

ArmorLock secure transport layer

All communication between your phone or computer and the ArmorLock drive takes place over the ArmorLock Secure Transport cryptographic protocol. This protocol incorporates a multi-step handshake that provides guarantees similar to the Transport Layer Security (TLS) protocol used for HTTPS connections on the Internet.

When connecting to the drive, your phone or computer receives a certificate that identifies the drive as a genuine ArmorLock product and verifies this using a chain of signatures. This certificate is cryptographically tied to the label on the back of the drive, providing a guarantee that no malicious party is tampering with or eavesdropping on the connection to ArmorLock.

When you take the drive out of the box and set it up for the first time, your phone or computer obtains a certificate that it presents on future connections to the drive. The drive then validates this certificate from your phone. Any other phones or computers you authorize also receive a certificate signed by the drive, extending the ArmorLock chain-of-trust from our root key into your authorized devices.

The ArmorLock Secure Transport protocol incorporates modern best practice in connection security, including Perfect Forward Secrecy (PFS) and Authenticated Encryption with Associated Data (AEAD) ciphers. To ensure that our protocol was designed correctly, we created a formalized model of the protocol and mathematically proved its security against a wireless attacker using the verification tool ProVerif. Through formal verification, ArmorLock Secure Transport provides a level of design assurance which is not present in traditional Bluetooth connections.

Data Protection

Overview

ArmorLock protects your data with hardware-backed encryption. This encryption is based on a new approach to public-key management which allows your data to be secured by the hardware-based key storage in your smartphone or computer. ArmorLock drives have been designed to ensure that your data can't be distinguished from one that has been factory reset.

Authorization

The most important function of a self-encrypting drive is verifying that the user of the drive has authorization to access the data. Critically, this verification must be done by binding the authorization to the encryption key used to access data on the drive. This is traditionally done with a username and password, which is then associated with a list of permissions and keys that allow access to the data on the drive.

Passwords can be a weak link in security, while also interfering with the usability of a device. Simply put, people may choose weak passwords, or they forget them. Once the password of a self-encrypting drive is lost, the data on the drive is lost as well.

To address these issues, ArmorLock uses a new approach to securing data on a self-encrypting drive. ArmorLock uses your device – such as a smartphone or laptop – as a "key" that can unlock your drive. Specifically, this is done through an elliptic curve private key in hardware-backed key storage on your device.

When you set up an ArmorLock drive for the first time, or when an authorized manager of an ArmorLock drive gives you access to the drive, your phone or laptop's public key is sent to the drive through the ArmorLock Secure Transport protocol. The ArmorLock drive records the public key so that it can recognize it the next time you want to unlock the drive.

When you unlock an ArmorLock drive, it creates a "challenge" based on your public key and sends that challenge to your phone or laptop. Your device uses the private key in its hardware-backed key storage to create the response to this challenge, then sends it back to the ArmorLock drive. The drive then uses the response to derive the storage encryption key that allows you to access the content on the drive.

Each challenge is uniquely generated, and only your phone or laptop can produce the correct response for the challenge. Without having both the authorized device as a key, as well as the drive it's paired with, the drive cannot be decrypted.

Hardware backed keychain

To further protect the information for this key exchange, we utilize the isolated hardware-backed key storage available on Apple iPhone and Apple MacBook devices. This hardware-based protection also enforces the use of your mobile device's passcode or the biometric used to unlock the private key.

Plausible deniability

ArmorLock drives are designed for plausible deniability by default, which means that you can deny that the drive has any useful data stored on it. In this default configuration, nobody examining the state of your drive can tell the difference between a locked device and an erased device. If the drive is lost or stolen, even an attacker that disassembles the drive cannot reveal which users have access to the drive.

We accomplish this by not having a special state for an erased drive that is separate from that of a locked drive. When the drive is reset to factory defaults, the drive internally creates a new private key that has access to the drive, grants access to this private key, then erases the private key from memory. Thus, a drive that has been reset to factory defaults appears the same as a drive that has valid data on it. Similarly, a drive that has valid data on it which is in its default configuration appears the same as a drive that has been reset to factory defaults.

Privacy

Overview

Our primary goal with the ArmorLock drive is to help you maintain the privacy of your data without sacrificing usability. Wherever possible, we've minimized the use of Internet-based features. We've given you the choice of which cloud-based features you wish to enable. And you can authorize other people to share your drive in the way that best suits your needs.

Minimal internet requirement

We choose peer-to-peer connection methods that are between your authorized devices and drive wherever possible, instead of communicating with a centralized cloud. You can use your ArmorLock device without having a Western Digital account or subscription because your own authorized device provides access to the drive, rather than an external entity.

This allows you to use the product when the internet is not available, and it allows you to limit security issues with cloud usage. After downloading the ArmorLock app, any further cloud communications are by your choice.

QR code scanning

Your ArmorLock drive has a label on its back with a QR code that opens a website when you scan it with your smartphone. If you don't have the app installed, scanning the QR code will point you to a website where you can get the app from the appropriate store. If you already have the ArmorLock app, scanning the QR code will launch it directly.

The QR code on the ArmorLock drive also contains a unique key that your phone uses to help find the ArmorLock drive. Without knowledge of this key, it's impossible for someone to identify or track your ArmorLock drive just based on its Bluetooth transmissions. Because this QR code is unique to your drive, it can also be used as an asset management tag to identify the drive for inventory purposes. The key in the QR code is tied to the hardware identity certificate, which your phone verifies when connecting to the drive.

Next to the QR code is a "short" code consisting of eight digits. This code is used when connecting the drive to an ArmorLock app running on a laptop or desktop computer, since not all computers are able to scan a QR code. Because this code is too short to serve as a cryptographic key, it cannot be used to communicate with the drive over Bluetooth.

Authorized device management

You may wish to add another authorized user to your ArmorLock drive. When you're both in the same location, this process happens in a similar way to how you added your first authorized device.

Having both parties physically present at the same time and place to scan a QR code is sometimes inconvenient or impractical. In this case, you can pre-authorize a user before providing them the drive. The user who needs access to the drive sends their public key to you over the communications and messaging method of your choice, and you can use this key to authorize their access to the drive.

The ArmorLock drive helps protect the privacy of users who have access to the drive. Just knowing a user's public key doesn't let you determine whether they have access to a particular drive. This is true even if you can disassemble and fully access all components of the drive.

Last known location feature

Having the ability to see where your device is physically located can give you peace of mind. We give you the option to enable drive location sharing, which allows you to pinpoint the last known location of your ArmorLock drive. This information is not shared with Western Digital. Because this location awareness is provided by your phone, this information is only shared between your authorized device and your location service provider.

Anti-tracking features

Even though the ArmorLock drive uses Bluetooth, you can't be tracked through the drive. All identifiers broadcast by the drive are randomized periodically. Identifying a particular ArmorLock drive requires knowledge of the unique key contained within the QR code on the drive. Anyone who does not know this key will not be able to track the location of the drive through its Bluetooth radio.

When you use the ArmorLock app on a smartphone, the app quietly listens for an ArmorLock drive that it recognizes. Until it does, the app does not transmit at all over Bluetooth. Communications between the app and the drive are protected by the ArmorLock Secure Transport protocol, which helps prevent wireless attackers from being able to identify either the phone or the drive.

Conclusion

In creating the ArmorLock Security Platform, we began the design with privacy and security in mind, without sacrificing usability. We thoroughly re-examined how we protect your data – from when we manufacture the drive to how you use it – to provide the next stage of evolution in both security and user experience. In order to protect your data and your privacy we considered both the ways in which it could be used and how it could be misused by an attacker.

Our goal for the ArmorLock Security Platform was to set the bar for security and data protection in app-enabled, connected products. We're sharing the information in this whitepaper, as well as our work on the open source Sweet B encryption library, to provide transparency in our platform and demonstrate our commitment to the security and privacy of our users.

Security is an active process, and if you are a security researcher and wish to contact us regarding our products, please visit our Product Security Incident Response Team (PSIRT). For more information on Privacy at Western Digital, please visit our Privacy Center.

Western Digital.

To learn more about the ArmorLock encrypted NVMe SSD, visit GetArmorLock.com.

5601 Great Oaks Parkway
San Jose, CA 95119, USA
www.westerndigital.com

*As used for transfer rate, 1 MB/s = 1 million bytes per second. Based on internal testing; performance may vary depending upon host device, usage conditions, drive capacity, and other factors.

Western Digital, G-Technology, the G-Technology logo and ArmorLock are registered trademarks or trademarks of Western Digital Corporation or its affiliates in the U.S. and/or other countries. The NVMe™ word mark is a trademark of NVM Express, Inc. The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Western Digital is under license. Apple, iPhone and Mac are trademarks of Apple, Inc. App Store is a service mark of Apple Inc. All other marks are the property of their respective owners. Product specifications subject to change without notice. Pictures shown may vary from actual products.