International Research Journal on Advanced Engineering and Management

https://goldncloudpublications.com

e ISSN: 2584-2854
Volume: 02
Issue: 01 January 2024
Page No: 01-05

Data Wiping Journey Through Redkey

Kumudavalli M V[1], VidhyaShankar[2], Gunav S[3], Hemanth Uppala[4]*

[1]*Professor, Department of Computer Applications, Dayananda Sagar College of Arts Science & Commerce, Bangalore, Karnataka, India.*

[2,3]*UG- Department of Computer Applications, Dayananda Sagar College of Arts Science & Commerce, Bangalore, Karnataka, India.*

[4]*Assistant Professor, Department of Computer Applications, Dayananda Sagar College of Arts Science and Commerce, Bangalore, Karnataka, India.*

Email:*kumudavalli@dayanandasagar.edu*[1]*,overlordnandan@gmail.com*[2]*,gunavguru007@gmail.com*[3]*,uppala.hemanth@gmail.com*[4]

Corresponding Author Orchid ID: *0000-0001-5676-8770*

Abstract

Red Key is a powerful and trustworthy digital security system that grants users several advantages. Red Key guarantees the protection of sensitive data and reduces the risk of unwanted access with its increased security features. Red Key's user-friendly interface makes it simple for people to manage their security settings and offers a seamless user experience. Additionally, users can adjust their security preferences to their unique demands. The ability of Red Key to integrate with other security systems allows for smooth communication and collaboration, offering a complete security solution. Red Key receives regular upgrades to keep up with the most recent security protocols, protecting it from new attacks. Red Key is a trustworthy and effective digital security system overall. File Hex viewer which indicates the content on hard disk before and after the data wiping process, is a highlight of RedKey. It emphasizes on complete data-wiping process. The algorithm approach of RedKey makes the data-wiping process so unique that no other competitive device is capable of the same. This article emphasizes the working structural view of the device with its pros and cons making the end-user usage process simple.

Keywords: *Red Key, Security, Data, USB, Wiping.*

1. Introduction

It's simple to overlook that data breaches can easily happen if organizations don't erase confidential data when destroying or selling their old laptops, what with all the attention being paid to fraudsters and internet attacks. The PC will eventually go out of date. It can be something you want to sell or give to someone else. The Redkey is useful in situations like these. You must format the same to completely delete the system's data. However, in this technological age where there are so many clever hacking techniques, it is still reasonable to question whether our system is secure or whether there is a risk. Gareth Owen created the Redkey USB device to securely wipe data. The Redkey software is offered as a bootable live USB drive that can be used on a perpetual license basis. The best tool for wiping hard drives is Redkey USB. It's a simple, cost-effective solution that will help you maintain your privacy and make sure no one can access your sensitive data. You won't ever have to be concerned about someone obtaining access to private records or images.

2. End users of Redkey

Whether a computer newbie, general user, or IT professional, anyone can utilize Redkey USB. Redkey USB comes with basic, easy-to-follow instructions, so anyone can use it. Redkey USB has a great customer support service that will be

International Research Journal on Advanced Engineering and Management

https://goldncloudpublications.com

e ISSN: 2584-2854
Volume: 02
Issue: 01 January 2024
Page No: 01-05

pleased to assist you if you have any issues.

3. Usage of Redkey USB

These days, we go through technology like we do shoes. We replace our smartphones almost every year, along with a variety of other frequently used devices, and our laptops every few years. When you replace an older device, you'll likely sell it, give it to someone who can use it, or give it to someone else, all of which are much better options than just throwing it out to rot in a landfill. The issue is that should your gadget fall into the wrong hands, you'll want all of your important data destroyed. There is a technique to get rid of all traces of that data with the Redkey USB V4 Ultimate [1]. This tiny dongle, which is marketed as a "sophisticated permanent information disposal device," can wipe not only PCs and laptops but also cellphones and tablets. This device enables you to delete any data, including logs of your dubious online activity, private work documents, or even the tiniest traces of credit card information, without the need for technical expertise or specific software. Free disk-wiping tools are widely accessible, but few offer any certification of data eradication for auditing and regulatory compliance. As this modest memory stick is packed with military-grade tools for safely erasing SATA HDDs and SSDs as well as USB, NVMe, M.2, PCIe, and eMMC storage devices, Redkey USB appears to be the perfect option. RedKey USB can be used as many times as you'd like, unlike certain commercial erasing utilities that impose pay-per-drive licensing. You can use the gadget as often as you'd like on as many Windows or Mac computers and a single payment includes eternal online upgrades and support.

4. Redkey USB Ease of Use

Very few people who are knowledgeable about computer hardware and software are aware that lost data can sometimes be restored. Utilizing Redkey is simple. Simply connect it to the PC you want to clean. Once the computer has started, hit the key to access the boot menu. From this option, select Redkey, and then adhere to the prompts on the screen. You'll quickly be operational. Simply use a data cord to connect mobile devices to a computer running Redkey. It employs an effective way to delete all of the public and private information, including passwords and important files. Additionally, the entire procedure that makes Redkey USB the ideal tool for secure data erasure is covered in the working section that follows [2].

5. Redkey USB Device

5.1 Significant Features of Red Key

- Redkey USB: The approved data wiping solution you require for privacy protection.
- Unlimited use: Unlimited device wiping is permitted. No limitations.
- No hidden costs: Redkey just requires a single investment; there are no ongoing costs or license fees.

5.2 Updates included

Keep your Redkey up to date with our complimentary software update program.

5.3 Advantages and Specifications of the Device

- Easy to use Automatic Mode
- 25 Defense Wipe Standards
- Helps to View Reports & Check Results before and after the data erasure
- Unlimited Use & Online Updates (Does not expire)
- It will work on all with the same efficiency.
- It is also a powerful tool for businesses to redeploy their internal computer systems [5].

5.4 Disadvantages or Redkey as a threat

- Erases all the external devices connected to the very inconvenient target computer.
- It may be a threat and used in a data breach to target the consequences and aftermath is discussed in the below points. The destruction of any information such as Personally Identifiable Information, Financial Information, Health Information, Competition Information, Legal Information, IT Security Data [6].

5.5 Key Selling Points of Redkey

No subscriptions, no continuing fees, one-time purchase Regular online software upgrades,

International Research Journal on Advanced Engineering and Management

https://goldncloudpublications.com

e ISSN: 2584-2854
Volume: 02
Issue: 01 January 2024
Page No: 01-05

Certified (Scientifically Proven), unlimited use, and Does Not Expire.

1. **Security:** Security begins even before you receive the goods because it is dispatched through tracked shipping and comes with a robust, tamper-proof box for the Redkey USB. The Redkey USB Updater application, a portable executable that needs to be executed on a Windows PC with internet connectivity, is used to prepare it when it comes blank.
2. **Activation:** Inserting the device and entering the 20-digit authorization code that is tucked away under a scratch panel within the package is all that is required to activate it. After the code has been validated, you can let the software finish downloading all necessary data and setting up the Redkey USB as a bootable device. When scripting for the Ultimate version, which uses a text file on the device that may be updated to create unique wipe sequences, use the default automated erase settings or customize them from the application. You can, for instance, specify priorities for erase functions, plan a series of actions, such as turning off the computer automatically when the wipe is finished, and allow auto-saving for erasure reports [8]. A Simple Working Representation of Complicated Data Wiping Software is shown in Figure 1.

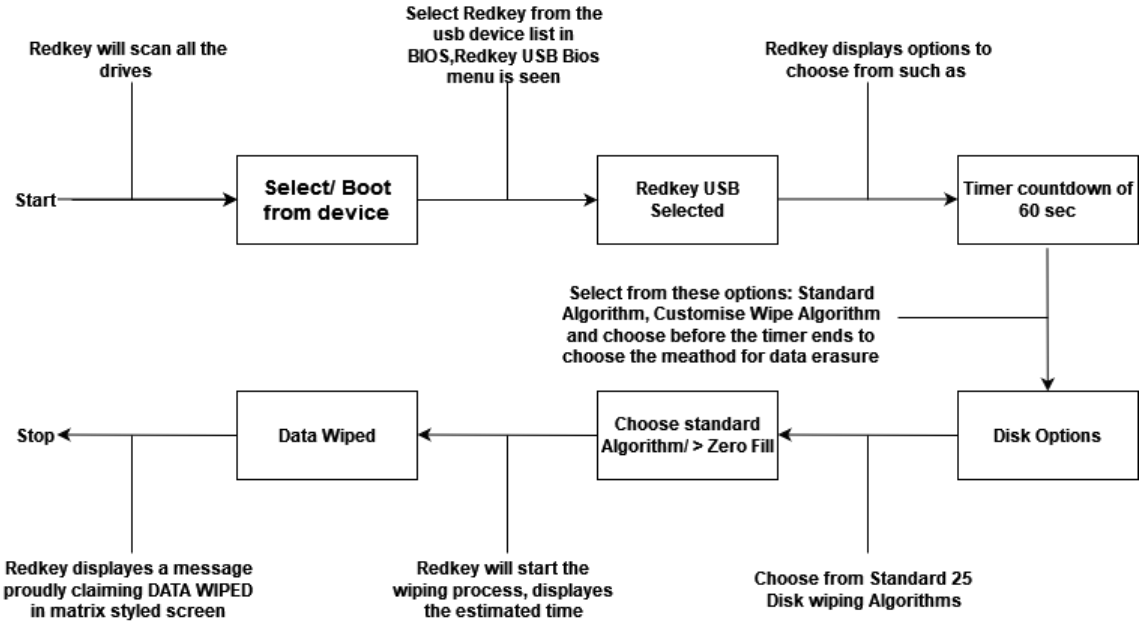

Figure 1 Simple Working Representation of Complicated Data Wiping Software

6. Future Enhancement

Redkey is a tool to erase data or is used for computer refurbishment purposes. So, when it comes to Security or Authentication, they have their process which adds security software fixes where it has a USB Updater utility which is a portable and executable utility that must be run on a computer with internet access which will update the wiping software. Not only that they also have another important security feature which will activate the device with a 20-digit authorization code to enter, hidden in a scratch panel inside the package. Once authorization is done, the code is verified from their servers, only then the device can be used to do the data erasure. Therefore, we can say that the activation process is the final step of security that Redkey USB has [9].

International Research Journal on Advanced Engineering and Management

https://goldncloudpublications.com

e ISSN: 2584-2854
Volume: 02
Issue: 01 January 2024
Page No: 01-05

7. Implementation of Strong Hardware Authentication

The given software layer of security such as online Activation or Live Software Updates might not prevent any user from using it on any computer to wipe the data, once the device is activated. To further add more security, a suggestive method is to suggest that they add a biometric scanner for authentication, such that it will provide an additional layer of security. This feature would ensure that only authorized individuals can access the files and password manager stored on the USB. USB Drive is shown in Figure 2.

Figure 2 USB Drive

8. Data Recovery Options

Introducing data recovery options, such as automatic backups or file versioning, would provide users with a safety net in case of accidental file deletion or corruption. This feature could help restore lost or corrupted data and prevent potential data loss scenarios [10].

9. Enhanced Speed and Capacity

Increasing the read and write speeds of the USB, as well as offering higher storage capacities, would improve overall performance and accommodate larger files. This upgrade would cater to users who work with high-definition media, large databases, or resource-intensive applications [11]

Conclusion

As a digital security system, Red Key offers several notably advantageous features. Red Key should give priority to integrating cutting-edge biometric authentication techniques like fingerprint scanning when it comes to software. The risk of illegal access would be lower and user authentication would be strengthened. Red Key would be able to dynamically modify security measures based on the perceived danger level thanks to contextual risk assessment, which is powered by machine learning algorithms. This would result in a more flexible and efficient security solution. Further enhancing Red Key's capabilities and preventative defense against new attacks would be the addition of secure collaboration features, sophisticated user behavior analytics, and integration with threat intelligence platforms. Red Key can maintain its position as a top digital security system by addressing these areas for development in both hardware and software aspects. To offer users a reliable and future-proof solution that assures maximum security and user happiness, Red Key must constantly evolve and keep ahead of new threats [10]. It is a dependable option for safeguarding sensitive data due to its improved security methods, user-friendly interface, customizable protection levels, integration possibilities, and dedication to routine upgrades [12]. Red Key may, however, be made even better in some areas to offer even greater security and user experience. Red Key should think about integrating secure parts like hardware security modules (HSMs) [13] or secure enclaves when it comes to hardware updates. These upgrades would protect cryptographic keys and guarantee the reliability of crucial security procedures. Red Key's security would also be greatly improved with the inclusion of hardware-based biometric authentication and quantum encryption, making it more resilient to attacks and illegal access. [14] [15].

Acknowledgment

The authors thank the management of Dayananda Sagar College of Arts Science and Commerce for facilitating us in carrying out this research work.

References

[1]. Thomas Martin and Andrew Jones, (2011), “An Evaluation of Data Erasing Tools”, https://www.researchgate.net/publication/342578310_An_Evaluation_Of_Data_Erasing_Tools.

[2]. Andreas Gutmann, Mark Warner, (2019), “Fight to be Forgotten: Exploring the Efficacy of Data Erasure in Popular Operating Systems”,

e ISSN: 2584-2854
Volume: 02
Issue: 01 January 2024
Page No: 01-05

https://www.researchgate.net/publication/333088698.

[3]. Mao Juan, Li Yong-Mei, Liu Min (2010), "Research for data erasure based on EEPROM", https://ieeexplore.ieee.org/document/5593720

[4]. Sun Liye, Liu Sheng, Jing Fei, Lin Yang, Wang Yingying, (2022), "Research Ideas and Analysis of the Electronic Archive Data Erasure and Destruction Platform", https://ieeexplore.ieee.org/document/9734513

[5]. Craig Wright1, Dave Kleiman, and Shyaam Sundhar R.S., (2008), "Overwriting Hard Drive Data: The Great Wiping Controversy", "https://www.researchgate.net/publication/221160815

[6]. Miroslav Ölvecký; Darja Gabriška, (2008) "Wiping Techniques and Anti-Forensics Methods", https://ieeexplore.ieee.org/document/8524756

[7]. George Pecherle, Cornelia Győrödi, (2010) "Data wiping system with fully automated, hidden and remote destruction capabilities", https://www.researchgate.net/publication/229014131

[8]. Kyungroul Lee, Byeong-Geun Son, Sun-Young Lee, Kangbin Yim, (2018), "Vulnerability analysis of secure USB: based on the fingerprint authentication of product B", https://dl.acm.org/doi/abs/10.1145/3264746.3264813

[9]. Suratose Tritilanunt, Napat Thanyamanorot, Nattawut Ritdecha, (2014), "A secure authentication protocol using HOTP on USB storage devices", https://ieeexplore.ieee.org/abstract/document/6946255

[10]. Ann L. Chervenak, Vivekanand Vellanki, Zachary Kurmas, (1998), "Protecting File Systems: A Survey of Backup Techniques", https://www.storageconference.us/1998/papers/a1-2-CHERVE.pdf

[11]. Radu Stoica, Manos Athanassoulis, Ryan Johnson, Anastasia Ailamaki, (2009), "Evaluating and repairing write performance on flash devices", https://dl.acm.org/doi/abs/10.1145/1565694.1565697

[12]. D. Roberts, H. B. Wolfe, "Data Remanence in New Zeland: 2011", (2011), https://www.researchgate.net/publication/342578310_An_Evaluation_Of_Data_Erasing_Tools

[13]. Stathis Mavrovouniotis & Mick Ganley, "Hardware Security Modules", (2013), https://link.springer.com/chapter/10.1007/978-1-4614-7915-4_17

[14]. Filippo Del Tedesco, Alejandro Russo & David Sands, (), "Implementing Erasure Policies Using Taint Analysis", https://link.springer.com/chapter/10.1007/978-3-642-27937-9_14

[15]. Martha Dewey Bergren, Elizabeth Ann Murphy, (2005), "Data Destruction", https://www.researchgate.net/publication/315216667_Data_Destruction.