A Survey On
Security Protocol for USB Mass Storage Devices

Mayuri K. Dhole
Department of computer Science and Engineering
G.H. Raisoni College of Engineering,Nagpur, India

Prof. SonaliNimbhorkar
Department of computer Science and Engineering
G.H. Raisoni College of Engineering, Nagpur, India

Abstract- The Universal Serial Bus (USB) is the popular interface for connection to hardware and the USB peripheral devices have also increased in numbersin recent decades. External USB storage device are considered as popular devices in market. USB can transmit data with high speed and is highly convenient to use. But many companies have banned the use of USB devices to prevent theft of confidential data from computers of the companies via USB ports. However, convenience of the USB connection is compromised. Therefore, finding a way to take into account security of environment in company along with the user's convenience has become an important issue. Many security protocols have been proposed till date to prevent the theft of confidential data. In this paper a survey on different security protocol for USB mass storage devices that are existing is given.

Keywords- Universal Serial Bus, USB storage device, Security protocols.

I. INTRODUCTION

Removable mass storage media such as portable hard disks, flash drives, memory cards etc. are connected through a USB (Universal Serial Bus) port. They are widely used to transfer or backup data because it has small size and they are convenient to carry. . But these MSDS are strictly prohibited in public workplaces due to security concerns. Universal Serial Bus (USB) is a common port used for connecting keyboards, mice, pen drives etc. It is a universal interface for hardware connection such as consumer/removable mass storage devices (MSDs).USB port provides high transmission speed but using this port can be considered as going through non secured gate. For example, flash drives or other storage device contains confidential data which can be at the risk of being stolen. Also theUSB interface has the following drawbacks when it is being used for consumer mass storage devices:

- Any unauthorized user could read or steal confidential data easily because the information is stored in plaintext format.
- An adversary could intercept or attack the transmitted data because the transmit channel between the device and the computer is not secure.

Therefore, despite their practicality, an enormous number of environments prohibit USB Mass Storage Devices (MSDs). That is why an effective authentication protocol should be provided for these mass storage devices.

II. LITERATURE SURVEY

1. ***A Secure Control Protocol for USB Mass Storage Devices***

   Fuw-Yi Yang, Tzung-Da Wu, and Su-Hui Chiu [1] proposed a protocol that gives mutual authentication and key agreement between client and server to solve the problem of both convenience and management. This protocol consists of two phase: Registration phase and verification and data encryption phase. This protocol realizes mutual authentication, key agreement, file protection and resists attacks.

2. ***Analysis and Improvement on an efficient Biometric-based Remote user Authentication Scheme using Smart Cards***

A.K. Das [2] proposed that the improved scheme provides strong authentication with the use of verifying biometrics, password and also random or arbitrary number that the user and the server generates as compared to other protocols.

3. ***Three factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices***
C. Lee, C. Chen, P. Wu [3] proposed a protocol that combines biometric, password and smart card to provide high security. They also adopt ECC (Elliptic Curve Cryptosystem) to encrypt data. This protocol cannot tolerate DOS attack, impersonation, Man-in-the-middle attack.

4. ***Enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices***
Debiao He, Neeraj Kumar, Jong-Hyouk Lee, and R. Simon Sherratt [1] proposed significant enhancements to the three-factor control protocol that now makes it secure from different types of attacks such as the password guessing attack, the denial-of-service attack, and the replay attack. The solution proposed is presented with a high security analysis and practical computational cost analysis to show that the new security protocol is very useful for consumer USB mass storage device.

5. ***A Secure Data Transfer Algorithm for USB Mass Storage Devices to Protect Documents***
In this paper A. N. Magdum, Y. M. Patil [5] proposed a secure control algorithm which provides mutual authentication and key agreement between client and server to avoid this problem. They have proposed a control algorithm which implements user authentication and for effectively governing file transmission via the USB port implements key agreement. Also to provide additional security a system that will encrypt or Decrypt the data which is to be transmitted via USB havebeen proposed.

III. CONCLUSION

This paper provides the complete analysis of the different security protocols for mass storage devices. Some protocols use only password for security, some use biometric keys, some use smart cards and some use combination of all these. Protocol must be strong enough to secure the data and documents stored in mass storage devices. Each technique is unique and is suitable for different applications in its way. Everyday new encryption technique is evolving. Hence fast, secure and conventional techniques for encryption will always have high rate of security.

REFERENCES

[1] Fuw-Yi Yang, Tzung-Da Wu, and Su-Hui Chiu,” A Secure Control Protocol For USB Mass Storage Devices”, IEEE Transaction on Consumer Electronics, vol.56, no. 4, pp. 2339-2343, Nov. 2010.

[2] A. K. Das,”Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards,” IET Informatio Security, vol.5, no. 3, pp. 145-151,Sept. 2011.

[3] C. Lee, C. Chen, and P. Wu, “Three-factor control protocol on elliptic curve cryptosystem for universal serial bus mass storage devices,” IET Computers and Digital Techniques, vol. 7, no. 1, pp. 48-55, Jan 2013.

[4] Debiao He, Neeraj Kumar, Jong-Hyouk Lee, R. Simon Sherratt, “Enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices,”IEEE Transactions on Consumer Electronics, Vol. 60, No. 1, February 2014.

[5] A. N. Magdum, Y. M. Patil, “A Secure Data Transfer Algorithm for USB Mass Storage Devices to Protect Documents”, International Journal of Emerging Engineering Research and Technology Volume 2, Issue 4, July 2014, PP 78-84.